Testimony of Robert H. Mayer
Vice President of Industry and State Affairs
United States Telecom Association
before the
House Homeland Security Subcommittee on
Cybersecurity, Infrastructure Protection and Security Technologies
Oversight of the Cybersecurity Act of 2015
June 15, 2016

Chairman Ratcliffe, Ranking Member Richmond, and distinguished members of the Committee, thank you for giving the Communications Sector and me personally the opportunity to appear before you today for this important oversight hearing.

My name is Robert Mayer, and I serve as Vice President of Industry and State Affairs at the United States Telecom Association. USTelecom represents companies ranging from some of the smallest rural broadband providers to some of the largest companies in the U.S. economy. I am a past Chair and current Cybersecurity Committee Chair of the Communications Sector Coordinating Council (CSCC) which represents the Broadcasting, Cable, Satellite, Wireless and Wireline segments. 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.

Today, our nation faces unrelenting assaults from a variety of bad actors including, among others, nation-states, criminal enterprises, terror organizations and individual and group hackers. And as new interconnected platforms, technologies and applications grow exponentially, so does the attack surface expand placing every U.S. citizen and organization in harm's way. In this setting,

information sharing represents a fundamental building block in protecting the vital interests of all well-intended stakeholders in the cyber ecosystem.

The United States Congress and this Committee in particular are to be applauded for passing bipartisan legislation that now serves as a cornerstone in protecting our nation's economic and national security from the perils of a cyber-attack. The Cybersecurity Act of 2015 is a complex bill that represents a careful balance of interests across a broad spectrum of stakeholders.[1] The Act is founded on the voluntary sharing of information and provides authority for preventing, detecting, analyzing and mitigating cybersecurity threats and includes fundamental protections important to our industry including those related to privacy; exposure to regulation; state, tribal or local disclosure laws; and general legal liabilities.

On the privacy front, great care was taken to safeguard individuals from having their personal information shared with the government in a manner not directly related to specifically authorized activities associated with cyber threat indicators and defensive measures. Of great importance to our industry were the assurances that information shared with our government partners would not be directly used to regulate -- including enforcement actions -- lawful activity to monitor, operate defensive measures or share cyber threat indicators. Similarly,

[1] Cybersecurity Act of 2015 was passed as part of the Consolidated Appropriations Act, 2016, Pub. L. 114-113, 129 Stat. 2242 (available at https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf).

protections from Federal and State disclosure laws provide the appropriate balance between interests in transparency while not impeding vital information sharing.

Finally, by authorizing the EINSTEIN 3 Accelerated (E3A) and Enhanced Cybersecurity Service (ECS) programs, and eliminating statutory obstacles to their implementation, the Act took important steps to make the networks of federal civilian agencies, state governments, critical infrastructure providers and other entities safer, especially from advanced persistent threats.

Perhaps of greatest significance on the impact of future information sharing were the protections from liability incorporated into the Act. While there may remain some lingering questions in this area that are now the subject of further clarification, the lack of such protections was one of the most serious impediments to sharing information. The law establishes an appropriate standard by applying an exemption to liability protection only in such instances where there was a knowing sharing of personal information or information that identifies a specific person not directly related to a cybersecurity threat or where there exists evidence of gross negligence or willful misconduct in the course of conducting the authorized activities.

The Communications Sector has been actively engaged in information sharing operational and planning activities at DHS and elsewhere, both before and subsequent to the passage of the Act. Today at the operational level, over 50

private sector communications and information technology companies and 24 Federal Government agencies share critical communications information and advice in the DHS National Coordination Center (NCC) which also operates as the Communications Information Sharing and Analysis Center (ISAC) in accordance with a 2000 Presidential Directive.[2] In this trusted NCC/Comms ISAC environment, information on cyber vulnerabilities, threats, intrusion and anomalies is routinely exchanged among government and industry participants.[3]

Another noteworthy undertaking is this area involves activity in a newly-established Information Sharing Committee under the CSCC. This committee was created following the passage the Act to evaluate current information sharing activities and what the sector can do to support new and evolving initiatives. The Committee has identified a variety of mechanisms and venues for information sharing including those with trusted peers and commercial partners, government agencies under contract, law enforcement, industry peers as part of the sector policy and planning process, DHS via the National Cybersecurity and Communications Integration Center (NCCIC) and other affiliated organizations like US-CERT, other public and private partners and finally by ISPs for their own internal use to protect their networks and customers. The Committee is also

[2] Presidential Policy Directive 63, (available at http://fas.org/irp/offdocs/pdd/pdd-63.htm).
[3] *See*, DHS description of the NCC/Comms ISAC (available at www.dhs.gov/national-coordinating-center-communications).

planning to conduct a preliminary assessment of how the current, more narrowly circumscribed information sharing has been effectively and appropriately expanded as a consequence of the legislation adopted by Congress.

While the Act is only six months old, it is already evident that this new law is having an impact on both industry and government efforts to facilitate greater information sharing. We want to take this opportunity to acknowledge the significant and largely successful efforts by DHS to meet their aggressive implementation and guidance deadlines. Both DHS and the Department of Justice have been extremely forthcoming with respect to explaining and clarifying administrative, operational, technical and legal aspects associated with implementing information sharing mechanisms including those associated with a newly modified, Automated Information Sharing (AIS) capability.[4] While there are still some operational improvements needed to facilitate the efficient sharing of both automated and non-automated processes, and government guidelines remain to be finalized, there is clear evidence of a strong commitment on the part of industry and government to address any remaining barriers. Several major companies in our sector are already enrolled in the program and others are in the process of completing their initial evaluations.

[4] *See* DHS information on Automated Information Sharing Program (available athttps://www.dhs.gov/ais).

One note of concern that we would like to share with this Committee involves the implications of potential privacy rules that the FCC announced in their recent Notice of Proposed Rulemaking.[5] Under the Act, an entity can share information on a specific person if at the time of the sharing that entity did not knowingly reveal personal information unrelated to a cybersecurity threat.[6] Unlike the language in the Act that would allow for liability protection in such instances, the FCC proposal would grant the protection only when the sharing is shown to be "reasonably necessary."[7] This language creates ambiguity and uncertainty and is likely to spur reticence on the part of companies who could fear enforcement action based on an after-the-fact FCC determination of reasonableness. We will work hard to secure the appropriate clarity as we continue to engage the FCC in this rulemaking proceeding.

In closing, let me once again thank this Committee for their ongoing work to oversee the implementation of this landmark legislation. Given the magnitude of the threat and the promise of this legislation, periodic oversight by this committee will only bring us closer to making the cyber world much safer.

[5] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, Notice of Proposed Rulemaking, FCC 16-39 (rel. Apr. 1, 2016) (FCC NPRM).
[6] *See*, Cybersecurity Act of 2015 Section 104(d)(2)(A).
[7] *See*, FCC NPRM at para. 117.