American Hospital Association

800 10th Street, NW
Two CityCenter, Suite 400
Washington, DC 20001-4956
(202) 638-1100 Phone
www.aha.org

February 9, 2016

Submitted Electronically

Richard R. Cavanaugh
Acting Associate Director for Laboratory Programs
Director of the Special Programs Office
National Institute of Science and Technology

Re: Views on the Framework for Improving Critical Infrastructure Cybersecurity

Dear Dr. Cavanaugh:

On behalf of our nearly 5,000 member hospitals, health systems and other health care organizations, and our 43,000 individual members, the American Hospital Association (AHA) appreciates the opportunity to reply to the request for information on the National Institute of Science and Technology's (NIST) Cybersecurity Framework published in the *Federal Register* on Dec. 11, 2015. As an important component of the Healthcare and Public Health Critical Infrastructure Sector, hospitals and health systems take seriously their responsibility to protect their information and other networked systems from unauthorized access and malicious attacks.

T**he AHA applauds NIST for engaging the private sector in an open and consultative process to develop the Framework, and for ensuring that tools and resources are available in the public domain. The Framework has become an important reference point for owners and operators of critical infrastructure. However, challenges remain in making information and resources actionable at the front lines of health care. Moving forward, we believe that the Framework should continue to be in the public domain, with no cost or other barriers to its use.**

THE FRAMEWORK IS A USEFUL ORGANIZING TOOL

Health care is increasingly connected. This growth in inter-connected systems, while bringing tremendous efficiencies and innovations, also introduces new types of vulnerability for inappropriate access to private information, and even criminal activity that can put individuals and institutions at risk. For example, billing systems use electronic transfers, medical devices upload vital statistics in real time to electronic health records (EHRs), hospitals allow patients and visitors access to hospital WiFi as a courtesy, and patients are being provided access to protected health information (PHI) via authentication on the Internet.

The NIST-developed Framework supports hospitals' efforts to protect their information systems by providing a helpful, high-level structure for individual organizations to think about and address cybersecurity risk. Specifically, it identifies five core functions– identify, protect, detect, respond, recover – that must be part of a risk-based approach to manage cyber risk, with specific categories of activity under each (such as asset management or access control). It then goes on to identify existing guidelines and technical standards that support the individual recommended functions, and offers a set of tiers to gauge performance. The AHA continues to share resources with hospital leaders to emphasize the importance of cybersecurity, including information about the NIST Framework and other tools.

SUGGESTIONS TO IMPROVE THE FRAMEWORK

Hospitals use many tools to address cybersecurity threats, including the Framework. While the guidance provided in the Framework is useful, some additional resources would be helpful. For example, for many smaller health care providers, tools that are more actionable and concrete in offering guidance scaled to that setting would be useful. For those using the Framework to gauge performance, more guidance on how to get from one tier to the next would be helpful. Similarly, greater transparency on the meaning of the tiers would allow those using the Framework to better understand the level of protection that can be expected at each tier. Finally, case studies and profiles of those who have made effective use of the Framework would be a tremendous resource to others. It is also crucial that the Framework be kept up to date.

POTENTIAL CONFLICTS WITH OTHER REGULATORY PROCESSES

In developing specific standards, NIST and others in the federal government must be aware of the existing privacy rules specific to health care, specifically the requirements in the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 to protect the security of patients' health information held in electronic form. The Cybersecurity Framework must be cross-walked to these specific requirements, particularly the requirements of the security rule issued under HIPAA and HITECH. While cybersecurity involves much more than protecting patients' medical information under HIPAA and extends to financial, personnel and other networked systems, a health care organization's activities related to PHI offer an important foundational base for comprehensive efforts to address the broader organizational risks related to cybersecurity.

Consideration of how the HIPAA and HITECH requirements map to the tools in the Framework ensures that contradictory and duplicative requirements are avoided and synergies are created. This work will be advanced by Sec. 405 of the Cybersecurity Act of 2015, which explicitly tasks the Department of Health and Human Services to work with the private sector and other federal agencies to establish voluntary, consensus-based best practices for reducing cybersecurity risk in health care that align with both the Framework and the HIPAA Security Rule. The AHA looks forward to collaborating with the Department of Health and Human Services and NIST on that endeavor.

CYBERSECURITY TOOLS ARE A PUBLIC GOOD

The request for information asks for input on the private sector's involvement in the future governance of the Framework, including whether NIST should consider transitioning some or all of the Framework's coordination to another organization. Because our critical infrastructure serves the entire nation, and due to the interconnectedness of critical infrastructure sectors, the AHA believes that there is significant value in keeping the Framework's cybersecurity tools in the public sector. These resources allow for the development of common approaches across sectors, which is particularly important to the health care field, as it is reliant on many other sectors, including communications, water, transportation and power, to name a few. In addition, having resources in the public sector levels the playing field by allowing access for all without cost barriers. Cost barriers can come both in the form of access fees and concerns over licensing issues as specific tools are adopted and repurposed. Therefore, as NIST considers future governance models, we urge you to maintain the Framework in the public domain, with no cost or other barriers to access and use its tools and resources.

Thank you for the opportunity to share our concerns and comments. If you have any questions, please contact Chantal Worzala, vice president of health information and policy operations, at cworzala@aha.org or Lawrence Hughes, assistant general counsel, at lhughes@aha.org.

Sincerely,

/s/

Ashley Thompson
Senior Vice President
Public Policy Analysis and Development