America's Health
Insurance Plans

601 Pennsylvania Avenue, NW
South Building
Suite Five Hundred
Washington, DC 20004

202.778.3200
www.ahip.org

AHIP

January 19, 2018

Submitted Via Email to: Cyberframework@nist.gov
Mr. Edwin Games
Cybersecurity and Privacy Applications
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Dear Mr. Games:

On behalf of America's Health Insurance Plans (AHIP), we appreciate the opportunity to comment on the second draft of the National Institute of Standards and Technology's (NIST) Version 1.1 Draft 2 of the "Framework for Improving Critical Infrastructure Cybersecurity" (the "Framework").[1]

America's Health Insurance Plans (AHIP) is the national association whose members provide coverage for health care and related services to 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. As individuals, businesses, and government organizations increasingly engage across digital platforms, the continuous threat of cyber attacks poses serious challenges to consumers' privacy, national security, and the broader U.S. economy. Health plans continue to prioritize and redefine their readiness to counter and defend against these attacks through targeted prevention and detection operations as well as consumer protection and support efforts. Our members remain committed to working with partners across all industries and sectors to identify threats early and provide a strong defense against cyber attacks in the future.

Health Plans Support an Industry-Driven and Flexible Approach to Cybersecurity
Executive Order 13636 encourages the sharing of threat information to identify, detect, contain, and respond to cyber attacks. The Framework developed by NIST as a result of this Executive Order has worked as intended, and AHIP does not perceive any of the refinements, clarifications, or enhancements in Version 1.1 Draft 2 as a potential hindrance to our members' management of cybersecurity risks. We support the latest version of the Framework as it continues to be risk-based, flexible, and vendor neutral. We also agree the federal alignment section should be

[1] The second draft was made available in December 2017 via the Internet at: https://www.nist.gov/news-events/news/2017/12/update-cybersecurity-framework.

removed to make the document industry-agnostic, which is important for wider adoption of the Framework. Importantly, adoption of the Framework should not prohibit industries and industry leaders from working in conjunction with other implementation models and approaches that best meet their unique needs and circumstances.

We have always supported the view that private entities are and should be encouraged to evaluate their business operations and potential risks, and to utilize NIST and/or other cybersecurity frameworks (e.g., HITRUST Common Security Framework, NH-ISAC, internal corporate proprietary solutions) that are best suited for the entity's business environment. As organizations become more aware of the various existing frameworks that are available to utilize in identifying, assessing, and managing its cyber risks, they are in a stronger operating position to protect consumers. Alignment of these various cybersecurity frameworks is valuable, as such coordination would ensure that organizations will consistently cover all core domains involved in assessment of their risks.

We appreciate the work that NIST has completed to revise and emphasize the Framework's focus on the correlation of business results to cybersecurity risk management. However, we do have some concerns about the emphasis on metrics and measures. As we have stated in prior comments and in public policy forums, the use of validated metrics and measures can help improve business processes, and we encourage continued research in identifying connections between metrics and beneficial cybersecurity outcomes. For example, as laid out under Section 4.0, in instances where an organization goes beyond self-assessment and seeks third-party input in measuring its cybersecurity risks, we would urge very careful consideration of how business metrics may be viewed and shared with those third-parties. While certain metric-sharing can ultimately lead to a stronger understanding of an organization's cybersecurity risks, costs, and benefits, we believe it is important to stress that any metric-sharing mechanisms are, and should continue to be, voluntary on behalf of industry. In addition, organizations' self-assessments of cybersecurity risks need to be managed in ways that keep that information confidential and secure.

Cybersecurity is a unique area where one technique that works within one operating environment may not be suitable for a different organization with a different operating environment. We encourage NIST to consider the use of metrics as a flexible measurement option an organization has to potentially achieve better cybersecurity outcomes, rather than the standard to quantify adequacy. We also offer reservations about metrics potentially becoming part of audit processes that can reveal entities' most trusted information. Particularly with respect to Tiering and "Maturity Scores," it would not be beneficial to mandate diverse entities of different sizes to achieve a certain "Tier Level" to show compliance. We believe this could compel an organization to deviate from effective cybersecurity practices it may already have in-place in order to avoid the potential of regulatory scrutiny for not achieving a certain Tier Level.

Protecting individual privacy was discussed at length at the NIST Cybersecurity Framework Workshops, but developing the appropriate methodology appears to be a work in progress. The current methodology to protect privacy focuses on five areas (governance of cybersecurity risk, access controls, awareness and training, monitoring and detection, and response activities). There seems to be other important activities related to protection of individual privacy that are not considered in the framework, such as encryption controls of individually identifiable information, identification and protection of highly sensitive information, and audit controls.

In addition, it can be important and extremely helpful to include industry references (e.g., HITRUST, SOC2 ISO) to related or similar standards that are used within the health care industry. We support including industry references when available and ask the NIST drafters to reconsider the current approach of removing such references from the current and future drafts.

Health Plans Are Committed to Consumers

While we work with other stakeholders to prevent and identify the ongoing threat of cyber attacks, our commitment to consumers remains our foremost concern. Health plans must be prepared to provide peace of mind to consumers if cyber criminals steal their information. The industry stands ready to face this growing challenge, and our members will continue to support ongoing collaborations with customers, NIST and other government representatives, and other key stakeholders.

Thank you for the opportunity to provide these comments. AHIP welcomes any questions you may have regarding these comments. Please contact Marilyn Zigmund Luke, AHIP's Vice President, Executive Department, at (202) 861-1473 or mzluke@ahip.org.

Sincerely,

Matthew Eyles

Matthew Eyles
Senior Executive Vice President & Chief Operating Officer