HIMSS
transforming health through information and technology™

33 West Monroe Street
Suite 1700
Chicago, IL 60603-5616 USA
Phone 312.664.HIMSS (664.4667)
Phone 312.664.6143
www.himss.org

January 19, 2018

Walter G. Copan, PhD
Under Secretary of Commerce for Standards and Technology and
Director, National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Dear Dr. Copan:

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 Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 Draft 2. 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 and technology can play a role in improving the cybersecurity infrastructure of our nation's healthcare sector.

HIMSS is a global voice, advisor, and thought leader of health transformation through health information and technology with a unique breadth and depth of expertise and capabilities to improve the quality, safety, and efficiency of health, healthcare, and care outcomes. HIMSS designs and leverages key data assets, predictive models and tools to advise global leaders, stakeholders, and influencers of best practices in health information and technology, so they have the right information at the point of decision.

HIMSS drives innovative, forward thinking around best uses of information and technology in support of better connected care, improved population health, and low cost of care. HIMSS is a not-for-profit, headquartered in Chicago, Illinois, with additional offices in North America, Europe, United Kingdom, and Asia.

Overall, HIMSS applauds Draft 2 of the NIST Cybersecurity Framework (the "Framework") and the NIST Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1. Improved cybersecurity practices, policies, and procedures are essential for all critical infrastructure owners and operators. HIMSS also applauds and supports the voluntary, non-proprietary nature of the Framework, as well as the universal applicability of the Framework (whether in the United States or beyond).

In the fall of 2016, the HIMSS North America Board of Directors approved the Cybersecurity Call to Action and since that time, HIMSS has been advocating for the adoption of holistic security measures. Accordingly, HIMSS supports NIST's inclusion of holistic security principles throughout the Framework—including the alignment of cybersecurity risk management with the business context and resources that support critical functions. Our Call to Action also advocates for adoption and use of the Framework, as well as fostering the growth of the healthcare cybersecurity workforce.

In the Implementation Tiers section of the Framework (section 2.2), HIMSS encourages NIST to include more guidance to elucidate when an organization can (or should) move from one tier to another. Certainly, in the healthcare sector—and other critical infrastructure sectors—having only a reactive security posture is detrimental for any organization. As such, not having formal policies and procedures and addressing matters "ad hoc" can lead to inconsistently applied security policies and procedures. Having these such gaps can lead to significant (and perhaps exploitable) vulnerabilities.

Given the complexity of cybersecurity, the threat landscape, and our dependence (and interdependence) on information technology and operational technology (OT) assets likely means that the implementation tiers should be analyzed further. Cybersecurity defense (and offense) are now multi-dimensional endeavors and the complexity of deploying cybersecurity within any given organization, a "flat" declaration that one has implemented "Tier 2" across his or her organization, for example, may no longer be accurate. Instead, a multi-dimensional analysis and characterization may be more appropriate. For example, a given organization could potentially be a blend of Tier 1, 2, 3, and 4, given that an organization may be a "Tier 1" in certain respects, but "Tier 3" in another. Organizations could benefit from assessing and tracking their implementation tiers with a numerical score (or other scheme), wherein certain aspects are scored for "Tier 1" and others are scored for "Tier 2", etc.

HIMSS recommends that the Framework should address in more detail how to assess and manage risk concerning information technology and OT assets. Whether in healthcare or other critical infrastructure sectors, information technology assets are generally secured better than OT assets. Furthermore, since a compromise of OT assets may have cyber-physical consequences, it is all the more critical that organizations do a better job protecting OT assets (and manufacturers do a better job at designing more secure devices).

In the realm of healthcare, the vast majority of devices are "connected" and thus part of the Internet of Medical Things (IoMT). The compromise of an IoMT device may have serious adverse consequences. For example, a fatal bolus of insulin may be delivered to a patient (via a wireless infusion pump). These are nightmarish scenarios that we all want to avoid and hope never transpire. HIMSS strongly recommends that we need guidance to assist owners and operators of critical infrastructure—including (but not limited to) in healthcare. The healthcare sector has numerous dependencies upon other critical infrastructure sectors—and, indeed, healthcare touches everyone and virtually everything.

In light of these dependencies, HIMSS supports the inclusion of supply-chain risk management (SCRM) in the Framework. Given the global NotPetya incident in 2017, our healthcare sector (and other critical infrastructure sectors) are acutely aware of the importance of supply chain integrity and security. The issue of SCRM is so important, however, that HIMSS recommends that the Framework could benefit from additional guidance on this subject.

Finally, HIMSS recommends that the Framework should be aligned with the National Infrastructure Protection Plan (NIPP) and the National Cyber Incident Response Plan (NCIRP). If anything, the recent NotPetya and WannaCry cyber incidents signaled a need for coordinated guidance. In essence, we need more unity, coordination, and information sharing and less fragmentation. The community needs to advance the state of cybersecurity together—and not foster uncertainty and silos.

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,

Denise W. Hines, DHA, PMP, FHIMSS
CEO
eHealth Services Group
Chair, North America Board of Directors

Michael H. Zaroukian, MD, PhD, MACP, FHIMSS
Vice President & CMIO
Sparrow Health System
Chair, HIMSS Board of Directors

Harold F. Wolf III
President & CEO
HIMSS