America's Health
Insurance Plans

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

202.778.3200
www.ahip.org


February 4, 2016

Via Cyberframework@nist.giv

Ms. Diane Honeycutt
Secretary
Computer Security Division
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Dear Ms. Honeycutt:

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 "Framework for Improving Critical Infrastructure Cybersecurity" (the "Framework").

AHIP is the national association for the health insurance industry. Our members provide health and supplemental benefits to the American people through employer-sponsored coverage, the individual insurance market, and public programs such as Medicare and Medicaid. AHIP advocates for public policies that expand access to affordable health care coverage to all Americans through a competitive marketplace that fosters choice, quality, and innovation.

As individuals, businesses, and government organizations increasingly engage across digital platforms, the growing 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 Cyber security**

The President's Executive Order (the "Executive Order")[1] on cybersecurity includes policy principles that correctly recognize a top-down regulatory approach to this national security issue is unlikely to be effective. Instead, the Executive Order encourages the sharing of threat information to identify, detect, contain, and respond to cyber attacks.

The voluntary Framework developed by NIST outlines cybersecurity objectives and focus areas that allow an organization to better manage its cybersecurity risks, but does not impose prescriptive implementation requirements in keeping with the principles laid out in the Executive Order. AHIP supports this approach. The Framework is risk-based, flexible and vendor neutral. Importantly, it does not prohibit industries and industry leaders from working in conjunction with other implementation models and approaches that best meet their unique needs and circumstances. AHIP has received anecdotal information that the NIST framework is working effectively for entities that have adopted the framework as a foundation for cybersecurity protections. It is AHIP's view that private entities are and should be encouraged to evaluate their business operations and potential risks and to utilize either the NIST or other cybersecurity frameworks (e.g. HITRUST Common Security Framework, ISO 27000 Series) that are best suited for the individual entity's business environment.

**Industry-Led Initiatives to Improve Cybersecurity Risk Management**

Last year, led by its Board of Directors, AHIP completed a comprehensive evaluation and strategic plan to address cyber threats from an industry perspective. These efforts were guided by members of AHIP's Cybersecurity Work Group, which includes Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) from AHIP's member plans, and a specified Task Force ("the Task Force") of CISOs to advise AHIP staff on day-to-day activities. To inform those cybersecurity efforts, AHIP engaged Deloitte LLP to collaborate with the Task Force to develop a comparative risk analysis profile based upon the Framework created by NIST. The risk analysis profile is designed for individual health plans to use as a risk management tool for evaluating and comparing their current cybersecurity risk prevention and detection strategies.

[1] Executive Order 13636 "Improving Critical Infrastructure Cybersecurity"

A core focus of this industry-driven response to emerging cybersecurity threats was to ensure the company-specific implementation flexibility that is necessary for assessing and guarding against an entity's specific risk environment. Today, AHIP's member plans are using the industry-led risk analysis profile, among other resources, to hone their risk mitigation strategies and protect consumers' information across all markets.

**The Framework is Working Well, as Intended**

At this time AHIP does not perceive a need for the substance of the framework to be altered or updated. Awareness of the Framework is extensive within the health insurance industry. The Framework serves as a basic, flexible, and adaptable tool for managing and reducing cybersecurity risks. In our direct experience, its blueprint is being used to improve cybersecurity risk management, as intended.

*For Example*: Using the Framework as a guide, AHIP's Task Force, with Deloitte, was able to effectively identify and prioritize specific areas of risk that should be considered by individual plans as they worked to refocus their company-specific strategies to address their unique technology systems and operations. Ultimately this led to the development of a risk analysis management tool, led by private industry and in keeping with the Framework's focus areas and overall purpose: to align the government and private sector and improve cybersecurity risk management.

**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. By sharing best practices and lessons learned from our industry-wide effort – and the broader nationwide effort – to identify and contain cyber attacks, we can strengthen our defense against this evolving and ever present threat.

Additionally, our member companies look forward to new opportunities for the sharing of timely cybersecurity information under the policies enacted with the Cybersecurity Act of 2015.[2] Because better, more actionable information is the best defense against emerging cyber threats, AHIP supports this landmark legislation. Throughout the next year NIST will play a key role in acting to implement that law. In its work to develop and maintain the Framework, we appreciate that NIST has executed an inclusive approach, informed by the views of a wide array of individuals, organizations, and sectors. In its concurrent effort to implement the Cybersecurity Act of 2015, we urge NIST to continue this approach as steps are taken to build the infrastructure that will support the voluntary sharing of information across industries, as well as between the public and private sectors.

Thank you for the opportunity to provide these comments. AHIP welcomes any questions you may have regarding these comments. To inquire, please contact Amber Manko, AHIP's Director of Federal Affairs, at (202)861-6371 or amanko@ahip.org.

Sincerely,

Carmella Bocchino
Executive Vice President

[2] As passed in the *Consolidated Appropriations Act, 2016.* Pubic Law No: 114-113.