601 Pennsylvania Avenue, NW
South Building, Suite 500
Washington, D.C. 20004

T 202.778.3200
F 202.331.7487
ahip.org

April 25, 2022

Sent Via Electronic Mail to: CSF-SCRM-RFI@nist.gov

National Institute of Standards and Technology (NIST)
Attention: Katherine MacFarland
100 Bureau Drive
Stop 2000
Gaithersburg, MD 20899

Re: NIST Cybersecurity RFI / Docket Number: 220210–0045

Dear NIST Representatives:

Everyone deserves the peace of mind of knowing that their personal health information is private and protected. Health insurance providers have long-been committed to instituting privacy and cybersecurity practices to protect every individual's personal health information. That is why we write in response to the Notice and Request for Information (RFI) that was published in the *Federal Register* on February 22, 2022 (87 Fed. Reg. 9579).

AHIP[1] appreciates the opportunity to submit comments in response to the ongoing updates for the Cybersecurity Framework. This Framework has become a foundational document used by many sectors within the United States, including health care. As health care entities are part of the critical national infrastructure, the Cybersecurity Framework has helped to advance awareness of cybersecurity risks through a customized process, providing entities with the ability to evaluate their unique infrastructure in evaluating and assessing cybersecurity risks, needed protections, possible remediations, and designed outcomes for the consumers they serve.

Cybersecurity risks continue to evolve from a lone hacker to nation-state, complex geopolitical campaigns. As cybersecurity risks become more commonplace, public and private entities should take reasonable and prudent steps to protect individually identifiable, proprietary, corporate, and other information held electronically and in physical form. In addition, we have witnessed ransomware and similar events pose serious threats to conducting ongoing business operations. In health care specifically, patient safety and access issues are of primary concern. No individual or entity should be harmed because of ransomware or similar cybersecurity events that can interfere with care delivery, services, accessibility, or outcomes. Our members remain steadfast

[1] AHIP is the national association whose members provide coverage for health care and related services to hundreds of millions of Americans every day. Through these offerings, we improve and protect the health and financial security of consumers, families, businesses, communities, and the nation. We are committed to market-based solutions and public-private partnerships that improve affordability, value, access, and well-being for consumers.

in protecting the consumers they serve and diligently work to stay ahead of trends as they face these real-life situations and potential consequences.

We appreciate the ongoing collaboration between NIST and public and private sector entities, which are the end-users of the Cybersecurity Framework. By enabling public and private sector input into the Framework, the process serves as a current and "living document" that keeps pace with innovations, technological developments, and new and emerging threats.

Our comments are focused on the following key issues:

- **Entities should be encouraged to use the NIST and/or other cybersecurity frameworks that are best suited for them based on their business operations and potential risks.** Implementing strong protections for consumers is the goal. Alignment of the various cybersecurity frameworks (e.g., HITRUST Common Security Framework, the Health Information Sharing and Analysis Center (H-ISAC), internal corporate proprietary solutions) is valuable, as such coordination would ensure that organizations will consistently cover all core domains involved in assessment of their risks. Likewise, this approach allows entities to implement protections based on their unique administrative, financial, technical, and administrative resources.
- **We support maturity targets and similar criteria for risks based on an entity's size, scale, preparedness, and history of events.** While there is more work to be done and public discussions to be held on this topic, we are open to exploring maturity targets to measure the success of ongoing cybersecurity methods. Entities across different sectors compare their environments and risks to other entities that are similarly situated in terms of type, function, and use. For example, leveraging "lessons learned" from broadscale or common attacks, as well as comprehensive cyber campaigns, can be "use cases" for developing criteria that may be used by public or private entities and similarly situated events.
- **Where possible, we support aligning the various NIST frameworks[2] with the Cybersecurity Framework.** These NIST tools, Supplemental and Special Publications, and the variety of NIST resources can then be utilized for various functions that intend to accomplish the same objectives. NIST should either cross-reference or integrate these resources to prevent a siloed approach and to permit businesses to use the NIST tools in an integrative and cohesive approach.
- **The Health / Public Health Sector (HPH) Coordinating Council (SCC) should be leveraged to promote the NIST Cybersecurity Framework.** Much education has been done to date. Future collaboration between NIST and the HPH SCC, as well as other similar activities across other critical business partners, would be beneficial.

[2] *E.g.*, The Privacy Framework, the future Artificial Intelligence Framework, the Integrating Cybersecurity and Enterprise Risk Management Resource (NISTIR 8286), and Special Publications such as 800 -53.

- **The Health Insurance Portability and Accountability Act (HIPAA) should be referenced and discussed where possible in the Cybersecurity Framework.** The HIPAA Privacy and Security rules have been effective for establishing physical, administrative, and technical safeguards, which can encompass cybersecurity protections. We recognize that the NIST Cybersecurity Framework is intended to be agnostic and applicable to sectors beyond health care. NIST should include discussions of the existing HIPAA privacy and security protections when possible, and when issuing guidance and related educational materials that can be used by health care entities.
- **NIST should consider the bipartisan omnibus spending bill for the Cybersecurity Framework and should work with the U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA) to help inform future regulations.** The new law entitled the "Cyber Incident Reporting for Critical Infrastructure Act of 2022" includes several important cybersecurity reporting provisions. A Center will be established within CISA to receive these reports from "critical infrastructure sectors," which includes HPH entities within specific timeframes. A future Notice of Proposed Rulemaking (NPRM) will be issued with details for implementation.

In the attached chart (labeled "Attachment A"), we address more specific, substantive topics to help inform updates to the Cybersecurity Framework. We stand ready to support NIST's work and look forward to public dialogue on these important topics. Please contact me at [redacted] if you have any questions.

Sincerely,

Marilyn Zigmund Luke
Vice President

AHIP
Attachment A
NIST Cybersecurity RFI

Our specific comments below address issues raised in the Cybersecurity Framework. Our comments are organized to correspond with the sections and questions listed in the RFI.

Cybersecurity Framework	AHIP Comment	AHIP Recommendation
Relationship of the NIST Cybersecurity Framework to Other Risk Management Resources	The NIST Framework should be available to use on a voluntary basis, but NIST should recognize that other frameworks and tools may be used in conjunction with, apart from, or in place of the NIST Framework.	Entities should remain free to develop proprietary resources for themselves, their business associates, customers, and partners. There are commonalities between the NIST framework and other voluntary, consensus resources. Existing efforts from HITRUST, the Electronic Health Network Accreditation Commission (EHNAC) and other groups and bodies can provide similar value. Entities should be free to select the tools and approaches that are best for them. For example, a "scorecard" is part of the HITRUST certification and focuses on things to do to help an organization leverage strengths and weaknesses. NIST Frameworks can serve as a model but should not be a mandated approach.
	Alignment or integration of the NIST framework may be done with other international	Entities vary in size, sophistication, and approach to cybersecurity. If possible,

	approaches (e.g., the International Organization for Standardization or "ISO").	international standards could be referenced or "cross-walked" for use by U.S.-entities. For entities who conduct business in other countries, and/or who use business associates or vendors on an international basis, the international standards can promote efficiency and effectiveness. Not all organizations may have the sophistication, need, or resources for international work, and in those cases, the international work can inform but not be made mandatory.
	NIST should consider updates to the Cybersecurity Framework as needed, as opposed to a scheduled interval review.	Allowing for more-frequent or less-frequent updates will provide NIST with the ability to be nimble in response to industry needs and cyber threats. Updates done on a pre-scheduled basis may be unnecessary.
	NIST asked for comments related to background and backward compatibility in relation to the Framework.	The basic structure exists for background and backward compatibility. If there is no specific function to accomplish from a cyber perspective, then backward compatibility appears unnecessary.
	Demonstrating conformance to the NIST guidance can be done internally, but NIST does not provide a "seal of approval," certification or	Existing private industry efforts exist for this purpose. We agree that it is outside the scope of NIST's role to establish such review and

	similar "qualified labeling program."	approval processes given the agency does not operate as a regulatory oversight body (i.e., as opposed to the Centers for Medicare & Medicaid Services which oversees and is responsible for direct administration of the Medicare program).
	NIST helps organizations assess and understand what is important, why they are doing what is important, and what to do if a cyber event occurs.	"Lessons learned" are helpful to explain in practical terms what cyber risks are and what to do when cyber events occur. Some organizations view cybersecurity individually rather than looking at it across a system or the nation. While each focus is important, systemic risks should be communicated so that individuals and organizations can be prepared. When a cybersecurity event occurs, time is of the essence. Helping establish a set of "what-to-do-when" procedures can help entities respond and quickly recover. This is particularly important in health care and for other sectors that comprise the critical infrastructure.
Cybersecurity Supply Chain Risk Management	An entity will determine what its "supply chain" entails based on its own unique business operations.	The definition of a "supply chain" will vary by entity and experience. For example, a retail supply chain will focus on products and availability

		of supplies, whereas in health care a supply chain can be defined more broadly to include things such as devices, tests, blood and blood products, access to claims software, contingency sites for business operations, workforce availability, etc. NIST should define what is meant by "supply chains" and how the diverse and complex structures can be affected by cyber risks.
	NIST can build on the National Initiative for Improving Cybersecurity in Supply Chains (NIICS) with a focus on security and software security to increase trust and assurance in technology products, devices, and services. Likewise, NIST should discuss interoperable frameworks and potential cyber risks, such as the Trusted Exchange Framework and Common Agreement (TEFCA).	While NIST documents are intended to be agnostic by industry sector, there is a specific need within health care to better understand the NIICS work and how it relates to software used within the industry. In addition, NIST should discuss the cyber risks inherent in interoperable frameworks including TEFCA and similar environments. NIST should outreach to other federal and state agencies to ensure that existing NIST tools and resources are understood and used as guidance for impending implementation efforts.
	For managing cybersecurity-related risks in supply chains, NIST seeks input on resources in narrowly-defined	To the extent a system design flaw presents a cyber risk, NIST could work with CISA and other agencies to better define those vulnerabilities on

	areas (e.g., pieces of hardware or software assurance or assured services, or specific to only one or two sectors) that may be useful to utilize more broadly.	an ongoing basis. In addition, NIST and CISA could be more transparent about the work they perform together or in consultation with each other. This transparency should extend to how the Federal Bureau of Investigation becomes involved and in what stages of the processes.
	Communications technology, the Internet of Things (IoT), metadata, the "dark web," and technology that "scrapes" data can pose cybersecurity risks and threats.	NIST can do more to help individuals and entities better understand the threats from uncommon or nefarious applications, which may include tools available in the IoT space, metadata, the dark web, and scraping tools.
	NIST should integrate cybersecurity supply chain risks into the existing Cybersecurity Framework.	We do not recommend establishing a separate framework for Cybersecurity and Supply Chains. If specific information is needed, educational materials or guidance could be developed by NIST as a companion piece or supplemental attachment to the Cybersecurity Framework.