RILA
RETAIL INDUSTRY LEADERS ASSOCIATION
Educate. Collaborate. Advocate.

1700 North Moore Street, Suite 2250, Arlington, VA 22209

Via Electronic Filing

September 9, 2016

Thomas E. Donilon, Commission Chair
Commission on Enhancing National Cybersecurity
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Dear Chairman Donilon:

The Retail Industry Leaders Association (RILA) respectfully submits the following comments to the Commission on Enhancing National Cybersecurity regarding its request for information about the current and future states of cybersecurity in the digital economy. RILA appreciates the opportunity to provide the unique perspective of its members and looks forward to working in partnership with the federal government to help address the challenges of the digital age.

RILA is the trade association of the world's largest and most innovative retail companies. RILA members include more than 200 retailers, product manufacturers, and service suppliers, which together account for more than $1.5 trillion in annual sales, millions of American jobs and more than 100,000 stores, manufacturing facilities and distribution centers domestically and abroad.

Key Areas of Need

Retailers are deeply committed to addressing cybersecurity and believe the Commission should focus on 3 key areas of need:

1. Enabling a proactive federal government;
2. Creating a robust talent pipeline; and
3. Empowering a cyber savvy consumer.

(R)Tech Shaping the Digital Economy

The retail industry is being fundamentally disrupted by technology. This sea change ushers in a new era focused on the mobile, online, and in-store customer experience. The ubiquitous use of retail technology ((R)Tech) as the entry point and enabler for all retail experiences places information technology squarely at the center of the 21st century retail business model. Our business is no longer technology adjacent, (R)Tech is core to our business and to delivering delightful customer experiences.

To place customer experience through technology at the center of the retail business, retailers must keep faith with our customers and maintain a trusted relationship. Failing to understand and anticipate customer expectations about their data or failing to protect it

erodes the trust necessary to deliver the customer experience that is the currency of the retail realm.

Recent history has shown that no organization is immune from attack and no security system is invulnerable. This experience has served as a catalyst for our industry to reevaluate our approach to cybersecurity. While retail brands compete fiercely in the marketplace, there is a clear recognition that cybersecurity is truly a collaborative effort. The retail industry came together to create the Retail Cyber Intelligence Sharing Center (R-CISC)[1] in order to share threats and best practices to fight a fast iterating, sophisticated adversary. Retail brands of all sizes and sophistications are participating in the R-CISC and are actively sharing threat intelligence, learning best practices, and collaborating to protect their customers.

We highlight three areas where we believe Commission focus will deliver the largest return on investment in fighting a determined cyber adversary. We do not have all the answers, but view these comments as the beginning of a broader and deeper search for iterative solutions. They are offered in a spirit of collaboration with the goal of working in partnership to fight a problem spilling the lifeblood of the 21st century economy.

Enabling a Proactive Federal Government

Retailers believe the federal government has a vital role to play in cybersecurity. The private sector is facing an unprecedented scale and scope of attack. Government should play a leading role in protecting our economy from harm.

Retailers recognize the critical importance of working in partnership with the government to fight the adversary. One aspect of this partnership requires addressing information asymmetry. This is why retailers created the Retail Cyber Intelligence Sharing Center to enable industry-wide sharing of cyber threats. In addition, retailers welcomed the passage late last year of the Cybersecurity Information Sharing Act of 2015. As the law continues to be implemented, retailers will judge its success not only by the increase in threat indicators shared with the government, but also by the government's ability to enhance its own sharing with the private sector. Retailers support Commission recommendations that encourage government to more heavily weigh sharing with trusted partners over secrecy.

Retailers agree with the U.S. Chamber of Commerce's comment highlighting the good cybersecurity story of the public-private collaboration that produced the NIST Framework for Improving Critical Infrastructure Cybersecurity (Framework). The Framework was truly driven by private sector input and it therefore delivered an important risk management tool.

One reason the Framework has been so successful is that it fosters communication and engagement within companies, between companies, and across sectors. The Framework's name is a misnomer in that its tenets apply across all industries. This should be a lesson for the Commission. While a critical infrastructure designation is important to allocate limited resources, the government should look for opportunities to maximize impact by

[1] Retail Cyber Intelligence Sharing Center, https://r-cisc.org/.

making available services and resources that have already been created to protect critical infrastructure more broadly. The entire digital economy is under attack and maximizing the impact of existing programs to benefit everyone should be a touchstone for the Commission's recommendations.

Creating a Robust Talent Pipeline

Retail is hiring. But our sector, like others, is faced with the shortage of cybersecurity talent. The challenge for our sector is not only finding talent, but retaining it once we have invested in training. Retailers are strongly supportive of programs that emphasize STEM education as well as expanded access to computer science courses. We make no recommendations at this stage as to the solution, but believe it is important to add our voice to many others underscoring the critical need.

Empowering a Cyber Savvy Consumer

Retailers are deeply committed to our customers and to protecting their data. While retailers continue to make every effort to deploy technology and personnel to protect customer data, a cyber savvy customer is our best ally. Whether it is a login or password or some other method of authenticating identity, customers have a critical role to play in their own protection. Retailers recognize the importance of innovation and are augmenting customer adoption of multi-factor authentication with encryption and tokenization. Retailers applaud the President's BuySecure Initiative which resulted in the use of 2.5 million more chip and PIN cards. Retailers continue to believe this technology should be available to protect all customers.

Retailers recognize public-private partnerships are making strides to empower more consumers through awareness campaigns like STOP. THINK. CONNECT.[2] as well as through programs like the National Initiative for Cybersecurity Education (NICE) led by NIST. These public-private partnerships depend on a clear commitment from a variety of stakeholders as well as the government funding necessary to ensure the programs are viable. Retailers suggest the Commission should evaluate expanding the depth and breadth of that educational commitment.

RILA appreciates the opportunity to offer our views and assistance to the Commission. If you have any questions or would like to discuss retailer views in more detail, please do not hesitate to contact me at nicholas.ahrens@rila.org or 703-600-2065.

Sincerely,

Nicholas R. Ahrens

Nicholas R. Ahrens

Vice President, Privacy and Cybersecurity

---

[2] National Cybersecurity Alliance STOP. THINK. CONNECT. awareness program https://staysafeonline.org/stop-think-connect/