From: **Willis, Sarah**
Date: Mon, Apr 10, 2017 at 5:37 PM
Subject: EHR Association Comments on Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity
To: "cyberframework@nist.gov" <cyberframework@nist.gov>
Cc: Nam Nguyen, "Chandrasekaran, SayeeBalaji", "Arnett, Gail", "Burchell, Leigh", "Cholmes, Henry", "Dvorak, Carl", "Fleet, Eli", "Ganley, Joseph", "Buitendijk, Hans", "Dhanani, Nadeem", "Ramirez, Nancy", "Pantuso, Erica", Richard Loomis, "Rick Reeves", Sasha TerMaat, "Segal, Mark", "West, Liddy", "Willis, Sarah"

Good Afternoon,

On behalf of the EHR Association, we are pleased to submit our comments on NIST's Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity. Please let us know if you have any questions.

We look forward to continuing to work with you on our shared objective to make this guidance as useful as possible for all stakeholders.

Warm Regards,
Sarah

Sarah Willis-Garcia | Program Manager, EHRA | HIMSS North America | 33 W Monroe, Ste 1700, Chicago, IL 60603

www.ehrassociation.org | @EHRAssociation

[Attachment Copied Below]

33 W. Monroe, Suite 1700
Chicago, IL 60603
swillis@himss.org
Phone: 312-915-9518
Twitter: @EHRAssociation

April 10, 2017

Edwin Games
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Dear Mr. Games,

The Electronic Health Record Association (EHRA) is pleased to comment on the draft revision of the NIST Framework for Improving Critical Infrastructure Cybersecurity. As our members embrace this framework as a cybersecurity implementation tool, our comments are focused on improving the usability of the document to 1) decrease the learning curve for the novice user and 2) increase adoption of the framework in the industry. With the national push to train more cybersecurity professionals, we believe it is of paramount importance that this next iteration of the framework be more accessible.

Comments are noted by page or section where appropriate:

Line 814 through 828
The section on Types of Cybersecurity Measurement is a challenge to navigate to get a clear understanding of all the relevant guidance to consider. For instance, the document states, "A measure of the extent that governance and risk management process address cybersecurity risk (ID.GV-4) is reflected in the metric." We follow the references to COBIT 5 DSS04.02 and then need to do our own interpretation of that document. The framework would be more useful if it specified actual examples of measurements for each measurement type. As measurement is key to any security program, we believe that the new draft should have clearer and stronger guidance on measurement.

Line 830
This section alludes to some form of aggregation methodology. However, no guidance is given on how to aggregate the metrics. A clear example or reference to how aggregation can or should be done would be useful for implementers.

Line 893 through 894 (Table 3: Framework Core)
Though we understand this document is meant to be a framework that references more detailed information on each subcategory, we believe it would benefit any user if the document also gave a descriptive, narrative example of each subcategory in addition to the title and the listing of informative references. While reviewing the document, the reader must interpret the subcategory using only its title. This became most apparent during our review when assessing new subcategories such as PR.AC-6 and PR.DS-8. With the addition of a simple example, the Framework Core table can better convey the intent of each category and subcategory, be more practical for the novice user, and better convey the intent of the framework authors.

Again, on behalf of the more than 30 EHRA member companies who develop and support the vast majority of EHRs in use by hospitals and ambulatory care organizations across the US, we appreciate this opportunity to provide feedback to NIST. We look forward to our ongoing collaboration to make this guidance as useful as possible for all stakeholders.

Sincerely,

Sasha TerMaat
Chair, EHR Association
Epic

Richard Loomis, MD
Vice Chair, EHR Association
Practice Fusion

HIMSS EHR Association Executive Committee

Hans J. Buitendijk
Cerner Corporation

Leigh Burchell
Allscripts

Cherie Holmes-Henry
NextGen Healthcare

Nadeem Dhanani, MD, MPH
Modernizing Medicine

Joseph M. Ganley
McKesson Corporation

Rich Reeves, RPh
Evident

About the EHR Association
Established in 2004, the Electronic Health Record (EHR) Association is comprised of over 30 companies that supply the vast majority of EHRs to physicians' practices and hospitals across the United States. The EHR Association operates on the premise that the rapid, widespread adoption of EHRs will help improve the quality of patient care as well as the productivity and sustainability of the healthcare system as a key enabler of healthcare transformation. The EHR Association and its members are committed to supporting safe healthcare delivery, fostering continued innovation, and operating with high integrity in the market for our users and their patients and families.

The EHR Association is a partner of HIMSS. For more information, visit www.himssehra.org.