

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:

On behalf of the Healthcare Information and Management Systems Society ([HIMSS](#)), we are pleased to provide written comments regarding the request for information (RFI) on [Current and Future States of Cybersecurity in the Digital Economy](#), Docket Number: 160725650-6650-01, which was published in the Federal Register on August 10, 2016. HIMSS appreciates the opportunity to comment on this RFI, and we look forward to continuing our dialogue with the National Institute of Standards and Technology (NIST) on how health information technology (IT) can play a role in improving the cybersecurity infrastructure of our nation's healthcare sector.

HIMSS is a global, cause-based, not-for-profit organization focused on better health through information technology (IT). In North America, HIMSS focuses on health IT thought leadership, education, market research, and media services. Founded in 1961, HIMSS North America encompasses more than 64,000 individuals, of which more than two-thirds work in healthcare provider, governmental, and not-for-profit organizations, plus over 640 corporations and 450 not-for-profit partner organizations, that share this cause.

Included below are our comments on our relevant areas from this RFI:

Top Area Challenges and Approaches

Current and future trends and challenges

- A. **Healthcare is Vulnerable to Cyber Attacks.** Much like other sectors, and society as a whole, the healthcare sector uses technology extensively. Healthcare organizations, especially hospitals and other healthcare providers, are very reliant upon IT systems and networks. Unless addressed with appropriate controls and mechanisms, technology vulnerabilities inevitably follow. Healthcare organizations are vulnerable to cyber-attacks. Negligent and malicious insider activity are on the rise, as well as cyber-attacks from cybercriminals. Cybercriminals have various motivations, such as the disruption of or damage to critical infrastructure services, which may negatively impact the safety, health, and economic welfare of individuals and entities.
- B. **Greatest Cybersecurity Concern for the Healthcare Sector is Patient Safety.** A cyber-attack may result in serious harm or result in the death of a patient. Additionally, a cyber-

attack that cripples the IT infrastructure of a care provider may severely limit its ability to effectively care for its patients. For instance, providers victimized by ransomware may not be able to properly care for patients due to technology resources and data being unavailable, resulting in compromising patient safety.

- C. **Healthcare Organizations Still Need to Improve their Security Posture.** According to the [2016 HIMSS Cybersecurity Survey](#) report, respondents generally reported that their organizations do not have a strong ability to detect and protect IT infrastructure and data from such attacks. As reflected in the report, the technology to help safeguard data is available, but many healthcare organizations are not taking advantage of such technology (e.g., encryption, multi-factor authentication, intrusion detection systems, etc.). The chief barriers for mitigating cybersecurity risks include a lack of appropriate cybersecurity personnel and a lack of financial resources.
- D. **Aging and Outdated Technology Poses Risks to the Healthcare Sector.** Many organizations have to deal with aging, and potentially outdated, IT infrastructure, software applications, legacy devices and equipment, and old, unsupported operating systems. All of these factors lend themselves well to a reactive approach (and culture) to cybersecurity in the healthcare sector.
- E. **Too Many Vulnerabilities in Technology to Contend with.** Many organizations are often overwhelmed by the sheer numbers of vulnerabilities that are discovered and need to be addressed. Too many applications (in the form of a software program or an embedded program for a device) are designed without security in mind. As a result, much effort, time, and resources are spent updating, upgrading, or patching programs to address cybersecurity threats.
- F. **Third Parties Introduce Risk.** Healthcare organizations are reliant on third parties for their products and services, including procuring computer systems from a third party manufacturer or reseller; relying on a Software as a Service provider for web-based software (such as an Internet-accessible EHR application); and utilizing specific billing and administrative functions. Engaging third parties always introduces risk, since an outsider now has access to the client's data; third parties may not have security policies that align with the client's policies. The risk is further compounded when a hacker gains access to the client's data through that trusted third party.
- G. **Medical Device Security is a Challenge.** The "Internet of Things" has experienced explosive growth in recent years. Devices have transformed from traditional, stand-alone devices to devices with Internet connectivity. Risk that is inherent in connecting devices to the Internet is that the device (hypothetically) may be accessible to anyone, without appropriate controls. Additionally, security researchers are discovering significant vulnerabilities in these connected medical devices. Examples include hard-coded passwords, buffer overflows, and other significant flaws that can be easily exploited. The main concern providers have with unsecure medical devices is that a patient may suffer serious harm as a result of a medical device being exploited.
- H. **Too Much Malware Exists.** Malware has grown to epic proportions. Many malware strains are machine-generated—thus, thousands of new malware strains are generated each day. Additionally, ransomware and other types of malware have grown in sophistication with respect to credential stealing capabilities, detection avoidance tactics, and propagation techniques.

Progress being made to address the challenges

- A. **The Healthcare Sector is Experiencing Stunted Growth in Cybersecurity.** According to the [2016 HIMSS Cybersecurity Survey](#), most respondents reported improved network security and endpoint protection in the past year. Some respondents reported improved IT continuity and improved data loss prevention. In spite of these reported improvements, the statistics were essentially the same as those reported in the 2015 edition of the same survey.

What can or should be done now or within the next 1–2 years to better address the challenges

- A. **More Outreach to the Healthcare Sector regarding Federal Government Resources.** Healthcare organizations need to improve their baseline security. Many organizations still have a reactive stance towards cybersecurity. Healthcare organizations can improve their security posture by adopting and implementing a framework, such as the NIST Cybersecurity Framework. Additionally, many organizations may not be aware of the Framework or the Critical Infrastructure Cyber Community Voluntary Program (C³VP), which can assist healthcare organizations with implementing the Framework and improving their security baseline. Additional outreach to the healthcare sector is recommended so that more organizations are aware of the invaluable resources which the US Department of Homeland Security and NIST offer.
- B. **More Outreach to the Healthcare Sector on Cyber Threat Intelligence Sharing with ISACs and ISAOs.** Greater outreach to healthcare organizations is recommended about the benefits of participating in information sharing and analysis centers (ISACs) and information sharing and analysis organizations (ISAOs). Due to a lack of appropriately trained personnel, budget, and resources, small organizations and organizations with smaller IT budgets than-average are especially vulnerable. The importance of information sharing might be something that the new [Health Care Industry Cybersecurity Task Force](#) at the Department of Health and Human Services would be able to assist in.

What should be done over the next decade to better address the challenges

- A. **More Certified and Educated Cybersecurity Professionals are Needed for the Healthcare Sector.** Healthcare organizations have a shortage of qualified and experienced healthcare cybersecurity personnel. The state of healthcare cybersecurity can be vastly improved with the following: (1) more educated and qualified cybersecurity personnel (e.g., graduates of the National Security Agency's [Centers of Academic Excellence in Cybersecurity](#)) and professionals (such as the [CISSP](#), [HCISPP](#), and other credentials), and (2) encouraging innovation with an eye towards more technology-driven solutions for cybersecurity.

Future challenges that may arise and recommended actions that individuals, organizations, and governments can take to best position themselves today to meet those challenges.

- A. **Need for Secure Coding of Computer Programs and the Need for a More Secure Internet.** In addition to the foregoing, there are two sources of challenges in cybersecurity today: (1) the lack of securely coded computer programs, and (2) the insecurity of the Internet. Requiring developers to use secure coding could dramatically reduce the number of vulnerabilities, thereby improving overall Internet security from attack or breakage.

Additional Questions

Emerging technology trends and innovations; the effect these technology trends and innovations will have on the digital economy; and the effect these technology trends and innovations will have on cybersecurity.

- A. **The Future of the Digital Economy is Uncertain, Unless Cybersecurity is Made a Priority.** Historically, emerging technology trends and innovations have increased economic growth and business competition. To ensure such a trend continues for the digital economy, cybersecurity must be made a priority by innovators.
- B. **Harness Cybersecurity to Propel Forward Emerging Technology and Innovation.** In the healthcare sector, emerging technology trends and innovations are welcome and embraced. But, such emerging technology and innovations may not be embraced in the future if there are significant adverse risks that could happen (such as serious patient injury or even death). For example, a cyber-attack on a life-sustaining medical device could result in significant, adverse consequences for a patient. As a result, emerging technology and innovations need to be designed with security in mind. Otherwise, the associated risks may outweigh the benefits.

Government-private sector coordination and cooperation on cybersecurity.

- A. **Government-Private Sector Coordination and Cooperation on Cybersecurity Must be a Two-Way Street.** In order for government-private sector coordination and cooperation on cybersecurity to be most effective, the federal government must welcome and adopt a bilateral engagement to include receiving input from private sector sources and ensure a willingness to share meaningful information with the private sector. Additionally, the federal government should share with the private sector the necessary “know-how” to ensure that the information being shared can be consumed and used by the private sector.

The role(s) of the government in enhancing cybersecurity for the private sector.

- A. **More Outreach to the Healthcare Sector is Needed with Regard to Government Cybersecurity Resources.** In the healthcare sector, the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) can significantly improve

the security posture of our healthcare organizations' programs through greater outreach. While HIMSS is doing its utmost to educate health stakeholders, many healthcare organizations still do not know about the invaluable resources of DHS (such as C³VP) and the FBI. Additionally, many healthcare organizations do not know how to engage with DHS and FBI. A clear path needs to be created so that the private sector can engage more with the federal government on cybersecurity.

Despite the challenges and issues stated above, the private sector is proactively working to address cybersecurity with "all hands on deck." Healthcare providers, vendors, security researchers, and other stakeholders are all working together to improve the healthcare cybersecurity baseline for all constituents. For example, new cybersecurity solutions are being innovated and meaningful information is being shared about cyber threats and defending against them through the Health Care Industry Cybersecurity Task Force, the InfraGard Cyber Health Working Group, the National Health Information Sharing and Analysis Center, and other ISAOs in the healthcare sector.

It is also important to highlight and emphasize the work that HIMSS is undertaking in this area. At HIMSS, we have our HIMSS [Privacy and Security Toolkits](#) that provide informative, up-to-date information on healthcare privacy and cybersecurity subject matter. We give healthcare providers and other stakeholders the tools they need to keep information safe and secure in today's high tech world. We also are launching our HIMSS Cybersecurity Hub at the [HIMSS Innovation Center](#) which will provide valuable information on today's cybersecurity challenges and cutting-edge solutions. In addition, we also will have our [HIMSS Cybersecurity Command Center](#) at the [HIMSS17 Annual Conference](#), which will feature educational sessions, cybersecurity challenges, and vendors, showcasing our healthcare sector's expertise and know-how in combatting today's as well as tomorrow's cybersecurity threats.

Overall, HIMSS is committed to being a resource to NIST in its mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life as it relates to the healthcare sector.

We look forward to the opportunity to further discuss these issues with you in more depth. Please feel free to contact [Jeff Coughlin](#), Senior Director of Federal & State Affairs, at 703.562.8824, or [Eli Fleet](#), Director of Federal Affairs, at 703.562.8834, with questions or for more information.

Thank you for your consideration.

Sincerely,



Michael H. Zaroukian, MD, PhD, MACP, FHIMSS
Vice President & Chief Medical Information Officer
Sparrow Health System
Chair, HIMSS North America Board of Directors



H. Stephen Lieber, CAE
President & CEO
HIMSS