From: **Fleet, Eli**
Date: Mon, Apr 10, 2017 at 12:49 PM
Subject: HIMSS Response to NIST Cybersecurity Framework v 1.1
To: "cyberframework@nist.gov" <cyberframework@nist.gov>

On behalf of the Healthcare Information and Management Systems Society (HIMSS), we are pleased to provide written comments to the request for comment on the Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity, Document Number: 2017-01599, which was published in the Federal Register on January 25, 2017. HIMSS appreciates the opportunity to comment on this document 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.

Eli Fleet
Director, Federal Affairs
HIMSS North America

4300 Wilson Boulevard | Suite 250 | Arlington, VA 22203

HIMSS | HIMSS Analytics | HIMSS Media | PCHA
HIMSS Asia | HIMSS Europe | HIMSS Latin America | HIMSS Middle East | HIMSS UK

[Attachment Copied Below]

April 10, 2016

Kent Rochford, PhD, MBA
Acting Under Secretary of Commerce for Standards and Technology
and Acting Director, National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Dear Dr. Rochford:

On behalf of the Healthcare Information and Management Systems Society (HIMSS), we are pleased to provide written comments to the request for comment on the Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity, Document Number: 2017-01599, which was published in the Federal Register on January 25, 2017. HIMSS appreciates the opportunity to comment on this document 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 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 67,000 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.

HIMSS applauds NIST for the creation of this Draft Version 1.1 for the Framework for Improving Critical Infrastructure Cybersecurity (the "Framework"). The Framework is an excellent work product resulting from a robust public-private partnership. HIMSS has tracked the development of the Framework since its inception and advocates for healthcare organizations to adopt and implement it in our Cybersecurity Call to Action. Specifically, HIMSS supports the adoption of the Framework by healthcare organizations so that these organizations "adopt a voluntary, universal information privacy and security framework."

In light of this, HIMSS respectfully suggests several areas of improvement to enable healthcare organizations and others to improve their cybersecurity capabilities and reduce cybersecurity risk.

1. **Cyber Supply Chain Risk Management**

HIMSS supports NIST's inclusion of cyber supply chain risk management in the Framework. In terms of the highest implementation tier (Tier 4: Adaptive), it states:

"The organization can quickly and efficiently account for emerging cyber supply chain risks using real-time or near real-time information and leveraging an institutionalized knowledge of cyber supply chain risk….The organization communicates proactively and uses formal…and

informal mechanisms to develop and maintain strong relationships with its suppliers, partners, and individual and organizational buyers."

HIMSS suggests the addition of an explanatory text to emphasize the mission critical nature of cyber supply chain risk management (SCRM) as not all products and services are created with the same level of scrutiny toward cyber threats. For example, some computer hardware, mobile devices, and other types of computing devices have been sold with embedded malware. While the insertion of such malware may have been unintentional by the manufacturer, supplier, or vendor, the very fact that this has occurred highlights the dangers of insider threat (see, "Analog Malicious Hardware").

Furthermore, both care providers and public health leaders have great concerns with respect to the medical device supply chain, given the potentially significant risk to patient safety. Accordingly, HIMSS recommends that the Framework provide more granular detail on the "how" and "why" of SCRM, to include a relevant context of insider threat detection and management.

2. **Asset lifecycle and management**

HIMSS acknowledges that the Framework addresses "system lifecycle phases" (e.g., design, build, and deploy phases). However, we propose that it also address the lifecycle of assets (e.g., software, hardware, devices, equipment, etc.).

In the health sector, as in other sectors, it is not unusual to have aged and/or outdated assets (e.g., medical devices, industrial control systems, etc.). Especially in the case of legacy devices, the manufacturers/vendors may have discontinued support for these devices long ago. In the absence of sufficient compensating controls for these legacy devices, organizations may be presented with an unacceptable level of risk. Furthermore, in the health sector, many of these legacy devices may be life-sustaining devices and thus may pose a level of unacceptable risk to patients as well (e.g., serious injury or possibly death).

Accordingly, HIMSS suggests that the Framework address asset lifecycle and management including, with respect to an organization, keeping an inventory of its assets, the age of such assets, and the lifecycle of such assets.

3. **Measuring Framework Progress**

HIMSS suggests NIST utilize the next iteration of the Framework to explain how metrics and measures are used to assess progress with it (e.g., guidelines for using metrics and measures, use cases, etc.).

4. **Insider Threat Management**

As mentioned above in Section 1 (Cyber Supply Chain Risk Management), insider threat is a pervasive problem that all organizations are encountering. Whether insider threat is due to negligent or malicious insiders, the problem is real and any individual has the potential to

expose an organization to significant risk, depending upon his or her actions or inactions. Furthermore, insider attacks are usually much more common than external attacks.[1]

Insiders, whether malicious or negligent, often abuse or exceed their authorized access. For example, a negligent insider may deviate from an organization's security policy or procedure with a "work-around", which may lead to the inadvertent leakage of sensitive information. In another example, a malicious insider (e.g., a disgruntled employee) may plant a "logic bomb" which—upon the triggering of a certain event—may wipe out an organization's servers (or cause other damage).

An organization that only addresses external threats is not fully addressing cybersecurity risks. Therefore, HIMSS recommends NIST address insider threat management in its next iteration of the Framework.

5. **Holistic Cybersecurity**

HIMSS supports the notion of holistic cybersecurity by aligning people, processes, and technology to support sound cybersecurity procedures and policies. Yet, many organizations are struggling with their cybersecurity programs, due to a lack of alignment of these three elements. Oftentimes, cybersecurity is seen as a barrier, especially in the eyes of a non-cybersecurity professional. As an example, a significant challenge that many organizations face is the fact that many individuals work around security measures that are in place because these security measures are perceived to result in inefficient or complicated workflows. As we have outlined in our Cybersecurity Call to Action, HIMSS supports the notion of cybersecurity being "an enabler for the health sector, supporting both its business and clinical objectives and a facilitator of efficient, high quality patient care."

Cybersecurity can only be an "enabler" if the organization's cybersecurity procedures and policies support the mission and objectives of the organization. (This necessarily means that workforce members can efficiently and effectively perform their work functions without having to invent work-arounds.) In fact, organizations can gauge the effectiveness of their cybersecurity program by tracking how many work-arounds (or other violations) of security policy and procedures are happening, and track the number of requested exceptions to the security policy and procedures. If there is an unacceptable number of such violations, it may be time for the organization's leadership to re-evaluate or redesign its cybersecurity program.

Accordingly, HIMSS proposes that NIST update the next iteration of the Framework by addressing holistic cybersecurity as an enabler of the organization's mission and objectives in light of the foregoing considerations.

---

[1] According to the IBM X-Force Threat Intelligence Index 2017, the percentage of insider attacks for healthcare organizations is 71 percent compared with 29 percent of external attacks. The breakdown of insider attacks within healthcare is 46 percent for negligent actors and 25 percent for malicious actors. Further, both the IBM X-Force Threat Intelligence Index 2017 and the Verizon Data Breach Investigations Report 2016 report that the health sector is one of the top sectors for insider attacks.

6. **Awareness and Training**

HIMSS recommends that NIST update the next iteration of the Framework by stating that all of an organization's workforce members should participate in cybersecurity workforce training and awareness activities. If only cybersecurity personnel participate in such activities, a large number of the workforce remains untrained and hence the organization—as a whole—may still be very vulnerable. For instance, the untrained workers may be much more likely to fall for a phishing e-mail or other scam. Additionally, untrained workers may be more prone to utilizing work-arounds because they do not understand the potential consequences of their actions.

7. **Internal and External Information Sharing**

HIMSS supports the inclusion of external information sharing with other stakeholders to improve situational awareness and exchange of cyber threat intelligence information in the Framework.

In addition, we support the inclusion of internal information sharing. The cybersecurity capabilities of an organization do not just depend upon the technology. An organization can have the best technology in the world, but if it lacks a robust internal information sharing program, its ability to identify, detect, protect, respond, and recover will be hindered. As an example, a worker may hesitate to report a security incident (especially a significant security incident) due to worries about job security or other concerns. It may take days, weeks, or even months for management to become aware that such an incident occurred. An unaddressed, unmitigated security incident can potentially harm patients, and/or lead to significant damage to an organization (e.g., sizeable data breaches, loss of reputation and goodwill, downtime, etc.).

Accordingly, HIMSS suggests that NIST update the next iteration of the Framework by addressing internal information sharing, in addition to external information sharing, to ensure that organizations are addressing incidents in a timely and efficient manner.

8. **Implementation of Framework Tiers**

HIMSS proposes that NIST provide more granular guidance on how to implement the Framework tiers and, just as importantly, "how", "why", and "when" organizations should advance from one Framework tier to the next.

Conclusion

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.

HIMSS applauds NIST for its efforts in working collaboratively with the private sector to develop the Framework. And, HIMSS recommends additions to the Framework to enable users of the

Framework to better adopt and implement the Framework. In particular, our suggestions are based upon the HIMSS Cybersecurity Call to Action. We note that, while healthcare organizations are the focus of our response, our recommendations are equally applicable to other critical infrastructure sectors. Finally, HIMSS encourages NIST to continue to collaborate with the private sector in the future with respect to future enhancements to the Framework.

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, or Eli Fleet, Director of Federal Affairs, 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 &
Chief Transformation Officer
Sparrow Health System
Chair, HIMSS North America Board of Directors

H. Stephen Lieber, CAE
President & CEO
HIMSS