October 20, 2016

Via cybercommission@nist.gov

Thomas E. Donilon
Commission Chair
Commission on Enhancing National Cybersecurity
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Samuel J. Palmisano
Commission Vice Chair
Commission on Enhancing National Cybersecurity
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Dear Chair Donilon and Vice Chair Palmisano:

Our organizations, which represent nearly every sector of the U.S. economy, write to express our support for the views that Secretary of Commerce Penny Pritzker voiced on September 27 at the U.S. Chamber of Commerce concerning cybersecurity policy.

Secretary Pritzker recognized the meaningful progress that industry and government have made together to strengthen the cybersecurity of the public and private sectors. A particularly noteworthy achievement, she remarked, is the joint industry-National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (the Framework), which our organizations promote widely and enthusiastically.

Our groups want to highlight three essential points in Secretary Pritzker's speech that we urge the Commission on Enhancing National Cybersecurity (the Commission) to consider as it develops its report for the next administration.

First, the Secretary stressed that public-private collaboration needs to be taken to a higher level. She said that cyberattacks cannot be handled solely by the U.S. government. Yet cyberspace is the "only domain where we ask private companies to defend themselves" against foreign powers and other significant threats. She wondered aloud, "Does that sound as crazy to you as it does to me?" Indeed, government does not stand between private entities and malicious hackers.

Second, the U.S. government has an obligation to protect its people and institutions against illicit actors that endanger our national and economic security. However, Secretary Pritzker noted that federal laws and regulations are unable to keep pace with rapidly evolving cyber threats. "No static checklist, no agency rule, no reactive regulation is capable of thwarting a threat we cannot foresee." A core problem, she observed, is that relationships between

businesses and regulators are "inherently adversarial," not collaborative, and this inhibits sound security.

Third, proactive discussions about a cyber incident should not lead to punitive blame-the-victim regulatory enforcement. Thus, policymakers need to change the value proposition for industry to engage voluntarily with government. To be sure, said Secretary Pritzker, many companies and agencies are jointly mitigating cyber risk by utilizing the Framework and exchanging cyber threat indicators. But, she added, "We need new laws to facilitate continuous, candid collaboration between industries and agencies—outside of the enforcement space."

Further, she expressed support for industry recommendations that push policymakers to create "reverse Miranda protections" that reflect industry input and support. In practical terms, one could anticipate businesses freely discussing cyberattacks in a safe setting without fearing that regulators would use the information against them with respect to liability, rulemakings, and public disclosure.

Our associations agree with Secretary Pritzker's view that cybersecurity requires a concerted team effort. Government officials should work with industry leaders, technical experts, and information security professionals to manage cyber risks and threats. Effective cybersecurity requires organizations to adapt to a constantly changing and menacing environment.

Also, overlapping government policies and sector-specific mandates can confuse industry actors regarding which agency leads on certain cybersecurity activities. Our organizations support greater clarity concerning the roles and responsibilities of the public and private sectors to strengthen partnerships.

It is worth saying that no single private entity, sector, or government institution can be expected to tackle the significantly larger, complex issues associated with the growing threats to U.S. cybersecurity. Government and industry must foster partnerships among interdependent actors that have much to gain by lessening potential cybersecurity crises.

We look forward to engaging the Commission and policymakers on the details of a workable solution that embodies Secretary Pritzker's proposal and industry's recommendations to bolster the security and resilience of U.S. industry.

Sincerely,

ACT | The App Association
Alliance of Automobile Manufacturers
American Cable Association (ACA)
American Chemistry Council (ACC)
American Fuel & Petrochemical Manufacturers (AFPM)
American Gas Association (AGA)
American Hotel & Lodging Association (AHLA)
American Petroleum Institute (API)

American Public Power Association (APPA)
ASIS International
Association of American Railroads (AAR)
Association of Global Automakers
College of Healthcare Information Management Executives (CHIME)
CompTIA
CTIA–Everything Wireless
Edison Electric Institute (EEI)
GridWise Alliance
HITRUST–Health Information Trust Alliance
ITI–Information Technology Industry Council
National Apartment Association
National Association of Manufacturers (NAM)
National Association of Mutual Insurance Companies (NAMIC)
National Association of Water Companies (NAWC)
National Multifamily Housing Council
National Rural Electric Cooperative Association (NRECA)
NCTA–The Internet & Television Association
Nuclear Energy Institute (NEI)
NTCA–The Rural Broadband Association
Property Casualty Insurers Association of America (PCI)
The Real Estate Roundtable
Retail Industry Leaders Association (RILA)
Security Industry Association
Software & Information Industry Association (SIIA)
TechNet
United States Telecom Association (USTelecom)
U.S. Chamber of Commerce