January 19, 2018

Walter Copan, M.D.
Director
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Dear Director Copan:

The College of Healthcare Information Management Executives (CHIME) and the Association for Executives in Healthcare Information Security (AEHIS) are pleased to submit comments on the National Institute of Standards and Technology's (NIST) "Framework for Improving Critical Infrastructure Cybersecurity," Draft 2, Version 1.1 published on December 5, 2017.

CHIME membership consists of more than 2,500 chief information officers (CIOs) and other senior information technology executives at hospitals and clinics across the nation. CHIME members are responsible for the selection and implementation of clinical and business information technology (IT) systems that are facilitating healthcare transformation. Launched by CHIME in 2014, AEHIS represents more than 800 chief information security officers and provides education and networking for senior IT security leaders in healthcare.

CHIME and AEHIS continue to be strong champions of the NIST CSF and believe it should be used by the entire healthcare sector. We are pleased that NIST took many of our suggestions and incorporated them into Draft 2, Version 1.1, including an increased focus on identity management and supply chain controls. Our comments will focus primarily on three areas: identity management and access control; supply chain; and measurement. Our comments work off the redlined version NIST published. We also offer some ideas for future consideration. Each of these topics is discretely addressed in greater detail in the body of our letter. Our overarching comments and recommendations are summarized below.

I. Overarching Comments & Recommendations

- **We strongly support the NIST CSF and the changes NIST has made to improve the CSF.**
- **The need for a shared responsibility for managing risk has never been more important. Our members still struggle to obtain manufacturer disclosure sheets (MDS).**
- **The language added around communication in Section 3.3 is very helpful and will help create a more equitable environment where the risk is indeed shared; however, some clarification is needed.**
- **Managing residual risk should be addressed in Section 4.0.**
- **NIST should recommend that users of the CSF use a maturity model and that CMMI be used as the example.**
- **Under the "Protect" function, we agree with the way NIST has structured this category and the associated subcategories.**
- **We support NIST's increased attention around supply chain, especially the reference to ISAOs, which is very helpful. However, we recommend NIST revise the language to reflect that there**

needs to be cooperation between the manufacturers/vendors and those implementing the NIST CSF.

- **For future drafts, we recommend NIST address cloud security.**

II. 3.0 How to Use the Framework

Section 3.3: Communicating Cybersecurity Requirements with Stakeholders

We appreciate and support the language NIST added under this section. Broadly, the new emphasis on supply chain risk management (SCRM) reflects our members' concerns about our growing need to manage cybersecurity risk in external parties, including software vendors, cloud vendors and medical device manufacturers. Especially in cases where vendor choices are limited, we feel the language added by NIST will be helpful in furthering a more equitable environment where supply chain cybersecurity risk can be discussed candidly, and perhaps addressed more consistently through contracting and ongoing monitoring.

While the language of section 3.3 does include the statement that cyber SCRM activities include potentially "verifying that cybersecurity requirements are met through a variety of assessment methodologies" (lines 691-692), some additional narrative emphasis on potential assessment approaches would be appreciated. What approaches or standards might NIST recommend here? As one member reflected, line 660 suggests using target profiles to "express cybersecurity risk management requirements to an external service provider." While they found the target profile definitions to be sufficiently flexible they said, "I wouldn't know what to do with someone's request to "build for Tier 2. Encouraging the development of security baselines, likely based on the CFS categories then encouraging people to consider the "Identify" section includes the need to verify/communicate baseline requirements with suppliers," might be more be helpful.

Additionally, line 715 includes the acronym "OT," but the meaning is not immediately apparent to readers from the healthcare sector. Could such terms include a definition?

Section 3.4: Buying Decisions

We appreciate the language NIST added in this section explaining that buying decisions will not always be able to satisfy our security requirements, and noting that additional management actions may be necessary to address residual risk. This revision spells out how things really work in the field.

III. Measurement

Again, we appreciate NIST' added attention to the topic of measuring cybersecurity risk. Our members have noted, however, that there is no defined maturity model in the CSF. **There is still no reference to whether our members should be using Prism, CMMI, Gartner, etc. CHIME and AEHIS suggest NIST edit the draft to recommend that users of the CSF use a maturity model and that CMMI be used as the example.**

Some members felt NIST attempted a maturity model in Section 2.2 which the agency refers to as Tiers. While NIST states that Tiers do not represent maturity, some members find this makes this section more confusing because they don't know how you separate the Tier concept from a maturity model. They felt NIST tried to focus specifically on the risk management process, offering a general broad-brush measure of maturity that would merely

result in a “feel-good number” without a strong connection to how a company is actually performing. Without a specific connection to the controls in the CFS designating which Tier a control might address, this concept they feel is merely conceptual, and not actionable in a consistent way. Therefore, an alternate approach would be to replace the Tier concept with a full CMMI concept to measure individual control progress (which by themselves can be too broad to measure accurately in some cases), and encourage a more quantitative measure of progress. This could have the benefit of informing providers which areas of the CFS where improvement is most needed.

IV. 4.0 Self-Assessing Cybersecurity Risk with the Framework

Our membership recommended that NIST produce a toolkit that allows for the easy and consistent self-assessment practices. If NIST could produce a recommended methodology and provide the tool for self-assessment, this would ensure consistency was being applied across all critical infrastructure. Additionally, the provided spreadsheet in the original version 1.0 makes capturing adjustments to sub-categories and the related industry standard controls (ISO, 800-53, etc.) quite difficult due to the use of merged cells.

We also believe the need to track and managing residual risk should be addressed more clearly. We recommend that this could be added to the language under Section 4.0, “Self-Assessing Cybersecurity Risk with the Framework"

V. Appendix A: A Framework Core

Identity Management and Access Control

Under the “Protect” function, we appreciate NIST taking our suggestion to modify the Access Control Category to now include identity management, as well as authentication. It now reads, “Identity Management, Authentication and Access Control (PR.AC).” In Draft 1, Version 1.1, NIST listed five subcategories under this category. In the current draft, there are now six subcategories as PR.AC.6 has been added. It reads, “Identities are proofed and bound to credentials and asserted in interactions when appropriate.” **We agree with the way NIST has structured this category and the associated subcategories.**

Supply Chain

We also appreciate that NIST added more language that bolsters the supply chain category. In our comment letter on the previous draft, we recommended NIST expand the scope of this category. We are pleased NIST accepted our suggestion to expand the scope of the “Supply Chain Management Section” to reflect the wider array of parties with whom users of the framework are encountering data that must be protected; in the case of healthcare providers, this is considered “protected health information” or PHI.9

Discussed under “Framework Basics,” under the discussion of Tiers, is the following (lines 437-441):

> *The organization does not collaborate with or receive information (e.g., threat intelligence, best practices, technologies) from other entities (e.g., buyers, suppliers, dependencies, dependents, ISAOs, researchers, governments), nor does it share information. The organization is generally unaware of the cyber supply chain risks of the products and services it provides and that it uses.*

We believe the reference to ISAOs is very helpful and we support its inclusion. It is worth noting that healthcare providers still do not have all the tools in place to support the needed information sharing. Our members

report they still are challenged getting information from vendors. As one member reflected, "We can barely get the vendors to patch the systems or for us to be able to touch the devices to get a picture of the state of risk." Additionally, the Internet of Things (IoT) provides another reason we believe the language around the ISAO and information sharing is important. **We therefore recommend NIST revise the language to reflect that there needs to be cooperation between the manufacturers/vendors and those implementing the NIST CSF.** Adding this additional language will provide another avenue for a shared responsibility for protecting patient information – one that is shared by vendors/manufacturers as well as providers.

VI. Topics for Future Consideration

One area which we would have liked to have seen more attention is around cloud security. The only mention in the document on this is in Section 3.3 (line 661). As more healthcare is being pushed further into the cloud, services and accountability becomes less clear. Given to proliferation of cloud-based vendor solutions and that security with these vendors comes down to another parties' risk assessment, we believe this topic warrants its own section. As one member shared with us, his organization is using a well-known electronic health record vendor's cloud, which involves 80 applications and other solutions used for the administrative side of their business. A total of 80 percent of their core business is thus cloud-based. He noted, "As you begin to look at some of these framework issues, there is a question about who has the responsibility to protect… they are being pressed on cost more than any other industry and this is forcing vendors coming to healthcare with cloud solutions because it's cheaper. They will be pushed more into this environment more than other industries." This situation came to light with a prominent breach last year involving a cloud-transcription service used by many hospitals.

Finally, on the matter of cloud security it is also worth highlighting that the security requirements between IAAS, PAAS and SAAS are different and thus cause confusion and challenges between vendors and clients. There are several things an organization should be doing if they are running IAAS, but as one member noted, many think "it's in the cloud, they secure it better than we can" without realizing the obligation is on the client.

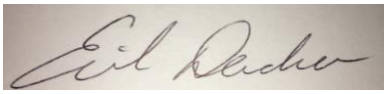
VII. Conclusion

CHIME and AEHIS appreciate the chance to offer our ongoing input to this important document and will continue to champion the need for the use of the CSF across the entire healthcare sector. If you have any questions concerning our comment letter, please contact Mari Savickis, vice president, federal affairs, at msavickis@chimecentral.org.

Sincerely,

Russell Branzell, FCHIME, CHCIO
CEO & President, CHIME

Cletis Earle, Chair,
CHIME Board of Trustees
Vice President and CIO
Information Technology
Kaleida Health



Erik Decker
Chair, AEHIS Board
CISO and Chief Privacy Officer
University of Chicago Medicine