UTILITIES TELECOM COUNCIL

1129 20th Street | Suite 350 | Washington, DC 20036
202.872.0030 *Phone* | 202.872.1331 *Fax*
www.utc.org

April 8, 2013

Office of Policy Analysis and Development
National Telecommunications and Information Administration
U.S. Department of Commerce
cyberincentives@ntia.doc.gov

Re: Notice of Inquiry: Incentives to Adopt Improved Cybersecurity Practices

Greetings,

UTC is pleased to submit our response to the Department of Commerce Notice of Inquiry regarding Incentives to Adopt Improved Cybersecurity Practices

UTC is looking forward to continue participating in the development of the Cybersecurity Framework through the workshops, dialog, and other venues. If you have any questions about the content of this response, please do not hesitate to contact us.

Sincerely,

Nadya Bartol, CISSP, CGEIT
Senior Cybersecurity Strategist
202-833-6809
Nadya.bartol@utc.org

UTILITIES TELECOM COUNCIL

1129 20th Street | Suite 350 | Washington, DC 20036
202.872.0030 *Phone* | 202.872.1331 *Fax*
www.utc.org

Introduction

Utilities Telecom Council (UTC) is pleased to submit this response to the Department of Commerce Notice of Inquiry in support of the efforts to facilitate adoption of the Cybersecurity Framework. Our response reflects input from UTC's municipal, cooperative and investor-owned utilities. Our response is also based on a listening tour that UTC performed over the last 6 months. The listening tour included various UTC member organizations, collectively providing electric power and natural gas services to over 40 million customers in North America. It was conducted with utility technology practitioners (cybersecurity, information technology, telecommunications, and control systems personnel) at a variety of organizational levels, including engineers, Chief Information Security Officers (CISOs) and Chief Information Officers (CIOs).

UTC Overview

Founded in 1948, the Utilities Telecom Council (UTC) is a global trade association dedicated to being the source and resource for information and communications technology (ICT) solutions for utilities and other critical infrastructure industries. UTC brings a worldview with a regional focus as a market leader for utility telecommunications advocacy and education with members in Europe, Canada, Latin America, the Middle East, Asia and Africa. UTC core members include utilities (energy, water, gas), pipelines and other critical infrastructure companies that operate mission-critical telecommunications and data networks in support of their core business operations. UTC's members include large investor-owned utilities that serve millions of customers across multi-state service territories, as well as relatively small rural electric cooperative utilities and municipal utilities that may serve only a few thousand customers each.

Utility Cybersecurity Challenges and Incentives

Over the recent past, the utilities sector has made remarkable progress in cybersecurity. Several significant challenges need to be overcome to ensure that this progress continues. During UTC's informal survey, UTC members identified several key challenges that applied across the utilities sector and across utility ownership types, including investor-(IOU), cooperatively-, and municipally owned utilities. Subsequent sections mention the challenges and match them with several types of incentives that were mentioned in these discussions.

Robust Legal Framework

UTC believes that a robust legal framework, including liability and information protections, is needed to provide incentives to promote cybersecurity by critical infrastructure entities.

UTILITIES TELECOM COUNCIL

1129 20th Street | Suite 350 | Washington, DC 20036
202.872.0030 *Phone* | 202.872.1331 *Fax*
www.utc.org

Regulatory and legal barriers exist that effectively dis-incentivize utilities from sharing cybersecurity threat and vulnerability information. Currently, utilities hesitate to share such information with each other and with the government, due to:

- Overall reputational risk of acknowledging a cybersecurity issue
- Concerns about having the shared information be subject to disclosure (especially in regard to state commissions)
- The possibility that the information may be subject to non-disclosure agreements with their vendors which prevent utilities' ability to share product-specific vulnerabilities
- Privacy protections and/or prohibitions on sharing customer information with the government
- Potential for use of shared information as the basis for additional or more stringent regulations, standards and oversight
- Uncertainty associated with the legal definition of the respective roles of the government and the private sector in terms of cyber warfare. To address that uncertainty, the private sector's responsibility for defending itself from a state-sponsored cyber-attack needs to be legally defined including clarifying the liability for consequences of a failure to act/exercise reasonable care, including the definition of reasonable and adequate.

Business Case for Cybersecurity

UTC believes that incentives are needed to establish a clear business case for cybersecurity in the critical infrastructure sector. The business case can be established through a combination of financial and non-financial incentives including streamlining regulations, raising awareness, and increasing outreach to critical infrastructure boards and executives.

One of the primary cybersecurity challenges in the utilities sector is the legacy infrastructure that is functional but not secure. Improving cybersecurity of this legacy infrastructure ranges from difficult to impossible. Replacing this infrastructure would impose a severe financial burden for the utilities industry but this process can be accelerated through incentives and policy changes. For example, the current rate-based recovery policies and depreciation schedules in the utilities sector have traditionally been aligned to the lifecycles of power equipment, which are much longer than the information technology (IT) refresh lifecycles. This creates a financial disincentive to replace obsolete IT equipment with state of the art, more secure equipment due to the creation of stranded costs.

The following are potential financial incentives to explore with regards to addressing the above challenges:

- Tax policy changes
- Changes in depreciation schedules to align IT equipment schedules with actual IT refresh lifecycles.

UTILITIES TELECOM COUNCIL

1129 20th Street | Suite 350 | Washington, DC 20036
202.872.0030 *Phone* | 202.872.1331 *Fax*
www.utc.org

It should be noted that everyone is a user of electricity and water. The added costs associated with improved cybersecurity posture resulting from the future implementation of the Cybersecurity Framework will be in effect a hidden tax on energy, water, and natural gas consumption. Government investment in infrastructure upgrades to replace obsolete and insecure legacy systems could serve as an incentive for the utilities to adopt the Cybersecurity Framework.

Collectively the utilities industry is a very diverse group. In addition to diverse ownership types, it includes combined companies that cross several critical infrastructure sectors, such as those companies that provide a combination of electric, gas, and water services. By virtue of belonging to more than one critical infrastructure sector at the same time, as well as by being subject to a variety of Federal, State, and Local laws and regulations utilities are concerned about duplicative requirements and regulations touching all these different areas.

Simply streamlining existing regulations could serve as an incentive for adopting the Cybersecurity Framework. To make that happen, the Framework should align any cybersecurity practices that may impact these combination companies in the electric, water, and gas sectors to ensure that the companies are able to use a single set of practices to address cybersecurity for these different critical infrastructure functions. The same applies to any potential regulations that reach beyond the entities currently subject to NERC CIP. For example, the Framework could name a standard or a set of practices that would translate into compliance for the utilities supporting multiple critical infrastructure sectors. If utilities could demonstrate compliance with that particular standard they would then be compliant with applicable requirements (e.g., NERC CIP) across these multiple sectors.

US government investment into cybersecurity Research and Development (R&D) and cyberecurity education for the critical infrastructure sector that results in real benefits to the industry will also serve as a non-financial incentive.

Incentives for Utilities' Industry Partners

UTC believes that Information and Communication Technology (ICT) vendors that provide critical infrastructure components and related services to the utilities should also be incentivized to improve their cybersecurity practices through the adoption of Cybersecurity Framework. We believe that the subject of acquirer/supplier relationships and dependencies in the utilities space should be closely studied and evaluated for what incentives could be offered to the utilities industry partners.

Utilities rely on their ICT vendors to implement a number of cybersecurity controls that could be effective in reducing cybersecurity risks. However, current standards and regulations, as well as market pressures, place a disproportionate burden of cybersecurity risk management on utilities.

UTILITIES TELECOM COUNCIL

1129 20th Street | Suite 350 | Washington, DC 20036
202.872.0030 *Phone* | 202.872.1331 *Fax*
www.utc.org

Current Costs of Compliance

Utilities are subject to mandatory cybersecurity requirements that apply to the bulk electric system, which includes all facilities operated at or above 100 kV.[1] These requirements are developed and adopted through the North American Electric Reliability Corporation (NERC). The NERC critical infrastructure protection (CIP) standards have been in place for years, but were made mandatory in accordance with the provisions of the Energy Policy Act of 2005 (EPACT 2005). Utility compliance with the mandatory NERC CIP standards is audited by NERC auditors, and utilities are subject to fines and penalties of up to $1 million per day/per violation. In addition to the costs of implementing security controls and possible costs of non-compliance, utilities expend substantial human and financial resources on the audit process itself, from ensuring availability of numerous staff members who are pulled away from their direct responsibilities to providing space, technology infrastructure, and facilities for sizeable auditing teams.

Promoting the Framework

UTC believes that requiring entities to join the DHS Program prior to receiving government financial guarantees or assistance is potentially problematic.

The diversity of the electric power industry is difficult to comprehend. Utilities have huge, widely varying scope, customer base, risk profile, and corporate structures. As such it is unlikely that the DHS Program will, at least initially, be a good fit for every single utility. The needs and resources of the largest Investor Owned Utility (IOU) differ substantially from those of the smallest cooperative. Requiring all entities to participate could therefore have the unintended consequence of forcing a utility to participate in a program that is not a good fit for its needs. Therefore, the DHS program should be carefully piloted with a diverse set of entities before entities are required to join it.

As previously mentioned, the Cybersecurity Framework itself, if designed to streamline standards and requirements, can serve as an incentive for adoption. If the industry believes that the Framework will facilitate streamlining numerous compliance requirements, the Framework is more likely to be adopted.

[1] Revisions to Electric Reliability Organization Definition of Bulk Electric System and Rules of Procedure, Final Rule, Docket Nos. RM12-6-000 and RM12-7-000; Order No. 773, 141 FERC ¶ 61,236, http://www.ferc.gov/whats-new/comm-meet/2012/122012/E-5.pdf.