USTELECOM
THE BROADBAND ASSOCIATION

Testimony of Robert H. Mayer
Senior Vice President Cybersecurity
USTelecom
and
Chair
Communications Sector Coordinating Council

Before the
House Homeland Security Sub-Committee on Cybersecurity and Infrastructure Protection
Maximizing the Value of Cyber Threat Information Sharing
November 15, 2017

Chairman Ratcliffe, Ranking Member Richmond, and distinguished members of the subcommittee, thank you for giving the Communications Sector and me personally the opportunity to appear before you today for this important hearing on maximizing the value of cyber threat information sharing.

My name is Robert Mayer, and I serve as Senior Vice President Cybersecurity at USTelecom which represents companies ranging from some of the smallest rural broadband providers to some of the largest companies in the U.S. economy. I also serve as chair of the Communications Sector Coordinating Council (CSCC) which represents the broadcast, cable, satellite, wireless and wireline segments of the communications industry.[1] The CSCC is one of the sixteen critical infrastructure sectors under the Critical Infrastructure Partnership Advisory Council (CIPAC) through which the Department of Homeland Security (DHS) facilitates physical and cyber coordination and planning activities among the private sector and federal, state, local, territorial and tribal governments.

I want to thank the members of this subcommittee for emphasizing the concept of value in the context of information sharing. Of course, we endeavor to share cyber threat information not for information sharing's sake, but for the purpose of adding value to our operational and strategic cyber preparedness and defense efforts.

Today, the wide variety and large volume of cyber threat information sources, along with the growing number of information sharing venues, presents both opportunities and challenges in creating real value to information sharing. Since the passage of the Cybersecurity Information Sharing Act of 2015 [2], much has been done to reduce obstacles to sharing and to facilitate enabling mechanisms and venues. Still, this law is just the statutory foundation that will enable the actual sharing processes that need to be implemented; getting the right information to the right people at the right time with the appropriate privacy and security safeguards. This massive effort requires constant innovation, ongoing evaluation and disciplined resource allocation. Below I briefly outline the work of our sector in this area, some on-going challenges, and the important role of the DHS as a facilitator of cybersecurity information sharing.

The Communications Sector works on multiple fronts to share cyber threat information, and individual companies use a variety of information sharing platforms and services to achieve their objectives. From a sector perspective, two

[1] Communications Sector Coordinating Council, https://www.comms-scc.org.

[2] Cybersecurity Information Sharing Act of 2015, https://www.congress.gov/bill/114th-congress/senate-bill/754.

of the most prominent and robust information sharing venues operate in partnership with DHS.

First, the relationship between the Communications Sector and the DHS National Coordinating Center for Communications (NCC)[3] stands alone among critical infrastructure information sharing partnerships in both depth and length of partnership. Jointly, the relationship between the Communications Sector Information Sharing and Analysis Center (Comm-ISAC) and the NCC is one that many sectors are attempting to replicate. For more than 35 years, dating back to Cold War era existential concerns about telecommunications reliability and disaster recovery, the U.S. Government has worked in operational partnership with leaders of the communications sector to better assure the reliability, availability and resiliency of our networks. DHS NCC provides our industry with 24/7 on-site watch desk functions, helps coordinate the communications sector for preparedness and response to both physical and cyber events, and acts as the information exchange portal to government for us, and likewise as government's portal to the Communications Sector. The Comm-ISAC includes over 65 private sector companies that convene weekly, and on an as-needed basis, to share information about events and threats that have or could have adverse impacts on network service providers and their customers.

Second, aligned with NCC activities is the Network Security Information Exchange (NSIE) which meets every two months and is comprised of companies that support DHS's and the Communications Sector's national security mission.[4] During these sessions, analysts and security managers discuss threats and other issues that directly implicate the reliability, resiliency and integrity of the communications environment. Five of the largest domestic network service providers have representatives embedded within the NCC and are on-call to respond to government inquiries related to infrastructure-impacting events of either a cyber or physical nature. Since the NCC is one of three operational components along with US-CERT and the ICS-CERT on the National Cybersecurity and Communications Integration Center (NCCIC) floor, these same individuals are embedded within the NCCIC.

The NCCIC is a 24/7 cyber situational awareness, incident response, and management center and operates as the principal federal civilian interface for multi-directional and cross sector information sharing. Through the auspices of the NCCIC, and more broadly the DHS Office of Cybersecurity & Communications, communications sector companies currently work with the DHS Automated

[3] National Coordinating Center for Communications, Department of Homeland Security, https://www.dhs.gov/national-coordinating-center-communications.

[4] Network Security Information Exchanges, Department of Homeland Security, https://www.dhs.gov/sites/default/files/publications/NSTAC_08_0.pdf.

Information Sharing (AIS) portal using the STIX/TAXII protocols, which is designed to facilitate real-time sharing of cyber threat indicators.[5] Many of the largest providers are working through the AIS portal, as well as other related venues, to improve and increase the effectiveness and efficiency of automated sharing for more end users. Also under the NCCIC, member companies participate in the Cyber Information Sharing and Collaboration Program (CISCP) which provides a collaborative and trusted environment in which analysts from multiple sectors learn from each other to better understand and address emerging cybersecurity risks.[6]

Many more formal and informal venues and sharing mechanisms are described in the March 2017 report on Cybersecurity Information Sharing from the Federal Communications Commission's Communications Security, Reliability and Interoperability Council (CSRIC) Working Group 5 (CSRIC report).[7]. I now wish to touch on some significant findings in that report, as well as general observations about current information sharing venues and platforms.

First, as a practical matter and returning to the question of value that is the focus of this hearing, companies will participate in information sharing activities to the extent that they perceive the benefits outweigh, or at least match, the costs. Given the pressures on providers to ensure the confidentiality, integrity and availability of their communications networks and systems, any information sharing venue or mechanism that does not produce contextualized, timely, accurate and actionable information that improves providers' security posture will not meet that test of value.

More broadly, the CSRIC report found that a critical organizational challenge facing the communications sector is the wide variety of private, public, public-to-private, and international activities devoted to cyber threat information sharing.[8] Many organizations, especially smaller service providers, are unfamiliar with the breadth and depth of information sharing entities or lack the resources to commit to these enterprises. The rapid expansion of information sharing venues such as the Information Sharing and Analysis Organizations (ISAOs) called for under the 2015 Executive Order "Promoting Private Sector Cybersecurity

[5] Automated Indicator Sharing (AIS), Department of Homeland Security, https://www.us-cert.gov/ais.

[6] Cyber Information Sharing and Collaboration Program (CISCP), Department of Homeland Security, https://www.dhs.gov/ciscp.

[7] CSRIC Working Group 5 – Final Report, Federal Communications Commission, https://www.fcc.gov/files/csric5-wg5-finalreport031517pdf.

[8] *Id*. at 13.

Information Sharing" threatens to dilute resources and expertise through redundant or conflicting activities and objectives.[9]

For many of the larger service providers, the distribution of classified information from the federal government is an essential element of their overall risk management capabilities and this can impact the quality of information shared between private parties and within organizations. Having access to contextualized and actionable classified information is highly valuable. Similarly, not having access to such contextual information is detrimental to operations, but so is being unable to share some, or most, of the information with non-cleared colleagues. We continue to request classified information, when available, and we also ask that those pieces be downgraded as much as possible so that dissemination to the practitioners in the sector can take place quickly.

With respect to the DHS AIS portal, there is still important work that needs to be done to increase the value proposition for companies within our sector. Most of the concerns with AIS relate to the quality and usability of the information for the particular needs of an ISP and its enterprise. AIS is, and was intended to be, a platform for broad, cross-sector sharing that has resulted in information being downgraded or simplified to be appropriate for all participating entities. While the information distributed via AIS may be helpful to certain entities, the value proposition remains elusive for companies with more mature, sophisticated cybersecurity programs.

To make cyber threat information sharing more viable and valuable, we encourage the government to look across the various information sharing programs such as AIS and CISCP and analyze whether they are functioning as intended, meeting the needs of their target audiences and identify gaps that need to be filled. For example, the government needs to take the next step and determine whether there are more effective ways to share information with companies who have more mature programs, and specifically those who have been described as "ICT enablers"—i.e., the ICT companies that provide key services that enable the cyber ecosystem. Doing so will ultimately result in better and more timely information being shared.

I want to be clear that in highlighting current challenges we are working on with government, I do not mean to suggest that there is not currently valuable information sharing underway. A Comm-ISAC member receives more than one dozen alerts a day through the NCC from NCCIC, US-CERT, ICS-CERT, ISACs and joint law enforcement bulletins, and one company reports that it can trace the

[9] Executive Order – Promoting Private Sector Cybersecurity Information Sharing, The White House – President Barack Obama, https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.

addition of 2800 unique indicators in the past 10 months from the various DHS sources.

The good news is that DHS is aware of the current limitations and appears to be committed to a multi-year effort to enhance the automated machine-to-machine sharing capabilities. Our industry is committed to this program as evidenced by broad sector participation in a pilot managed by CTIA.[10] That program is about to be operationalized after testing new adaptations of the sharing platform to conform to communications sector operating environments.

Finally, I want to draw attention to the hundreds of smaller companies in our sector who face a different set of challenges due largely to their limited financial resources, technical skill-sets and operational priorities. These organizations are in most cases unable to devote scarce resources to time consuming efforts to filter numerous sources of threat intelligence, validate what is applicable, and then set implementation priorities. In many instances, they are unaware of information sharing venues, especially those venues that are operated by the private sector and accessed via exclusive invitation. While there are no easy solutions for these companies, trade associations like USTelecom and multiple other associations that comprise the CSCC are providing a critical link to information resources that can enhance their security posture.

Despite these and other challenges, and the risk of oversaturating the information sharing space with low-value activity, I do want to emphasize that without effective information sharing we have no hope of combatting emerging threats to our national and economic security. DHS is to be applauded for its ongoing efforts to engage industry and to increase the value of their information sharing programs. We remain committed to bringing all available industry resources to bear in this vital area, and I look forward to answering any of your questions.

[10] Protecting America's Wireless Networks, CTIA, https://www.ctia.org/docs/default-source/default-document-library/protecting-americas-wireless-networks.pdf at 9.