Comments of
Pepco Holdings, Inc., and its Subsidiary Companies
To
The National Institute of Standards and Technology ("NIST")
Preliminary Cybersecurity Framework

Pepco Holdings, Inc. ("PHI"), and its jurisdictional subsidiaries, Potomac Electric Power Company ("Pepco"), Delmarva Power & Light Company ("Delmarva"), Atlantic City Electric Company ("Atlantic City"), (collectively referred to as the "PHI," "Company" or "Companies"), hereby submits these response comments to the National Institute of Standards and Technology ("NIST"), Preliminary Cybersecurity Framework ("Cybersecurity Framework"), released on October 22, 2013. The PHI Companies are each regulated transmission and distribution utilities, and together, provide transmission and distribution services to over 1.8 million retail customers in the Mid-Atlantic region, including the nation's capital. PHI submits these comments in order to assist NIST in its efforts to finalize the Cybersecurity Framework as required by Executive Order 13636, *Improving Critical Infrastructure Cybersecurity* ("EO"), issued February 19, 2013. The Company appreciates the opportunity to comment on the Cybersecurity Framework and commends NIST for its successful efforts in bringing a collaborative approach, across diverse industries, to the development of its Preliminary Cybersecurity Framework. PHI recognizes the monumental task NIST has undertaken to ensure the applicability and success of the Cybersecurity Framework and expresses its appreciation to NIST and all the volunteers for their efforts. The development of the Preliminary Cybersecurity Framework is particularly noteworthy given its broad scope and tight delivery deadlines set forth by the EO. The response comments provided herein are offered as guidance to assist NIST in effectively finalizing the Cybersecurity Framework.

At the outset, PHI joins in and supports the thorough and well-reasoned comments submitted by the Edison Electric Institute ("EEI") and Utilities Telecom Council ("UTC"). As EEI's comments are thorough, PHI will not repeat them, but submits these additional comments to highlight certain matters we wish to emphasize.

I. With certain clarifications to its scope, the NIST Cybersecurity Framework approach adequately identifies outcomes that strengthen cybersecurity to appropriately integrate cybersecurity risk into business risk.

By proposing a foundation for organizations to identify their respective risks and objectively assess the capability and maturity of their cybersecurity processes and procedures, the Preliminary Cybersecurity Framework effectively defines outcomes that strengthen cybersecurity across multiple industries. It is essential, however, that the Framework's focus be on solely those organizations and their associated assets and systems that are essential to critical infrastructure functions which are key to the security of nation's economic, health, and safety. Accordingly, to provide needed clarity as to Framework's scope, a listing of the 16 critical sectors should be included in the Framework introductory as those within the Framework's scope. Language currently within the Framework Core that references, "business purposes," "business needs," "business objectives," and other similar business-mission focus should be removed. To do otherwise suggests a scope that would reach beyond the critical infrastructure assets and systems, and divert organizations' limited resources to assessing assets and systems not vital to critical infrastructure cybersecurity. The appropriate definition of critical infrastructure, as set forth in the Framework is, "[S]ystems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on cybersecurity, national economic security, national public health or safety, or any combination of those matters" (EO 13636 Sec. 2). Therefore, only those businesses with systems and assets critical to the national economy, health, safety and security should be within Framework's focus.

II. The Framework provides sufficient guidance and resources to aid diverse businesses in assessing cybersecurity risks while maintaining use flexibility.

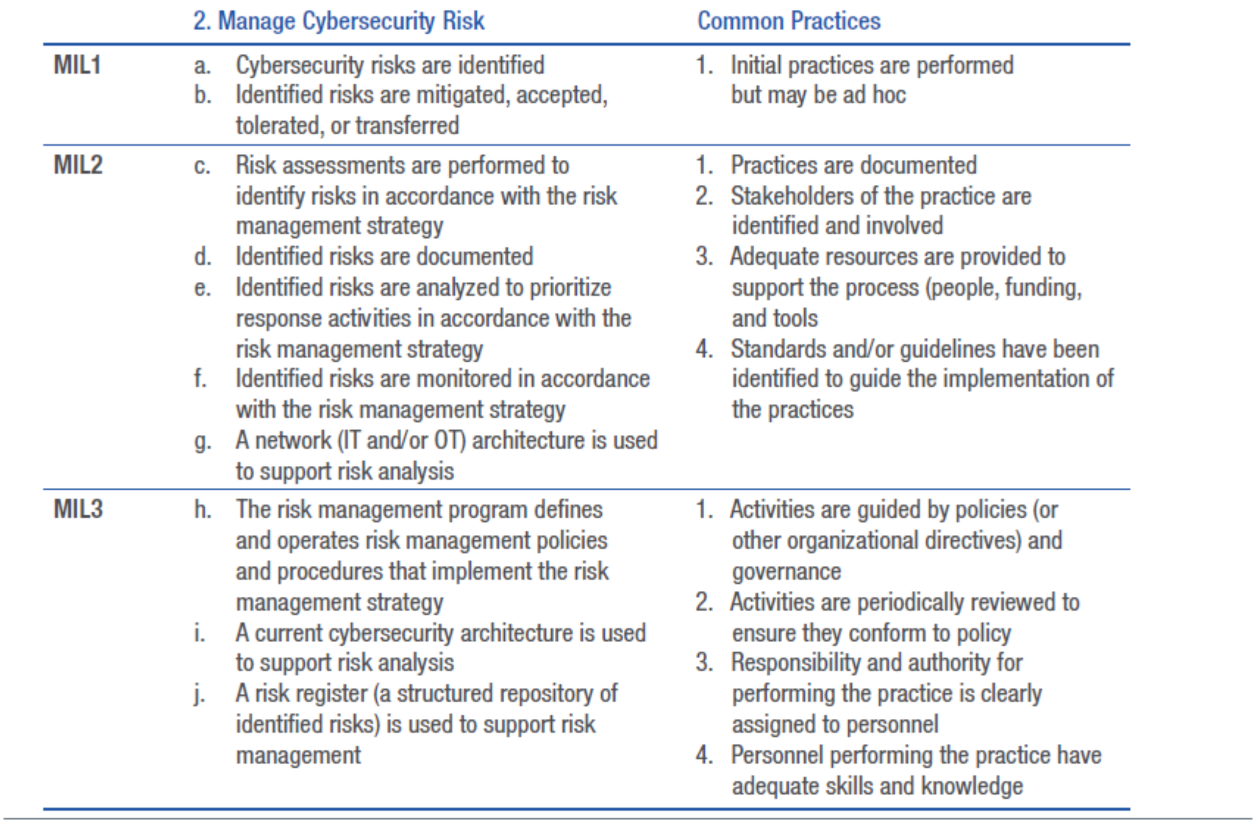
NIST's Cybersecurity Framework is balanced and adaptive which affords critical infrastructure the flexibility to use appropriate tools and technologies to achieve desired outcomes as described in the Framework's Core. However, the definition of "Framework adoption," has not reached general agreement. Without a clear and generally understood definition of what it means to "adopt" the Framework, ready application of it by sector organizations can be slowed. The proposed definition should be clear and straightforward and easily applied across business sectors. Accordingly, we recommend that NIST simplify the adoption definition to an organization adopts the framework, "when it voluntarily uses the framework as a part of its risk management process."

The finalized Framework should remain adaptive in order for diverse industries critical to the nation's economic security, health and safety to effectively apply the Core and its Subcategories to their specific industries. The Framework in its current state is practical and useful. The goal moving forward will be to continue to permit adaptability in the application of the Framework tools within an environment with ever changing challenges. In order to achieve this, the Framework will need to be maintained, updated and challenged. We therefore recommend a continuation of a collaborative industry approach, as adopted by NIST in the development of the Preliminary Cybersecurity Framework, to ensure that future changes and updates to the Framework provide adaptability across industries.

The Framework's risk-based approach is sound. Deployment of a risk-based management process appropriately begins with an assessment of cyber risks, and then a prioritization of those risks that lead into a development of responsive actions to address the risks identified via the implementation of effective cybersecurity practices. The Framework's risk-based approach enables decision makers to evaluate their cyber risk and make informed decisions. Further, the approach allows organizations to leverage practices that maximize the use of resources to reduce risk, while enabling each organization to advance its cybersecurity management in a manner that is cost-effective and tailored to the industry and readiness needs of the organization implementing the practice. PHI complies with mandatory cybersecurity requirements and appropriate voluntary guidelines developed through federal and private entities partnerships. While these existing requirements and guidelines provide comprehensive guidance to electricity asset owners and operators to assess, develop, and improve cybersecurity capabilities, the Framework's risk-based approach can be integrated into current activities without disrupting the practices already established.

The Framework's Tiers provide a potential tool for senior executives and boards to better understand the current security level of their organization; however, the Tiers fail to provide the intended opportunity for increased understanding of cybersecurity risks and mitigation methods because of the confusion created by the introduction of an additional, and materially different, maturity model approach. The Framework Tiers' use of terminology within its categories and subcategories are inconsistent and do not translate to the maturity models adopted in the energy sector's use management practices. Specifically, the Tiers' terms do not translate easily to the functions, categories and subcategories provided in the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2). For example, the ES-C2M2 provides ratings in the categories of "not implemented, partially implemented, largely implemented, and fully implemented," scoring based on Mil 0-3[1].

Table 1: Mapping of Common Practices to Domain-Specific Practices, Example: RISK domain



	2. Manage Cybersecurity Risk	Common Practices
MIL1	a. Cybersecurity risks are identified b. Identified risks are mitigated, accepted, tolerated, or transferred	1. Initial practices are performed but may be ad hoc
MIL2	c. Risk assessments are performed to identify risks in accordance with the risk management strategy d. Identified risks are documented e. Identified risks are analyzed to prioritize response activities in accordance with the risk management strategy f. Identified risks are monitored in accordance with the risk management strategy g. A network (IT and/or OT) architecture is used to support risk analysis	1. Practices are documented 2. Stakeholders of the practice are identified and involved 3. Adequate resources are provided to support the process (people, funding, and tools 4. Standards and/or guidelines have been identified to guide the implementation of the practices
MIL3	h. The risk management program defines and operates risk management policies and procedures that implement the risk management strategy i. A current cybersecurity architecture is used to support risk analysis j. A risk register (a structured repository of identified risks) is used to support risk management	1. Activities are guided by policies (or other organizational directives) and governance 2. Activities are periodically reviewed to ensure they conform to policy 3. Responsibility and authority for performing the practice is clearly assigned to personnel 4. Personnel performing the practice have adequate skills and knowledge

The varying language of the Framework and the ES-C2M2 model would create complexity that could potentially inhibit the electric sector's implementation and adoption of the Framework. Accordingly, such as the ES-C2M2, which already provides a proven implementation system,

[1] MIL0: Incomplete, MIL1: Initiated, MIL2: Performed and MIL3: Managed.

PHI recommends that a common language be established among the Framework and such other industry models.

III. The Framework approach generally provides specificity and guidance for mitigating the impact of cybersecurity measures on privacy and civil liberties.

The Framework’s proposed method for the protection of privacy and civil liberties for a cybersecurity program, as set forth in Appendix B, *Methodology to Protect Privacy and Civil Liberties for a Cybersecurity Program,* provides a sufficiently straightforward example and guidance on how an organization’s practices and procedures can be effectively integrated to protect against the release of Personally Identifiable Information (PII) and data. The methodology, organized by Function and Category, is consistent with the Framework’s Core. Section 7(c) of the Executive Order; however, specifies that, "[t]he Cybersecurity Framework shall include methodologies to identify and mitigate impacts of the Cybersecurity Framework and associated information security measures or controls on business confidentiality, and to protect individual privacy and individual liberties." It appears, however, that the focus of the Framework, as set forth in Appendix B, is to recommend independent privacy protections that are not directly related to protecting critical infrastructure. We believe to fulfill the mandate of the EO for the protection of individual privacies and liberties, the appropriate focus should be on outlining approaches that would limit the privacy impacts of the Framework. Furthermore, the Executive Order mandates that the Cybersecurity Framework, “incorporate voluntary consensus standards and industry best practices to the fullest extent possible” which is not fully addressed in the proposed Framework.

Appendix B can be improved by adoption of a more clear and actionable methodology. We note that Harriet Pearson has provided NIST with an alternative approach for the protection of individual privacy and individual liberties.[2] She proposes this approach as an alternative to Appendix B. Her approach sets forth concepts and principals that are more actionable and processes driven than what currently appears in Appendix B. NIST should consider this alternative approach for how to improve its method for protecting the privacy and civil liberties of individuals.

It is also important to note, like the Framework's Core, the objective of the proposed method for protecting privacy and civil liberties should be neither to impose additional privacy oversight on owners of assets and systems critical to industry infrastructure, nor to replace currently-existing legal obligations that afford best practices protection of PII. The methodology in Appendix B should be revised and tailored to the stated purpose of the Framework, ie., to improve critical infrastructure cybersecurity, in order to "help owners and operators of critical infrastructure identify, assess, and manage cyber risk."[3]

Lastly, the Framework's Core does not currently enable organizations to incorporate threat information. The Framework excludes from its Core an "*Automated Indicator Sharing*," tool. Rather, the Core leaves that effort to be among those areas for "improvement that should be addressed through future collaboration with particular sectors and standards-development organizations," Appendix C: *Areas for Improvement for the Cybersecurity Framework*. While a recommendation for immediate integration of an automated indicator sharing tool that provides organizations timely, actionable information for real time detection and response to

[2] December 5, 2013, Harriet P. Pearson.
http://csrc.nist.gov/cyberframework/framework.comments/20131205_harriet_pearson_hoganlovells.pdf

[3] Executive Order 13636, Improving Critical Infrastructure Cybersecurity Sec. 7(b)

cybersecurity events may be premature, this area of focus should be given priority for future improvement through collaboration and implementation among sectors.

Again, PHI appreciates the opportunity to provide these responsive comments to the Preliminary Cybersecurity Framework. PHI looks forward to continuing to collaborate with NIST to finalize the Cybersecurity Framework and move forward to develop sector-specific implementation guidelines for the establishment of and support for the creation of a Voluntary Critical Infrastructure Cybersecurity Program.