U.S. Communications Sector Coordinating Council

To: Nakia Grayson
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg 20899

Re: Commission on Enhancing National Cybersecurity
Request for Information: Current and Future States of Cybersecurity in the Digital Economy
Docket Number: 160725650

Dear Ms. Grayson,

The Communications Sector Coordinating Council (CSCC) submits the following comments on Current and Future States of Cybersecurity in the Digital Economy for the Commission on Enhancing National Cybersecurity (Commission) under the Request for Information (RFI) Docket Number, 160725650.

The CSCC was established in 2005 to help coordinate initiatives to (1) improve the physical and cyber security of Communications Sector assets; (2) ease the flow of information within the sector, across sectors and with designated federal agencies; and (3) address issues related to response and recovery following an incident or event. The CSCC's 40 members broadly represent the sector and include cable, commercial and public broadcasters, information service providers, satellite, undersea cable, utility telecom providers, service integrators, equipment vendors, and wireless and wireline owners and operators and their respective trade associations. Collectively the CSCC represents more than 33 U.S. companies and several trade associations covering hundreds more companies in our industry. The Communications Sector is also identified by Presidential Policy Directive 21 (PPD-21) as one of 16 Critical Infrastructure and Key Resource (CI/KR) sectors and has a long history of cooperation within its membership and with the Federal Government with respect to national security and emergency preparedness (NS/EP).

In these comments, we focus upon certain topics identified in the RFI that we believe are most relevant to the Communications Sector. These include critical infrastructure cybersecurity and the role of the public-private partnership, federal governance, the need to support flexible risk-based standards vs. prescriptive regulation, public awareness and education, incentives for small and medium sized business, state and local government, the role of metrics, and finally innovation to address the cybersecurity challenges of the future. The comments also incorporate the testimony of Christopher Boyer, Assistant Vice President, AT&T Services, Inc., that was presented at the Commission's meeting in Houston, Texas on July 14, 2016 on behalf of the CSCC. In his testimony, which we have attached here, Mr. Boyer addressed many of the questions contained in the RFI, and we align with his representations before the Commission.

In particular we urge that, to the extent the Commission issues recommendations with its final report, that the Commission consider recommendations that 1) continue to support and strengthen the public-private partnership to protect the Nation's critical infrastructure, 2) promote technology neutral, flexible risk-

management approaches to cybersecurity, as opposed to prescriptive regulation, and 3) consider the role of evolving technology to address the cybersecurity challenges of the future.

1. Regulation/Critical Infrastructure/Public-Private Partnerships

The current U.S. policy in regards to critical infrastructure is outlined in the National Infrastructure Protection Plan (NIPP), which was initially drafted in 2006 and subsequently revised in both 2009 and 2013. The NIPP "outlines how government and private sector participants in the critical infrastructure community work together to manage risks and achieve security and resiliency."[1] The U.S. Department of Homeland Security (DHS) has also established the Critical Infrastructure Partnership Advisory Council (CIPAC) which is "aligned and supports the implementation of the NIPP and PPD- 21 to provide a forum in which the government and private sector entities, organized as coordinating councils, can jointly engage in a broad spectrum of activities to support and coordinate critical infrastructure security and resilience efforts."[2] These various bodies, along with each individual Sector Coordinating Council, Sector Specific Agency (SSAs) and corresponding Government Coordinating Council (GCCs), make up what is commonly referred to as the public-private partnership to address critical infrastructure security.

The Communications Sector is strongly committed to this process and has a long-standing and extensive partnership with the Federal Government to collaboratively address cybersecurity and other national security matters. The Commission should recommend that this collaborative process be continued. Indeed, the Commission's work couldn't come at a more critical time. Cybersecurity threats are diverse, borderless and growing in sophistication and frequency every day. This dynamic, evolving threat will only be effectively addressed through continued growth and strengthening of the public-private partnership that has been so critical to-date.

Even as we engage in these cooperative efforts, however, a principal area of concern is the increasing interest among government agencies to adopt prescriptive, regulatory responses to cybersecurity threats. Such efforts are not only misplaced but also counterproductive. Given the constantly evolving nature of the threats, cybersecurity does not lend itself to a checklist or mandated solution. Protecting against cyber threats is a risk-management function, and there is no one-size-fits-all solution for all companies. To the contrary, a prescriptive regulatory "solution" would simply set a static and lowest common denominator bar that would create a disincentive for the innovation and agility needed to respond to an environment that is characterized by nimble, sophisticated, and well-funded hostile actors and constantly-evolving threats.

As such, we urge the Commission to recommend flexible, risk-based solutions and discourage a prescriptive or siloed regulatory approach. A flexible approach encourages technological innovation and individualized security plans designed to meet risk. Indeed, companies are able to invest in tailored security solutions to protect their systems by assessing relevant threats, and subsequently developing and implementing appropriate risk-management plans. Conversely, broad, one-size-fits-all security rules may result in

[1] https://www.dhs.gov/national-infrastructure-protection-plan
[2] https://www.dhs.gov/critical-infrastructure-partnership-advisory-council

vulnerabilities by potentially forcing companies to spend their limited time and resources protecting data or systems that present limited, or in some cases, no risk of harm, or meeting standards that do not address their individual security environments, instead of spending resources in a more productive way.

The NIST Cybersecurity Framework exemplifies this approach. It recognizes the diversity of companies and the need for flexible and evolving solutions, and allows companies large and small to tailor the Framework to their specific business needs commensurate to their risk posture and available resources. Many members of Congress, the Administration and other portions of government have also recognized this model as appropriate to address cybersecurity. In fact, the U.S. government is promoting the voluntary, risk-management approach espoused by the NIST Cybersecurity Framework internationally as a more effective model for addressing cyber threats than regulatory-oriented regimes. And within the United States, the Federal Trade Commission (FTC) recently supported the use of the Framework as an industry best practice consistent with the FTC's long-standing approach to data security.[3] The Communications Sector has also tailored the Framework to our sector through an extensive participation in the FCC's Communications Security Reliability and Interoperability (CSRIC) Working Group 4 last year culminating in a comprehensive report that included use cases for how the Framework could be applied across each of the five key segments of the sector, and to small and medium sized communications companies.

Notwithstanding this consensus in support of the Framework, some continue to advocate for imposing cybersecurity mandates upon industry. This topic has been debated for several years and the overwhelming consensus on the part of Congress, industry and the Administration has fallen on the side of perpetuating the existing partnership augmented by steps such as the NIST Cybersecurity Framework, the ongoing work to finalize the National Cybersecurity Incident Response Plan (NCIRP) and other actions intended to bolster the effectiveness of the partnership. A departure from this approach towards government setting prescriptive standards for industry would be a mistake. While we recognize the important role of government, a regulatory approach will undermine the existing public-private partnership and the progress that has been achieved under that model. First and foremost, the Commission should reinforce that government and industry continue to work cooperatively, building upon the many different voluntary mechanisms that are already in place today, thereby rejecting the siren call for prescriptive regulation.

We also recognize that companies have a responsibility to take appropriate and reasonable steps to protect their systems. In considering the appropriate role for regulation in this area, we encourage the Commission to consider the approach of the FTC, which is founded in promoting reasonable efforts by companies to protect their systems and data. The reasonableness standards used by the FTC in its enforcement regime, including considerations about the sensitivity of the data, the resources of participants and the cost of available tools, are more effective than a prescriptive standards based approach to security.

In conclusion, preserving the collaborative, trusted environment between the public and private sector is essential in promoting new technology growth and innovation without fear of reprisal. In its final report, we urge the Commission to consider recommendations that will strengthen and grow the private-public relationship

[3] https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc

so that we can continue to create innovative, effective solutions to meet rapidly growing cyber threats head-on. In particular, the Commission should recommend continued government support for efforts by the CSCC and others to promote adoption of the NIST framework through outreach and education, particularly for smaller companies. Further, a forward-looking recommendation would be to adapt the NIST framework for emerging issues, such as IOT security.

2. Federal Governance

Another topic raised by the Commission in the RFI is that of federal governance. We focus on two primary areas. First, the U.S. government needs to finalize a formal incident response plan that outlines how government will organize itself and work with industry in the event of a large-scale cyber disruption. This was a key finding of the recent Cyber Storm exercise conducted this past March and is one of the recommendations offered by the Homeland Security Advisory Council (HSAC) to DHS Secretary Jeh Johnson. It is critical that we have this plan in place before we encounter a large-scale attack that may impact critical infrastructure.

Second, there are a vast number of government initiatives addressing cybersecurity which, in some cases, are redundant and duplicative. For example, there are numerous supply chain efforts involving the communications sector which span DHS, the FCC, the Department of Commerce and other agencies. This makes the current process for industry engagement highly inefficient. Also, as noted above, the inconsistent and contradictory engagement by certain regulatory agencies undermines the public-private partnership process preferred by many in both government and the private sector.

We strongly encourage the Commission to make recommendations to the President to rationalize existing initiatives and to better organize these activities across government to address the duplication of efforts and misallocation of government and industry resources.

3. The Internet of Things

The Commission also asks for recommendations related to the Internet of Things (IoT). As a precursor to our comments, we note that the sector is keenly focused on the security issues around IoT services. As devices become ever more connected, potential security vulnerabilities are likely to increase across the ecosystem, which requires cooperation across traditional sectors. IoT security, therefore, is a necessity, and the Communications Sector has been diligently working through a wide variety of standards bodies, such as GSMA and the Alliance for Telecommunications Industry Standards (ATIS) among others, on security specifications for the IoT. Further, communications companies have significant incentive to address security from the outset in order to succeed in the marketplace. In the United States, the NIST Cybersecurity Framework is a useful tool for individual firms to evaluate cybersecurity risks of all kinds and therefore should be the starting point on all security questions related to the IoT.

It is also important that the Federal Government establish a consistent policy regime for IoT. Recently the Department of Commerce (DOC) and the National Telecommunications and Information Administration (NTIA) launched a cross-cutting inquiry into IoT technology and policy issues. As the DOC/NTIA works to

establish a coherent and consistently applied policy regime for the IoT, it is essential that they distinguish between unique, "vertical" issues that may fall within the purview of a particular expert agency, and "horizontal" issues that cut across the IoT ecosystem's verticals and that should be handled consistently across all IoT technologies, business models and use cases. Cybersecurity is a prime example of a "horizontal" issue. These are natural concerns with every IoT use case, and indeed, consumers will rightly expect that their chosen IoT solutions will be secure and respectful of their privacy. Establishing this trusted environment for consumers will require input by all players in the IoT ecosystem — device makers, connectivity providers, application developers and platform operators; doing so will be crucial to our shared success in the market, separate and apart from the policy frameworks for these issues.

Given the broad and ever-growing variety of industry players competing in the IoT ecosystem, it will be impossible to regulate a path to effective privacy and security protection. Rather, those protections will depend on a robust multi-stakeholder process to define the practices that will engender consumer trust—and therefore adoption—across the system. Thus, for these horizontal issues, government should opt for a common, IoT-wide framework that relies not on regulation, but rather on multi-stakeholder efforts—including the relevant expert agency—that will facilitate development of effective privacy and security approaches. We encourage the Commission to endorse the DOC and NTIA process as the proper venue to continue this work vs. individual, independent agencies establishing redundant, isolated course of actions that are likely to result in ineffective mechanisms to resolve the same issues.

4. Public Awareness and Education

We believe that raising public awareness of cybersecurity is an important issue, and one in which the Federal Government needs to make a firm commitment and invest resources. Many of the Communications Sector member companies have participated in a variety of education programs related to cybersecurity, including participating in consumer-directed campaigns like STOP THINK CONNECT as members of the National Cybersecurity Alliance (NCSA), raising internal employee awareness around cybersecurity and promoting the NIST Framework within the Sector itself to drive use by member companies. This work should and will continue but we believe that there is a need for additional government support and a higher priority to be placed on these efforts if we expect any form of success in the near future.

5. Incentives for Small and Medium Sized Businesses

The Federal government also needs to revisit its continuing support for the NIST Cybersecurity Framework – and the private-sector "incentives," which were envisioned and promised in Executive Order 13636, that are especially important as they relate to small and medium size communications companies. As sector members have noted in previous proceedings[4], Executive Order 13636 directed the Secretary of DHS to coordinate "the establishment of a set of incentives designed to promote participation in the [Cybersecurity]

[4] *See* Comments of NTCA–The Rural Broadband Association, Request for Information: Experience with the Framework for Improving Critical Infrastructure Cybersecurity, Before NIST, the Department of Commerce, Docket No. 140721609-4609-01, October 14, 2014.

Program under development by NIST."[5] The sector appreciates this forethought given the complexity of the subject matter, and that many small/medium communications companies often operate with extremely limited resources. Of note, however, this is the wrong characterization of the need for assistance. Rather, these communications companies already strive to be as secure as possible with respect to their cyber operations, but given their lack of access to financial and/or operational assets, they are in need of support in regard to digesting and using the complex NIST Framework.

The FCC's CSRIC IV Working Group 4 sought to minimize barriers to using the NIST Framework, including by simplifying the Framework into more digestible bites; recommending how to use the resource within a company's operations; suggesting prioritized implementation of the numerous subcategories within the Framework; and providing information focusing on barriers and the special problems of use by small companies. However, while small and medium sized communications companies, like their larger counterparts, have significant market-based incentives to improve cybersecurity and do engage in risk management specific to their environment, their challenges in fully implementing the NIST Framework and certain CSRIC best practices often relate to their scarcer financial, human, technical, information and other resource. Consistent with its presidential directive, NIST should collaborate with DHS to release a complimentary set of incentives designed to help small and medium sized companies overcome barriers to use, especially those challenges that are unique or disproportionately difficult for smaller entities as they continue to assess their risks, and develop and evolve comprehensive and individual risk-management programs.

In a public document released in August 2013, the White House acknowledged that barriers to adoption of the Cybersecurity Framework exist and offered an initial examination of potential incentives, including insurance, liability protection, technical assistance,[6] rate regulation, and streamlining regulation.[7] Although the Framework itself has been developed over time through an extensive process, the creation of adequate incentives has not yet come to fruition. DHS and NIST should clearly define the breadth of incentives, the timeline of their availability, and how a small or medium communications companies can qualify for the incentives. A diverse set of incentives is likely to appeal to a diverse set of companies with various operational challenges. Apart from technical assistance, small/medium communications companies are most in need of incentives or grants related to NIST Framework activities.

6. State and Local Government

There are a variety of existing initiatives in place to address cybersecurity for state and local government such as the National Association of State CIOs (NASCIO) Cyber Disruption Planning Guide, and efforts by the National Governor's Association. The Commission should support the continuation of these efforts; however, at the same time the Commission should recognize that it is inefficient to duplicate all of the federal cybersecurity processes in each state. To address that concern, states should be encouraged to plug into the existing federal

[5] Executive Order, Sec. 8(d).

[6] Furthermore, any government-led training or assistance aimed at facilitating implementation of the Framework should not be made contingent upon the collection of sensitive business data or any company-level identifiable information. Any such requirements could discourage small business participation and impede implementation efforts.

[7] Incentives to Support Adoption of the Cybersecurity Framework, The White House Blog, Released August 6, 2013, 11:04 a.m. EST (available at http://m.whitehouse.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework).

public-private partnership via the Multi-State ISAC (MS-ISAC), the State, Local, Territorial and Tribal Government Coordinating Council (SLTTGCC) and other mechanisms. Further, states should not attempt to develop their own sets of security standards or best practices that would be duplicative and inconsistent with efforts being conducted on the federal level at NIST.

7. Metrics

The CSCC has extensive experience with cybersecurity metrics. This was a topic the industry attempted to address within FCC's CSRIC IV Working Group 4 in 2014. Within the report, industry was tasked by the FCC with providing insight into a "meaningful cybersecurity metric," and to identify measures that the Sector has determined best demonstrate the overall availability, reliability, resiliency, and integrity of critical communications infrastructure. This work on cybersecurity metrics also was envisioned to inform future macro-level discussions about metrics. As a result of this process, it was evident that there are unique challenges to developing relevant metrics related to cybersecurity, including the following:

- Cybersecurity is not an exact science and does not provide for exact measurement such as water, temperature, or network throughput. In many cases, it is difficult to determine the success or failure of a given practice, or even if recommended practices are having an impact.
- Inputs, outputs, and outcomes of cybersecurity are separated in time, making authoritative measurement challenging. In other words, protective controls such as security training, access control, or firewalls are believed to work; however, it is very difficult to pinpoint cause and effect. This makes outcomes difficult to articulate and quantify.
- Correlation does not imply causation. For example, the increase in a number of attacks or incidents may simply mean that intrusion detection and prevention systems have been updated and fine-tuned to register a greater number of events that previously might have gone unnoticed.
- Different organizations have different risk environments, goals for cybersecurity, and tools that they use to capture measures, and therefore comparing organizations is challenging and may not be meaningful.

Working Group 4 also evaluated what constitutes a "good" cybersecurity metric. According to national and international standards and guidelines on security measures/metrics, cybersecurity metrics should be built to support specific performance goals and objectives. For example, the NIST Framework contemplates firms determining their core mission and the cybersecurity threats or risks to that core mission, and then developing a "profile" of internal practices and controls, pulling from the suggested practices in the Framework, to best manage those risks. Cybersecurity metrics should support those efforts. For example, a firm may elect to implement a standard to minimize security threats stating that, "All employees should receive adequate information security awareness training," which is consistent with the recommended prevention practices in the Framework. In this example, an appropriate goal may be that "All new employees receive security training on an annual basis." A metric would follow monitoring the accomplishment of the objectives by quantifying the implementation of that particular goal, such as periodic status updates on the percentage of employees trained. These metrics should include enterprise-level guidance and correspond to the operational priorities of the

organization. These same factors are also outlined in NIST Special Publication 800-55 Revision 1, which identifies the characteristics of good measures.

These documents drive a conclusion that relevant metrics identify the cause of poor performance and potential corrective action. This is the unique challenge for cybersecurity given the issues outlined above. We strongly urge the Commission to give the appropriate consideration and evaluation to any further recommendations with regard to cybersecurity metrics. Any guidance from the Commission to develop cybersecurity metrics could be taken out of context and result in unintended consequences, such as regulators pushing industry toward irrelevant reporting and metrics, i.e. generating time-consuming, expensive reports that are of limited to no value. That result would do little to actually improve the nation's cybersecurity posture. As such, any further work on metrics should be undertaken jointly with the private sector to develop mutually agreed upon, relevant metrics and recommendations aligned with helping individual companies assess and improve their cybersecurity risk-management programs.

8. Innovation to Address Challenges of the Future

Finally the Commission should also be cognizant of the impact of its recommendations on innovation. The current model has allowed companies to innovate promising new security solutions to meet evolving cybersecurity threats. For example, many sector members are focused on moving towards virtualized security technology. Software Designed Networks (SDN) is an approach to networking in which network control is decoupled from the underlying data plane, and is directly programmable. SDN is augmented by Network Function Virtualization (NFV), which decouples network functions from dedicated hardware devices. The SDN control layer creates a global view of the entire network by gathering information in near real-time from the routers and using that information to make real-time decisions to control network nodes or update routes.

If there is a cyber incident, this type of architecture makes it possible to shift resources around, quarantine data, or limit an attacker's access to resources outside of a specific data set, all of which helps limit the impact of the attack and to speed recovery. Another example of this is the work that NIST is doing in the area of improving tools for software assurance and around strong authentication, a topic raised by the Commission. The use of Big Data Analytics (BDA) is also an emergent technology that was recently addressed in a report developed by the President's National Security Telecommunications Advisory Council (NSTAC).

These types of advancements in computing architectures hold promise for improved security over time. As the Commission considers incentives and advancements, in particular as it relates to government networks, which can leverage their procurement capabilities to incent change in the private sector, it is important to keep these technological innovations in mind. The Commission could put forth recommendations for how government can use incentives and other means to expedite this longer term migration, which combined with efforts like education and awareness, and improved standards and best practices, will lead to improved cybersecurity over time.

In closing, we appreciate the opportunity to submit comments and commend the Commission for its important work to-date. We urge the Commission to build upon the public-private partnership model that has

shown great success to-date, and to promote continued innovation and flexible security solutions in its recommendations and final report.

Sincerely,

Nneka Chiazor Verizon Chair, CSCC	Kathryn Condello CenturyLink Vice Chair, CSCC	Rudy Brioché Comcast Corporation Secretary, CSCC
Chris Boyer AT&T Executive Committee, CSCC	Matt Tooley NCTA Executive Committee, CSCC	John Marinho CTIA Executive Committee, CSCC
Brian Allen Charter Communications Executive Committee, CSCC	Robert Mayer USTelecom Executive Committee, CSCC	Jesse Ward NTCA–The Rural Broadband Association Executive Committee, CSCC