From: **Alberts, Brian**
Date: Mon, Apr 10, 2017 at 2:46 PM
Subject: Comments on Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity
To: "cyberframework@nist.gov" <cyberframework@nist.gov>

To Whom It May Concern:

On behalf of America's Health Insurance Plans (AHIP), I am pleased to submit our comments on the draft update of the Framework for Improving Critical Infrastructure Cybersecurity.

Please let me know if you have any questions. Thank you.

Brian Alberts | Senior Policy Analyst, Federal Affairs
America's Health Insurance Plans

[Attachment Copied Below]

April 10, 2017

Via 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 respond to the National Institute of Standards and Technology's (NIST) request for information on the Version 1.1 draft of the "Framework for Improving Critical Infrastructure Cybersecurity" (the "Framework").

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 are prioritizing 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 are 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 as a potential hindrance to our members' management of cybersecurity risks. The Framework continues to be risk-based, flexible, and vendor neutral. Importantly, it has not prohibited industries and industry leaders from working in conjunction with other implementation models and approaches that best meet their unique needs and circumstances.

It is AHIP's 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) that are best suited for the entity's business environment.

We appreciate the work that NIST has completed to update the framework and the framework's focus on the correlation of business results to cybersecurity risk management metrics and measures. The use of validated metrics and measures are fundamental to all business practices, and we agree that more research should be directed towards identifying connections between metrics and beneficial cybersecurity outcomes. However, we would urge careful consideration of how business metrics may be viewed and shared between third-parties, and believe that any metric-sharing mechanisms should continue to be voluntary on behalf of industry.

Health Plans Remain Committed to Consumers

While we work with other stakeholders to prevent and identify 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 ongoing 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. To inquire, please contact Marilyn Zigmund Luke, AHIP's Vice President of Special Projects.

Sincerely,

Matt Eyles
Executive Vice President