American Hospital Association

Liberty Place, Suite 700
325 Seventh Street, NW
Washington, DC 20004-2802
(202) 638-1100 Phone
www.aha.org

Submitted Electronically

December 11, 2013

Patrick Gallagher, Ph.D.
Under Secretary of Commerce for Standards and Technology
U.S. Department of Commerce
1401 Constitution Avenue, NW
Washington, DC 20227

Re: Request for Comments on the Preliminary Cybersecurity Framework

Dear Dr. Gallagher:

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 comment on the Preliminary Cybersecurity Framework published in the Oct. 29 *Federal Register*.

Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," directed the National Institute of Standards and Technology (NIST) to develop the framework to "reduce cyber risk and help owners and operators of critical infrastructure identify, assess, and manage that risk." Hospitals are included in the Healthcare and Public Health Critical Infrastructure Sector, one of 18 identified in the executive order. Under the order, the framework is voluntary for the private sector, although it is mandatory for federal agencies. However, the executive order contemplates the use of incentives for private sector owners and operators of critical infrastructure to encourage their adoption of the framework.

The AHA applauds NIST for broadly engaging the private sector in an open and consultative process that provided multiple opportunities for input and feedback on the preliminary framework. We believe that the final framework, once released, will serve as an important reference point for all owners and operators of critical infrastructure. However, we urge that it remain flexible and strictly voluntary for the private sector, given the variability both across and within sectors.

In addition, we recommend that:

- **The final framework consider how the different critical infrastructure sectors might reconcile disparate cybersecurity implementation standards;**
- **The federal government acknowledge that it will take time for changes to be accomplished across the large number and variety of actors in health care sector and allow sufficient time for the important sector-specific definitions, tools and processes to be developed and implemented appropriately; and**
- **A detailed cross-walk to the *Health Insurance Portability and Accountability Act* (HIPAA) and *Health Information Technology for Economic and Clinical Health Act* (HITECH) requirements must be included directly in the final framework.**

THE FRAMEWORK IS A USEFUL ORGANIZING TOOL

The AHA agrees with the framework's central tenet that an ongoing risk management approach to cybersecurity is the most appropriate, given the dynamic nature of information systems and the rapid pace of change. Health care delivery is an increasingly connected enterprise, and hospitals take seriously their responsibility to protect their information systems from unauthorized access and malicious attacks. While bringing tremendous efficiencies and innovations, interconnected information technology 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, hospitals allow patients and visitors access to hospital WiFi as a courtesy, and patients are being provided access to protected health information via authentication on the Internet.

The preliminary cybersecurity framework supports hospitals' efforts to protect their information systems by providing a helpful, high-level structure for individual organizations to consider when addressing cybersecurity risk. Specifically, it identifies five core functions– identify, protect, detect, respond, recover – that must be part of a risk-based approach to manage cybersecurity, with specific categories of activity under each (such as asset management or access control). It then identifies existing guidelines and technical standards that support the individual recommended functions.

Given that there are 18 diverse sectors that are considered to be critical infrastructure, the high-level approach used in the framework is appropriate. The "layered" format allows organizational leaders to focus on a process for risk management, while technical professionals can drill down into specific standards and other resources. However, we recommend that NIST also consider some of the potential cross-sector interactions that occur. For example, a hospital cannot run without power or water, and is reliant on the communications sector to be a first line of defense against cyber attacks. Similarly, the emergency services critical infrastructure sector cannot successfully respond to an incident without access to hospital emergency rooms. Accordingly, we recommend the final framework include not only voluntary standards for each critical infrastructure sector, but also considerations for how the sectors might reconcile disparate cybersecurity implementation standards.

While organizational leaders will not have the technical skills to implement specific protections, they must incorporate cybersecurity into their overall risk management approach. To that end, the AHA continues to educate hospital leaders on the importance of cybersecurity. We have, for example, developed a primer directed specifically at hospital leaders urging them to incorporate cybersecurity into the organization's overall risk management and reduction strategy, launched a new webpage with cybersecurity materials, and scheduled a webinar series about cybersecurity issues.

SECTOR-SPECIFIC WORK WILL BE NEEDED

As cybersecurity awareness builds, there will be a clear need for sector-specific definitions, tools and processes that include best practice sharing and more specific help than the framework provides. The AHA is collaborating with the departments of Homeland Security and Health and Human Services in their public-private collaborations, including the Healthcare and Public Health Sector Coordinating Council, to work through health sector specific issues. The AHA also will work with other organizations within the health sector.

A key priority for the collaboration should be leveraging existing tools before building new ones, and ensuring that all health care entities have access to solid guidance. It will take public and private sector actions to achieve the crucial goals of Executive Order 13636: "to enhance the security and resilience of the nation's critical infrastructure and to maintain a cyber-environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties." Furthermore, we urge the federal government to acknowledge that it will take time for changes to be accomplished across the large number and variety of actors in health care.

ADOPTION OF THE FRAMEWORK SHOULD REMAIN VOLUNTARY

The AHA appreciates the urgency associated with building cybersecurity capacity and is engaged in building awareness of and a commitment to address cybersecurity issues among hospital leaders. However, we strongly believe that adoption of the framework must remain voluntary for private sector entities. We caution against a rapid move toward adoption of incentives that would essentially mandate adoption, particularly in the highly regulated health care space. We encourage the federal government to ensure a thorough dialogue with the health sector before any specific incentives are adopted. Further, we recommend that only positive incentives be contemplated, such as reduced premiums for cybersecurity insurance among those who have adopted the framework.

We are concerned that mandatory compliance against a checklist of items would go against the nature of a risk-based approach that can be responsive to a changing environment. It also could create an onerous, compliance-oriented approach to cybersecurity, rather than encouraging achievement of broader goals. Furthermore, a punitive approach could have unintended consequences, such as denying resources to organizations that are struggling to keep up, undermining their ability to put a solid cybersecurity program in place.

DIVERSITY WITHIN AND ACROSS CRITICAL INFRASTRUCTURE SECTORS NECESSITATES A FLEXIBLE APPROACH

The flexible approach taken by the framework is appropriate given the diverse institutions that are part of the nation's critical infrastructure. The hospital field alone can range from very large academic medical centers to small rural hospitals with fewer than 25 beds. The resources available to this wide range of organizations vary, as does the scope of their networked environments, their current level of connectivity, and the level of risk from exposure to the Internet. In addition, different health care entities may have unique circumstances that affect their cyber risks, such as size, location and the specific services provided. Indeed, even within a single health care organization, such as a hospital, diverse components may have different risk profiles. For example, the lobby gift shop generally is not connected to the organization's information systems that contain and communicate sensitive patient data. Accordingly, the flexible approach used in the draft framework should be preserved in the final version.

For health care organizations, patient care is the primary objective. Hospitals and health systems are on a path toward increasing information sharing in support of better and more efficient care. Therefore, the Healthcare and Public Health Sector by necessity may have more critical system access points than other infrastructure sectors. For example, medical device companies, physician offices, insurers and individual patients may all interact with a hospital's information systems. Therefore, it will be necessary for the health care sector itself to work to better define the entities and individuals who are part of the health care critical infrastructure. The NIST preliminary framework could help facilitate that important work if it explicitly acknowledged that a critical infrastructure entity, such as a hospital, must have the cooperation of all other entities that interact with its information system. These outside organizations also must engage in cybersecurity risk assessment and reduction activities. In the case of hospitals, for example, it will be important for the controls presented in the framework to flow down to medical device and IT vendors that create products that are attached to or integrated into a hospital's network. These subsidiary actors also will need to implement appropriate access controls, logging systems and vulnerability remediation tools.

THE FRAMEWORK SHOULD REFERENCE EXISTING INFORMATION SECURITY RULES APPLICABLE TO HEALTH CARE ORGANIZATIONS

In developing specific standards, NIST and others must be aware of the existing privacy rules specific to health care, especially the HIPAA and the more recent HITECH requirements, which include specific rules to protect the security of patients' health information held in electronic form. That means the cybersecurity framework must be cross-walked to the specific requirements of the security rule issued under these laws. Cybersecurity involves much more than protecting patients' medical information under HIPAA and extends to all financial, personnel and other networked systems. Nevertheless, a health care organization's activities related to personal health information serve as a foundation to manage broader organizational risks related to cybersecurity. Inclusion of a detailed cross-walk to the HIPAA and HITECH requirements directly in the framework would ensure that contradictory and duplicative requirements are avoided.

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

Sincerely,

/s/

Linda E. Fishman
Senior Vice President, Public Policy Analysis and Development

cc: Nicole Lurie, M.D., M.S.P.H., Assistant Secretary for Preparedness and Response (ASPR)
RADM, U.S. Public Health Service
U.S. Department of Health and Human Services

Phyllis Schneck, Deputy Under Secretary for Cybersecurity
U. S. Department of Homeland Security

Leon Rodriguez, Director
Office for Civil Rights
U.S. Department of Health and Human Services

Jacob Reider, M.D.
Acting National Coordinator for Health Information Technology
Office of the National Coordinator for Health Information Technology
U.S. Department of Health and Human Services