CHIME DIGITAL HEALTH LEADERS

AEHIS
Association for Executives in Healthcare Information Security

April 21, 2022

Dr. Laurie Locascio
Director
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Dear Dr. Locascio:

The College of Healthcare Information Management Executives (CHIME) and the Association for Executives in Healthcare Information Security (AEHIS) welcome the opportunity to submit comments in response to the National Institute of Standards and Technology *Request for Information: Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management* published in the *Federal Register* on February 22, 2022.

CHIME is an executive organization dedicated to serving chief information officers (CIOs) and other senior healthcare IT leaders. Consisting of more than 2,900 members in 60 countries, our members are responsible for the selection and implementation of clinical and business technology systems that are facilitating healthcare transformation. Launched by CHIME in 2014, AEHIS represents more than 950 healthcare security leaders and provides education and networking for senior IT security leaders in healthcare. CHIME and AEHIS members are among the nation's foremost health IT experts, including on the topics of cybersecurity, privacy and the security of patient and provider data and devices connecting to their networks.

CHIME and AEHIS are strong supporters of the NIST Cybersecurity Framework (CSF) and our organizations have contributed to the policymaking process by commenting on previous requests for comment. Our members rely on the CSF to help guide their cybersecurity practices and leverage it as a foundation for improving their overall cyber posture. Furthermore, we are avid supporters of 405(d) Program and Task Group which is based off the CSF.

We appreciate NIST looking for ways to improve the CSF by prioritizing supply chain-related cybersecurity needs across sectors. Below we have responded to several of the questions posed by NIST in this RFI. Outlined immediately below are our top points:

Key Takeaways

1) **Employing the NIST CSF continues to pose challenges for smaller and lesser resourced organizations who need more prescriptive steps they can take if they are to improve their cyber posture. A better jumping off point for resource-challenged organizations is a best practices guide.**
    a) Recommendation: **We recommend that NIST work with 405(d) to educate smaller providers on concrete steps that can be taken now.**
2) **The focus needs to shift away from the mindset of how one stacks up against another provider and focus more on the provider's own maturity journey. One way measurement could occur in our sector is through the use of the 405(d) tool, Health Industry Cybersecurity Practices (HCIP), which is attempting to address some of these challenges.**
    a) Recommendation: **We recommend NIST develop a flow chart or road map that can help organizations connect all of these resources and recommendations and map them back to the CSF.**

Current benefits of using the NIST Framework

Has communication improved between organizations & entities (e.g., supply chain partners, customers, insurers)?

Communication around the use of the CSF varies depending on the stakeholder, but in many cases our members find that they still must engage in considerable education around it. Many experience challenges specifically around supply chain partners as there are several who still have not embraced the CSF and securing buy-in still requires significant effort. Also, since healthcare providers are not in the supply chain, they are not the customer.

One partner that continues to present risks for our members and where the need for education is high is with physician practices who carry a substantial amount of risk given their cyber posture is still quite immature. These physician practices are typically how patients enter the bigger provider operations (hospitals, rehab facilities, long-term care facilities); they are a supply chain of patients and, consequently, highly valuable and protected personal information.

Given the proliferation of cyber-attacks over the past few years, cyber insurance carriers are taking a much greater interest in providers' cyber posture. The sophistication around what is truly required to improve cyber hygiene differs across our members as they have varying levels of sophistication and knowledge.

When it comes to cyber insurance, providers continue to be asked very basic questions about their environment such as whether they are using 8-character passwords / phrases or are required to complete a several hundred question survey. Often, the questions are seemingly arbitrary, and the line of questioning can be related to whatever the most recent cyber-attack centered on. Some members also report being asked whether they are using a proprietary framework (i.e., HITRUST) and report their first interaction with the carriers begins with the sales team who has limited technical knowledge. From the perspective of our members working in larger or more sophisticated organizations, cyber insurance carriers must also begin to move away from simply querying if they are using the CSF and begin drilling down into the tiers of the CSF.

Does the Framework allow for better assessment & management of risks?

Due to the risk-based and business-operations approach of the CSF, where the NIST CSF has been implemented, it is much more easily grasped and used by non-IT and non-security executives. This drives more engagement, participation and interest in security than those frameworks which are more technically focused and controls based. Everyone understands the impact to patient care if the electronic health record (EHR) is unavailable in a much more impactful way than just being told they need to run phishing exercises to prevent ransomware.

What are relevant metrics for improvements to cybersecurity as a result of Framework implementation?

Developing benchmarks against which to measure maturity continues to pose challenges for our members. And metrics for providers will vary from the metrics needs to measure supply chain partners.

We recognize that the CSF is not a maturity model, however the feeling is that as soon as you begin trying to compare yourself to others you are dealing with a maturity model situation. Boards of directors, eager for more cyber knowledge and metrics, can lead to scenarios where providers end up developing their metrics based on the CSF. **The focus needs to shift away from the mindset of how one stacks up against another provider and focus more on the provider's own maturity journey.**

One way measurement could occur in our sector is through the use of the 405(d) tool, Health Industry Cybersecurity Practices (HCIP), which is attempting to address some of these challenges. The development of these best practices were mandated by Congress under the Cybersecurity Information Sharing Act of 2015. Since that time, Congress also identified - under Public Law 116-321 - these best practices are among the ones that the U.S. Department of Health & Human Services' (HHS) Office for Civil Rights (OCR) must recognize when considering whether to mitigate length of audits and severity of fines imposed on a Health Insurance Portability and Accountability Act (HIPAA) covered entity or business associate if cybersecurity best practices are used.

Current challenges of using the NIST Framework

Challenges that may prevent organizations from using the NIST Cybersecurity Framework or using it more easily or extensively including: Resource considerations; Information sharing restrictions; Organizational factors; Workforce gaps; and Complexity

While most of our members do use the CSF, a lot do not and in many cases this is due to resource constraints. For instance, we have a member who is a federally qualified health center (FQHC) and while they have attempted on several occasions to start this work, it has sputtered due to staffing, complexity and the financial investment needed. Instead of adopting the CSF they elected to use the Center for Internet Security (CIS) top 20 and hired someone to lead their risk management work. Also, adopting a controls-based approach rather than a risk-based approach like NST, risks providers trying to control for risks they may not even have.

For members who have larger budgets and more staff, the CSF is an excellent tool and can be easier to digest than NIST 800-63. **A better jumping off point for resource-challenged organizations is a best practices guide; jumping straight into the CSF is simply too overwhelming.** The 405(d) HCIP resource, based on the CSF, has also been found to be very helpful and has been tailored for both smaller and better resourced organizations.

Any features of the Framework that should be changed, added, or removed

We believe that NIST's resources for small businesses could also be better leveraged, as well as NIST's National Cybersecurity Center of Excellence (NCCoE). **We recommend that NIST develop a flow chart or road map that can help organizations connect all of these resources and recommendations and map them back to the CSF.** This would include 405(d)'s HCIP and supply chain resources.

Impact to the usability and backward compatibility of the Framework if the structure is modified or changed

Our concern with modifying the CSF is that many organizations use government risk & compliance tools (GRCs) and that these tools map to the CSF, therefore, any changes will break the mappings and will require substantial effort to remap which will affect numerous internal operations such as audits.

Additional ways in which NIST could improve the Cybersecurity Framework or make it more useful

We recognize NIST is attempting to thread a needle in so far as the tool has been developed to be used by a variety of organizations in different sectors with different needs. Thus, NIST has purposefully developed the CSF to be flexible, not overly prescriptive, and does not consider the tool to be a standard. While we appreciate the balance NIST aims to strike, we believe smaller organizations will need more prescriptive steps they can take if they are to improve their cyber posture. **We thus recommend that NIST work with 405(d) to educate smaller providers on concrete steps that can be taken now.**

Suggestions for improving alignment or integration of the Framework with other NIST risk management resources

What are benefits / challenges of using these resources alone or in conjunction with the CSF?

As noted earlier, our primary recommendation is for NIST to create a flowchart or likeminded tool that helps users of the CSF navigate the tiers, profiles, models, and resources. Even our most sophisticated members experience challenges using the CSF, therefore, tools that can break this down into bite sized pieces will be welcomed.

Are there commonalities or conflicts between the NIST framework and other voluntary, consensus resources?

For the healthcare sector, we continue to point to the excellent work that resulted in the best practices known as HCIP, developed out of the 405(d) public-private collaboration.

Cybersecurity Supply Chain Risk Management

What are the greatest challenges related to the cybersecurity aspects of supply chain risk management that the NIICS could address?

We continue to assert that cybersecurity remains a shared responsibility. This means, when it comes to supply chain issues, the purchaser of technology – in our case the healthcare providers – cannot be solely responsible for breaches stemming from third party products (i.e., Log4j). OCR oversees breaches in the healthcare sector; however, their oversight only extends to those governed by HIPAA. Many third parties such as software and medical devices fall outside of HIPAA. Federal authorities must recognize – at least from a compliance standpoint – that much of the cyber risk providers take cannot be universally born by them.

We applaud the Food and Drug Administration (FDA) for taking steps to improve the pre-market device submissions through their revised draft guidance issues earlier this month, *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions.*

We furthermore support the extra authority they seek from congress to improve the cybersecurity of medical devices which they note in their budget submission is presently missing and which serves as an impediment to patient safety. They state:

> *FDA seeks to have express authority to require: that premarket submissions to FDA include evidence demonstrating reasonable assurance of the device's safety and effectiveness for purposes of cybersecurity; that marketed devices demonstrate a reasonable assurance of the device's safety and effectiveness for purposes of cybersecurity; that devices have the capability to be updated and patched in a timely manner; that manufacturers provide a device Software Bill of Materials (SBOM) with their devices so users know which components of their devices are or may be subject to cyber threats; and that device manufacturers publicly disclose when they learn of a cybersecurity vulnerability so users know when a device may be vulnerable, and to provide direction to users to reduce their risk.*

We also are very pleased to see the Protecting and Transforming Cyber Health Care (PATCH) Act legislation introduced on March 31 by Senators Bill Cassidy (R-LA) and Tammy Baldwin (D-WI) with companion legislation introduced in the House by Representatives Michael Burgess, M.D. (R-TX) and Angie Craig (D-MN). The legislation would, among other things, implement cybersecurity requirements for manufacturers applying for premarket approval through the FDA.

What are the greatest challenges related to the cybersecurity aspects of supply chain risk management that the National Initiative for Improving Cybersecurity in Supply Chains (NIICS) could address?

One approach that could be helpful is appropriate contract terms that protect both parties. Presently, healthcare providers are often at a disadvantage and contracts are lopsided frequently favoring the vendor. Furthermore, it requires heft and knowledge to negotiate favorable terms and small and lesser-resourced providers are at a disadvantage. Much of this comes down to resources. For instance, we have a member who works in a rural healthcare setting and his organization's geographic practices index is 0.71; if his organization index were set at 1.0, he would receive $60 million more in Medicare funding. Yet, he must pay the same prices as those who receive the full index meaning he ultimately has fewer resources to invest in his workforce and cyber posture. Simply put by one member, "Cost to be cyber secure is higher for disadvantaged providers."

Another member who works in a federally qualified health center in an urban area and whose patient census is three quarters Medicaid, also struggles to obtain the necessary resources to obtain favorable contract terms and make meaningful cyber investments. Not only this but this member's organization was unable to obtain the same amount of cyber coverage from the previous year despite purchasing a supplemental policy. These are systemic issues that are not easily and entirely addressable by NIST. However, we strongly encourage NIST to have these conversations with other federal partners such as the Centers for Medicare & Medicaid Services (CMS) who is the largest payer in the country so they can identify ways that the agency could help providers and other healthcare stakeholders to identify creative solutions to help incent investment in better cyber hygiene. We recognize that there will be areas that are simply outside of CMS' control and will require congressional action. Having these conversations, though, is helpful in identifying needs. Locating a sustainable funding pathway is going to be critical if we are to make a bigger dent in our sector's cyber posture.

Finally, another area we identified as a challenge involves vendors providing services in house but whose corporation is outside the US. Some of these vendors do not need to meet US standards. Any pressure that can be brought to bear on these vendors to emphasize that they must meet US standards would also be helpful. We encourage NIST to work with the FDA on this as it pertains to medical devices.

How can NIST build on its current work on supply chain security, including software security work stemming from E.O. 14028, (executive-order/14028) to increase trust and assurance in technology products, devices, and services?

With the newly enacted mandatory cybersecurity threat and ransomware provisions in the Cyber Incident Reporting Act included in the recent omnibus bill, there will be an even greater focus on threat sharing. We welcome this but we encourage NIST to work with CISA to ensure that threat sharing remains a two-way street. There is some concern in our community that we will be required to share threats but that we may not receive the necessary information back from federal partners to help improve our cyber posture. And confusion continues around when it's acceptable to share threats. According to our 2021 cybersecurity survey only ten percent of respondents felt they had a clear understanding of when they could share threat information.

While the NIST CSF does not contain very granular guidance related to supply chain, there are other more detailed documents and resources that exist related to Executive Order 14028. These include NIST's revised Secure Software Development Framework (SSDF) Version 1.1 (February 4, 2022) in response to Section 4e, a draft update of NIST's Secure Software Development Framework (SSDF) Version 1.1 (September 30, 2021) in response to Section 4e, and a second draft revision of NIST SP 800-161 Revision 1 (October 28, 2021) in response to Section 4c.

Are there gaps observed in existing cybersecurity supply chain risk management guidance and resources, including how they apply to information and communications technology, operational technology, IoT, and industrial IoT?

We also believe that NIST's Cybersecurity Center of Excellence (NCCoE) could help build this into their guidance on medical devices. And we recommend that NIST create a workgroup or detailed guidance that helps provide actionable items on how to operationalize the CSF.

If you have any questions related to our letter or would like to discuss further, please contact Mari Savickis, Vice President of Public Policy, at mari.savickis@chimecentral.org.

Sincerely,

Russell P. Branzell

Russell P. Branzell, CHCIO, LCHIME
President and CEO CHIME