BlueCross BlueShield Association

1310 G Street, N.W.
Washington, D.C.
20005
202.626.4800

September 9, 2016

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

[SUBMITTED ELECTRONICALLY]

Re: Comments to the Request for Information on Current and Future States of Cybersecurity

Dear Chairman Donilon:

The Blue Cross Blue Shield Association (BCBSA) appreciates the opportunity to submit the following comments to the Request for Information (RFI) entitled "Information on the Current and Future States of Cybersecurity in the Digital Economy," published by the National Institute of Standards and Technology (NIST) in the Federal Register on Wednesday, August 10, 2016.

The Blue Cross Blue Shield Association is a national federation of 36 independent, community-based and locally operated Blue Cross and Blue Shield companies that collectively provide healthcare coverage for 107 million members – one in three Americans. The BCBSA system and private networks are an integral part of the nation's digital economy. In addition to touching 107 million individuals, the BCBSA system and private networks:

- Reach into every zip code;
- Represent $350+ billion in annual claims;
- Touch over 500,000 physicians, hospitals, labs, pharmacies, etc.; and
- Sit in between the 36 BCBS Plans and their data systems through our BlueCard, FEHBP, and MSP programs, serving as a critical hub in support of the financing of the nation's health care delivery system.

BCBSA believes that every private sector entity should do its part to address the ever-shifting and heightened cybersecurity risks that are impacting the entire economy. The BCBS System has put aggressive measures in place to combat cybersecurity threats. More than 300 security and privacy experts work across the BCBS System and collaborate in

monitoring and communications to share vulnerabilities and solutions to mitigate risk. Each BCBS company regularly inspects its security practices and makes adjustments based on the most current cyber intelligence available from threat intelligence services. As a requirement of licensure the BCBS System engaged a leading cybersecurity forensic firm to assess the data security of every BCBS company and to help assure customers, regulators and our own employees that cybersecurity-related threats are identified and addressed.

The BCBS System is also at the forefront in collaborating with government and industry to gain a clear picture of the cyber threats that we, and frankly every business, are facing. We continue to actively engage with best-in-class external experts in key areas to strengthen cyber intelligence and protection of our customers' information on several levels. These experts bring cyber intelligence and cybersecurity best practices from government, financial services and academia that directly inform our national and local security practices.

We have also strengthened our relationship with key areas of the Department of Justice—including the National Security Division, the Computer Crime and Intellectual Property Section, the FBI's cybercrimes unit and HHS's cybersecurity and critical infrastructure leadership teams—to gain a real-time and focused picture of the cyber threats we face.

As a result of this activity, BCBSA is well aware of the scope of commitment and resources necessary to maintain a high level of vigilance and capability to deal with the constant and unrelenting threats to information security for business in the digital economy. However there are financial, resource and system capability limits to what any individual business can and should be expected to accomplish without the support and assistance of national resources. This support is needed across the spectrum of technical assistance, regulatory relief and statutory change.

In order to achieve this broad spectrum of support, BCBSA offers the following considerations to the Commission on Enhancing Cybersecurity as it develops its detailed recommendations.

Strong Federal support for information sharing in the private sector must continue and be further enabled. A key element in improving our cyber defenses is information sharing. The Cybersecurity Information Sharing Act (CISA), federal guidance and Executive Orders have all combined to strengthen and expand sharing within our government and between governments and between government and the private sector. And from these activities we anticipate a better coordination of cyber intelligence sharing across the various government departments and to enable a free flow of intelligence between the private and public sector. But there remain concerns about legal liability and risk in information / intelligence sharing across business associates within any given industry that need to be addressed if the private sector is to be an equal partner with government in identifying and controlling cyber system intrusions.

Reward the efforts of private sector entities that have committed to implementing good cybersecurity policy and safeguards and who have taken the appropriate steps toward that goal. There needs to be Federal support for a hold harmless from litigation for companies who demonstrate adequate protections of their cyber infrastructure, for their customers, and with alliance partners. The administrative and legal defense burden involved in the assessment of penalties and the award of damages is massive and irrational, diverting resources from actual cyber threat mitigation activities.

Support consumer confidence in private sector cybersecurity by standardization of government breach notification policies that also accommodate private sector realities. Like other industries, the health care sector is not immune to overlapping and sometimes competing government jurisdiction protecting the consumers' interests in their personally identifiable information. As a result we and other health care entities find ourselves repeatedly in a positon of juggling the competing demands of multiple government entities regarding notifications of cyber security incidents and data breaches. These competing demands affect when, how, what they must contain and to whom these notifications may (or may not) go. Compliance not only creates administrative burdens on the affected entities, but the inconsistency in the notification processes from one incident to another only serves to undermine consumer confidence and understanding in any steps being taken to remediate an incident. Consideration must be given to establishing consistent and realistic breach notification provisions across government departments as required of the private sector entities they oversee.

Higher levels of government support for innovation in cyber threat solutions. It is a rubric if not a cliché to say that there is a constant battle between intruders' creativity in finding new technical means to compromise the security of an IT system and the system defenders' efforts to close off and thwart those means. Only the largest private sector entities can afford the test beds and other resources necessary to play on an equal footing with elements in the criminal world. And we in the private sector are all presumably outclassed when those cyber threat development efforts are conducted by foreign governments. Therefore it is imperative that our government champion pilots of new technology solutions that could serve to thwart unauthorized access to sensitive data, in our case Personally Identifiable Information (PII) and Personal Health Information (PHI) (e.g., cypher block chaining of PHI; self-healing operating infrastructure, bit-splitting technology, etc.).

Enable the certification of government-developed security frameworks. Confidence in the implementation of any cyber security framework (CSF) is supported by the capability to obtain an accepted certification of an entities' implementation of that CSF. While certification is currently available in the health care sector for the Health Information Trust Alliance (HITRUST) CSF and the ISO27000 there is not certification available for

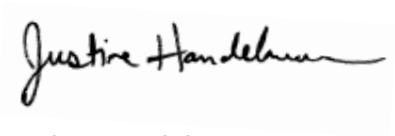
implementation of the NIST CSF. We are aware of interests in creating such a NIST certification and the government should be encouraged to take appropriate steps to enable that outcome.

Improve consumer confidence by achieving tangible crime prevention results. The public confidence is restored by more visible and active prosecution of disruptive cybercrime operatives.

Enable offensive measures by protective government sectors. The public perception is that our country is caught in the middle of cyber warfare. There is an expectation that we will soon have a more active, cyber-combat ready government entity in play, keeping us safe. An active "attack back" strategy should be developed and implementation authority granted to the appropriate government agency. We believe this is necessary to support the efforts of the nation's business community.

Again, BCBSA appreciates this opportunity to submit these comments for your consideration.

Sincerely,



Justine Handelman
Vice President, Legislative and Regulatory Policy