

October 10, 2014

Dr. Willie E. May
Acting Director
National Institute of Standards and Technology
Department of Commerce
100 Bureau Drive
Gaithersburg, MD 20899

Dear Dr. May,

On behalf of the Healthcare Information and Management Systems Society ([HIMSS](http://www.himss.org)), we are pleased to provide written comments to the National Institute of Standards and Technology (NIST) in response to the request for information (RFI), "[Experience with the Framework for Improving Critical Infrastructure Cybersecurity](#)," published in the Federal Register on August 26, 2014.

HIMSS is a cause-based, global enterprise producing health IT thought leadership, education, events, market research and media services around the world. Founded in 1961, HIMSS encompasses more than 57,000 individuals, of which more than two-thirds work in healthcare provider, governmental and not-for-profit organizations, plus over 640 corporations and over 400 not-for-profit partner organizations that share this cause.

HIMSS welcomes the opportunity to contribute to this dialogue, and outlines our answers below to the questions posed in the RFI.

Current Awareness of the Cybersecurity Framework

- *What is the extent of awareness of the Framework among the Nation's critical infrastructure organizations? Six months after the Framework was issued, has it gained the traction needed to be a factor in how organizations manage cyber risks in the Nation's critical infrastructure?*

In regards to the healthcare sector, HIMSS estimates that there is modest awareness about the Framework. There are a few organizations that have implemented the Framework; we note that our estimate is anecdotally based, and likely to be very small.

- *How have organizations learned about the Framework? Outreach from NIST or another government agency, an association, participation in a NIST workshop, news media? Other source?*

HIMSS observes that the modest awareness among healthcare organizations appears to have been generated through communications at the workplace, HIMSS and other professional organizations, federal announcements and newsletters, but not necessarily from the media or other mainstream publications.

- *Are critical infrastructure owners and operators working with sector-specific groups, non-profits, and other organizations that support critical infrastructure to receive information and share lessons learned about the Framework?*

HIMSS has monitored development of the Framework; we've shared its progress with our stakeholders. In addition, we've submitted [comments](#) on the discussion draft with expert input from our HIMSS Privacy and Security Committee, including the following observations:

- 1) To strengthen cybersecurity and support business objectives of healthcare organizations, we recommend that privacy and security be integrated into the organization's business objectives;
- 2) To strengthen cybersecurity, we suggest that organizations increase their resilience to cyber incidents by utilizing lessons learned as part of their short-term and long-term recovery efforts.
- 3) To better handle incidents, we suggest that healthcare organizations have an incident response plan in place which focuses on handling cyber incidents in terms of the roles and actions of people, processes, and technology within the healthcare organization.^[1]

We acknowledge and appreciate that NIST has incorporated HIMSS's comments into Version 1.0 of the Framework.

- *Is there general awareness that the Framework:*
 - a. Is intended for voluntary use?*
 - b. Is intended as a cyber risk management tool for all levels of an organization in assessing risk and how cybersecurity factors into risk assessments?*

a. Yes. For those organizations aware of the Framework, they understand the Framework is intended for voluntary use. However, further education and information-sharing is necessary to alleviate concerns that the Framework is being mandated by regulation or law.

b. Yes, we believe it is generally understood that the Framework is intended as a cyber risk management tool for all levels of an organization in assessing risk. We also note that the Framework makes clear how cybersecurity factors into risk assessments. However, we suggest that NIST consider publishing guidance on adoption and use of the Framework, tailored to the type and size of the organization, as we believe such guidance may be helpful.

- *What are the greatest challenges and opportunities—for NIST, the Federal government more broadly, and the private sector—to improve awareness of the Framework?*

NIST could improve the field's awareness of the Framework by providing a means for healthcare organizations – those that have adopted and implemented the Framework – to discuss use of the Framework to their advantage to manage risk. Input could be sought from small, medium, and large healthcare organizations in both urban and rural settings.

^[1] HIMSS' Response to NIST Preliminary version of the Cybersecurity Framework; December 2013. http://csrc.nist.gov/cyberframework/framework_comments/20131213_thomas_leary_himss_part2.pdf

- *Is your organization doing any form of outreach or education on cybersecurity risk management (including the Framework)? If so, what kind of outreach and how many entities are you reaching? If not, does your organization plan to do any form of outreach or awareness on the Framework?*

HIMSS utilizes a variety of outreach and educational initiatives to inform and educate our stakeholders. We also participate with other non-profit organizations representing critical infrastructure sectors, in an information sharing initiative to discuss the Framework. We work with our stakeholders through HIMSS's volunteer-led Privacy and Security Committee, and associated Task Forces and Work Groups to build educational deliverables relating to [risk management](#), through [blog posts](#) and [privacy and security toolkits](#), which are all available on our [website](#). HIMSS also has year-round educational initiatives and deliverables relating to risk management, including the biannual [Privacy and Security Forum](#), and the [mHealth Summit Mobile Privacy and Security Symposium](#).

Finally, as appropriate, HIMSS connects with government agencies to provide education and information relating to risk management.

- *What more can and should be done to raise awareness?*

We suggest that NIST widely present the Framework at health sector-oriented conferences. Another suggestion is NIST create a repository of information in which organizations across the various critical infrastructure sectors can contribute information, comments, and feedback relevant to experiences, lessons learned, and best practices with respect to adoption and use of the Framework.

Experiences with the Cybersecurity Framework

- *Do organizations in some sectors require some type of sector specific guidance prior to use?*

Yes, we have observed that the health sector has become acutely aware of cyber attacks, insider threats, and other malicious activity. However, traditionally, healthcare's focus has been on HIPAA compliance. Compliance, though, does not necessarily mean that information will be kept safe and secure. Accordingly, healthcare providers, other covered entities, and the business associates that do work on behalf of these covered entities, all need practical and detailed guidance on making the transition from "compliance only" to being secure (in the same sense that other critical infrastructure sectors, such as the chemical, electrical, and financial sectors have adopted and embraced security).

The healthcare industry also could benefit from specific guidance from NIST (with input from healthcare stakeholders) on what an ideal "target state" would be for a healthcare organization. Stakeholders would also benefit from a common, industry-wide understanding and agreement of what the target state should be as well as standard metrics/tools to measure current state and progress made by a healthcare organization towards that target state. Both privacy risk management and information security risk management should be addressed (as well as the points of intersection and other points of connection between these two spheres). The target state and standard metrics/tools are not provided by HIPAA, the HITECH Act, or other associated or related guidance.

- *Which activities by NIST, the Department of Commerce overall (including the Patent and Trademark Office (PTO); National Telecommunications and Information Administration (NTIA); and the Internet Policy Taskforce (IPTF)) or other departments and agencies could be expanded or initiated to promote implementation of the Framework?*

The National Initiative for Cybersecurity Education (NICE) could be used to promote better awareness and more specific guidance with regard to the Framework.

For example, the PTO could assist with the Framework by ensuring that the quality of patent review and patent application review remains high with respect to patents and patent applications relating to risk management and cybersecurity, in addition to other related arts.

Roadmap for the Future of the Cybersecurity Framework

- *Are key cybersecurity issues and opportunities missing that should be considered as priorities, and if so, what are they and why do they merit special attention?*

The Framework could explain in detail what constitutes an accurate, thorough, and holistic risk assessment. As we are in an age where much information is electronic and, if information is not secure, it very well may not be private. The Framework could explain in detail how privacy and cybersecurity interrelate.

Consideration should also be given to our global economy and global interdependencies and the need to manage risk on a global scale, with the understanding that entities can and do interact across critical infrastructure sectors. The interdependence among the critical infrastructure sectors can result in shared threats and vulnerabilities. This approach would truly be managing risk in the real world, as opposed to managing risk in a vacuum.

We suggest that NIST (with input from healthcare stakeholders) bring together government, academia, and industry to develop a Framework which is fluid and flexible enough to be a living document which can be improved and revamped to ensure that the Framework content reflects real world risks and risk management, including in view of interdependencies among the critical infrastructure sectors.

According to the [6th Annual HIMSS Security Survey](#)¹, released February 19, 2014, more than half of the survey's respondents (51%) have increased their security budgets in the past year. However, 49% of these organizations are still spending 3% or less of their overall IT budget on security initiatives that will secure patient data—the industry average is [cited](#) as 5% of the total IT budget on security. Information security in the health sector is generally underfunded. In spite of this, more healthcare stakeholders are strengthening their information security programs (or are interested in do so, but need additional guidance), in light of recent breaches and cyber attacks. To the extent that other critical infrastructure sectors have applied the Framework to address breaches and cyber attacks, these lessons learned may be of interest to HIMSS and its healthcare stakeholders.

¹ HIMSS Security Survey; February 2014: http://www.himss.org/files/2013_HIMSS_Security_Survey.pdf

HIMSS appreciates the opportunity to submit comments on this RFI—this framework presents an opportunity for HIMSS to work with NIST to further educate health stakeholders on appropriate information security practices. We look forward to continued dialogue with NIST and the Department of Commerce, and welcome any questions you may have. For more information, please contact [Jeff Coughlin](#), Senior Director of Federal & State Affairs, at 703.562.8824, or [Stephanie Jamison](#), Director of Federal Affairs, at 703.562.8844.

Sincerely,

Handwritten signature of Paul Kleeberg MD in blue ink.

Paul Kleeberg, MD, FAAFP, FHIMSS
Chair, HIMSS Board of Directors
Chief Medical Informatics Officer
Stratis Health

Handwritten signature of Steve Lieber in blue ink.

H. Stephen Lieber, CAE
President & CEO
HIMSS