February 9, 2016

Diane Honeycutt
National Institute of Standards and
Technology, 100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Dear Ms. Honeycutt:

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 (NIST) Request for Information (RFI), *Views on the Framework for Improving Critical Infrastructure Cybersecurity*, published December 11, 2015.

CHIME is an executive organization serving more than 1,700 chief information officers (CIOs) and other senior health information technology leaders at hospitals and clinics across the nation. CHIME members are responsible for the selection and implementation of clinical and business technology systems that are facilitating healthcare transformation. CHIME members are among the nation's foremost health IT experts including cybersecurity. Launched by CHIME in 2014, AEHIS represents more than 500 chief information security officers and provides education and networking for senior IT security leaders in healthcare.

Background

On February 12, 2013, the President signed Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," which is aimed at increasing the level of core capabilities for the nation's critical infrastructure to manage cyber risk by focusing on three key areas: (1) information sharing, (2) privacy, and (3) the adoption of cybersecurity practices. It further called upon NIST to lead the development of a framework to reduce cyber risks to critical infrastructure (the "Cybersecurity framework"). On February 12, 2014, NIST published the first step in meeting this piece of the Executive Order. Through this RFI NIST seeks feedback on different ways the framework is being used to improve cybersecurity risk management, how best practices for it are being shared, the relative value of different parts of the framework, the possible need for an update of the framework, and options for the long- term governance of the framework. This information is needed in order to carry out NIST's responsibilities under the Cybersecurity Enhancement Act of 2014 and the Executive Order.

According to NIST, "The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The framework consists of three parts: the framework core, the framework profile, and the framework implementation tiers. The framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors, providing the detailed guidance for developing individual organizational Profiles. Through use of the Profiles, the Framework will help the organization align its cybersecurity activities with its business requirements, risk tolerances, and resources. The Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk."

General Reflections

CHIME and AEHIS applaud NIST for updating the cybersecurity framework (hereinafter referred to as the framework). From a healthcare perspective, cybersecurity concerns continue to mount as more patient information is not only stored electronically but is also moving across the healthcare system and new threat actors emerge. Our members highlight NIST's activities and framework as one piece of a larger effort around risk management, but they would caution this is not a full solution for addressing it.

Need for Clearer Guidance for Healthcare Providers

One of the challenges is the lack of true guidance on what entails risk analysis and risk management. Even with the Office for Civil Rights (OCR) desktop audits and resolution agreements, and updates from the Office of the National Coordinator for Health IT (ONC), it is still unclear to providers how much "is enough?" Providers are left with the impression that what they are doing is enough until they are breached and it was retroactively determined it was not enough. They further note ongoing challenges within the healthcare community at large and within their own organizations to devote more effort to manage IT risk and in particular security-related risks in the wake of competing priorities and resources. Healthcare providers are also challenged by the fact that there is no unified and complete set of federal requirements on what constitutes good cyber hygiene.

Maturity Model

As is discussed later in the document, several of our members agreed that while NIST notes that the framework is not a "maturity" framework that is actually how providers tend to use it. We believe this should be remedied and adopted as a maturity model so that providers have a common lexicon for benchmarking themselves amongst one another.

OCR Requirements of Healthcare Providers

In many cases our members report that the demands placed on them by OCR within the U.S Department of Health & Human Services (HHS) - which has jurisdiction over the Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules - to protect patient's information has required them to devote resources and effort to meet requirements that may not result in better protections against cyber threats. An example of this is a recent resolution agreement between a provider and OCR. In a press statement about the resolution OCR noted, "All too often we see covered entities with a limited risk analysis that focuses on a specific system such as the electronic medical record or that fails to provide appropriate oversight and accountability for all parts of the enterprise." From our perspective this implies that all systems are in scope for individual risk analyses rather than enterprise, business level risk analysis and targeted (sample) system risk analysis being considered adequate. Statements made at the recent Food and Drug Administration (FDA) public workshop on medical device security pointed to this as well when an OCR representative described a resolution agreement where a HIPAA covered entity failed to "conduct a thorough risk analysis on a specific MRI system and associated workstation." CHIME and AEHIS are concerned that this level of compliance is unachievable without sophisticated and automated tools, when considering the typical large health system that operates hundreds, if not thousands, of information systems. This is a costly proposition and thus might not be available to all organizations.

Protecting Against Cyber Threats Goes Beyond Providers as Covered Entities

Our members report that while they can do their best to mitigate cyber threats, it becomes a challenge to the overall system when other actors remain unwilling and are not required to adopt similar controls. For instance, HVAC companies, third party technology companies that argue they are not a business associate as a result of the "conduit exception," and other business-to-business partnerships that providers must manage make navigating the compliance landscape challenging. Further, small practices acquired by larger health systems struggle immensely with this, and, as they get integrated into the system, they become weak spots and points of entry. Providers also face challenges with medical equipment (i.e. infusion pumps and MRIs), which is often kept for much longer periods of time than traditional information systems. This equipment must be connected to other systems so the data from it can be shared, however, these older devices were not developed with similar security standards as today's information systems. While we are not necessarily suggesting there is a NIST solution to these issues, we raise them to highlight the complexity of the healthcare landscape.

HITECH vs. HIPAA

Last, we would note that providers feel a "push and pull" in meeting both HIPAA and Health Information Technology for Economic and Clinical Health Act (HITECH). In order for healthcare providers to succeed in the evolving

healthcare landscape, the business must become digital. This means the patients' protected health information (PHI) must flow through the environment in a multitude of ways. The average large health system will send millions of transactions a day among systems which includes the data being downloaded, shared, and communicated with other entities. As data is moving providers feel challenged as they attempt to meet both HIPAA - which is aimed at ensuring patient information only gets into the appropriate hands – and HITECH - which attempts to create a more free flow of data. The end result is that healthcare providers find themselves devoting a lot of time to meeting the "letter of the law" enforcement activities. They find they must devote large amounts of resources dedicated towards compliance activities that by and large are not necessarily mitigating the cyber threats in order to provide justification for their decisions. Ultimately, this can leave the cyber threat unmitigated, which is part of the reason why the healthcare environment is behind in cyber threat management.

Risk Management Component to Authorization

We also wanted to also take the opportunity to highlight a persisting challenge raised by several of our members which is the need for a heavy risk management component to authorization; that is, who is the individual who is responsible for deciding what is an acceptable level of risk for an organization to take? While risk management goes beyond just cyber risk management, with the rise of cyber threats the need for a risk management framework within healthcare is taking on new importance. Today, risk management in healthcare organizations is typically based on general liability insurance. However, business risk is different from security risk and we are seeing security risks moving to the forefront. How respective technical, administrative and physical risks are accepted by a healthcare covered entity and put into practice is a concept that is generally missing within healthcare. Ideally, for healthcare organizations that have formulated executive risk management processes to adjudicate these items, if an event does happen, the process itself should provide a level of protection (i.e. safe harbor) against resolution agreements. OCR enforcement activities should be well defined and consistently applied across all regional OCR offices. Often, there is not a clearly defined business principal named to assume and accept any defined security risk on behalf of the organization. We raise this not because this is something we expect the framework to resolve, but rather to highlight the ongoing challenges in healthcare as providers navigate this space.

While we have provided detailed comments on the questions posed in the RFI in the next section, we offer our top recommendations below by highlighting the need for:

1. **More Education: More education and implementation guidance around the framework to generate greater awareness among healthcare providers.**
2. **Greater Certainty: Federal agencies involved with developing cyber and risk management guidance and overseeing compliance to work more collaboratively to provide more certainty for our nation's healthcare providers around the rules they must meet for whom the burden of protecting patients' PHI squarely falls.**
3. **Clearer Rules: A minimum set of compliance thresholds that providers can rely to be judged in compliance. This ideally would be developed by the industry with NIST support.**
4. **Balanced Compliance Approach: A balanced approach for monitoring compliance with risk management of cyber security is needed. The end goal should be to encourage providers to take steps that reduce their risks. This includes those who are just beginning to implement risk management or are confused by what they need to do, to providers with very sophisticated approaches. Organizations that can demonstrate they have taken good faith efforts implementing risk management practices should be given "safe harbor"' in the event of a breach. This will incentivize organizations to mature their practices, which in turn will lead to better security.**
5. **Better Guidance: NIST should work with the healthcare industry to develop guidance which is better aimed at helping larger healthcare providers protect themselves from cyber threats.**
6. **Adoption as Maturity Model: The framework should be positioned as a maturity model so that providers have a common lexicon for benchmarking themselves amongst one another.**
7. **Acknowledge Adopters: NIST should work closely with the Department of Homeland Security (DHS) and HHS to create a mechanism to acknowledge providers who have adopted the Framework.**
8. **Reorder Framework: Re-order pieces of the framework for a better flow as detailed under Questions and Answers 11 and 15.**

Responses to Specific Questions

Below are our responses to several of the questioned posited by NIST in the RFI.

#3. If your organization(s) uses the framework, how do you use it? (e.g., internal management and communications, vendor management, C-suite communication).

Our members recognize NIST is an integral partner as they act to deploy risk management strategies and they regard the framework as a good set of references. The framework is good at helping a provider to understand the current state of risk and targeting the desired end state at the programmatic level. However, it is not the answer for (nor should it be) the specific details of what is entailed to carry out activities needed to achieve the end state. While NIST notes that the framework is not a "maturity" framework that is how providers tend to use it. We believe this should be remedied and adopted as a maturity model so that providers have a common lexicon for benchmarking themselves amongst one another. Therefore, our members find that the framework is helpful to a degree but that in order to manage risk they must look elsewhere to locate actionable steps they can take to protect against cyber threats.

Furthermore, the framework is not universally known across the healthcare industry. CHIME and AEHIS strongly recommend the need for more and continuing education around the framework. We recommend that specific education be focused on NIST 800-171, NIST 800-39, SP800-66; Part 3, 800-100 in addition to 800-53 as it applies to healthcare covered entities. Specifically, we recommend NIST work with HHS to develop federally-recognized mappings back to HIPAA/HITECH. Implementation guidance should be created and should be succinct; NIST documents tend to be long and complex which makes it difficult for providers to determine how best to implement them.

#5 & #6. What portions of the framework are most useful and which are least useful?

The framework, when initially developed was done with the notion that this could be one that any number of industries could use. While the intent was to be industry agnostic, we believe that modifications are needed to be appropriately applied to healthcare.

- **Mappings:** Our members report the mapping that was done for categories and references in the core document is helpful.
- **Missing Areas:** Our members identified Payment Card Industry Data Security Standard Version 3 (PCI DSS) and the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27001 and 27002: 2013 as examples of areas that are missing and need to be addressed in the framework.
- **Profiling:** We received feedback that the profiling piece in the model is helpful as it can help providers benchmark their programs against others.
- **Data at Rest:** One area identified as a priority was the need for NIST to begin developing actionable steps providers can take for protecting data at rest rather than just pointing to the need for data to be protected. For example, multiple encryption models exist, including disk encryption, database encryption, table encryption, column level encryption, and row level encryption. Depending on the threat scenario being managed, certain encryption models do not add any protections. In the case of a hacker accessing a workstation through malware, full disk encryption provides no protection against access of the data as this encryption model only mitigates the threat of loss and theft of the device. However, OCR continues to make general statements that because "encryption was not enabled," a breach was achieved. This leads to confusion in the industry in adoption and implementation of the right control to the right threat.
- **Tiers:** The tiers are very useful for all cybersecurity programs to measure against whether a small provider's office or large health plan and partner practices (as long as they have staff who understand them).

#7. Has your organization's use of the framework been limited in any way? If so, what is limiting your use of the framework (e.g., sector circumstance, organizational factors, framework features, lack of awareness)?

NIST notes in this document, "The Framework enables organizations… to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure." In order for our members to better leverage use of the framework, they have highlighted the need to have a better understanding of how this document's efforts to help with risk management relate to other NIST risk management guidance. Some of the NIST documents have extremely detailed steps and are complex in their own right (I.E. 800-30 which is 95 pages with 11 factors to consider for every risk being evaluated). OCR has made statements that a provider apply 800-30 for every asset, or business process that sends PHI. As stated earlier, when a typical large health system maintains hundreds or thousands of information systems, this level of specificity is costly and not scalable in the digital age.

While the HIPAA security rules calls on providers to address technical safeguards, it does not outline for providers in any detail what actionable steps should be met, choosing instead to take a more flexible approach that allows providers of different sizes to scale their approach to their specific needs. While this does provide flexibility particularly for smaller providers, it also creates a lack of certainty especially for larger providers regarding how best to mitigate risk. The security rules point to certain NIST guidance documents (i.e. SP 800–30, 37, 39, and 53), however, HIPAA does not offer prescriptive approaches for managing risk. Without a set of concrete steps, providers believe there is a level of uncertainty that leaves them vulnerable to audits and significant financial penalties. For instance, when conducting a risk analyses at the Tier 1 or Tier 2 levels, as defined within 800-39, a provider can be penalized if they experience a breach because the system in question might not have been evaluated at the Tier 3 level.

#8. To what extent do you believe the framework has helped reduce your cybersecurity risk?

As is discussed elsewhere in our comments, CHIME and AEHIS believe that the NIST framework is helpful. However, they also believe that providers need more detailed guidance in order to not only operationalize risk management threats and keep patient information secure, but to ensure providers are best positioned to successfully withstand an audit.

#9. What steps should be taken to ''prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes'' as required by the Cybersecurity Enhancement Act of 2014? 7

CHIME and AEHIS recommend more alignment within the federal government in applying risk management principles. Today, there is a level of inconsistency and variability among the way federal agencies approach cybersecurity which in turns presents challenges for provider compliance. For instance, OCR may point to a NIST protocol, but the protocol gives optionality. The guidance OCR offers on encryption is one example. In one location online, OCR notes that the provider is not liable for data that is intercepted electronically when the patient asks for the information to be shared in an unsecure manner. On the other hand, OCR separately notes online that valid encryption processes for data in motion are those which comply, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140-2 validated.

We recommend that the federal agencies involved with developing guidance (i.e. NIST) or have other key roles (i.e. ONC and FDA), together with those auditing providers (i.e. OCR), work collaboratively to provide more certainty around what constitutes compliance. This is important for our nation's healthcare providers for whom the burden of protecting patients' PHI falls squarely as HIPAA covered entities. We also believe that monitoring compliance with risk management of cybersecurity requires a balanced approach. On the one hand, providers acting in good faith should be shielded from punitive audits while auditors are still able to root out real issues with compliance and negligence. Further, recognition is needed that smaller, less-resourced entities will not have same capability to meet threats as larger, well-resourced ones. In short, we continue to be very concerned with the way HIPAA enforcement is being applied and the effort of compliance needed to meeting the rules which in many cases are detracting from providers' ability to combat cyber threats.

10. Should the framework be updated? Why or why not?

While CHIME and AEHIS support updating the framework to address current deficiencies (see responses to questions 5 and 6), it is more important to have clear and actionable guidance for use by providers in operationalizing cybersecurity risk management. Without a single "source of truth" providers continue to feel

hampered in their compliance and confused by what standards they are being held to. Ideally, these guides would be developed by the industry. However, as we will discuss in more detail below, CHIME and AEHIS recommend NIST work with the industry to come up with implementation guides for each industry when a second edition of the framework is released.

#13. Are there approaches undertaken by organizations—including those documented in sector-wide implementation guides—that could help other sectors or organizations if they were incorporated into the Framework?

Our members do not believe the NIST framework should incorporate sector-specific guidance.

#14. Should developments made in the nine areas identified by NIST in its framework-related ''roadmap'' be used to inform any updates to the framework? If so, how?

The NIST Roadmap for Improving Critical Infrastructure Cybersecurity's (February 12, 2014) nine areas for development, alignment, and collaboration include: authentication; automated indicator sharing; conformity assessment; cybersecurity workforce; data analytics; federal agency cybersecurity alignment; international aspects, impacts, and alignment; supply chain risk management; and technical privacy standards. CHIME and AEHIS recommend that NIST publish Version 2.0 of the framework, however, more importantly, they work with the industry to come up with implementation guides for each industry. We believe this is the best approach for helping organizations work with their leadership to achieve compliance; organizations' top leadership needs information that is easily understood by non-cyber experts. Those operationalizing the framework need specific guidance on how to achieve this.

As noted earlier, many believe that there are no agreed upon set of requirements that a healthcare provider must meet in order to be deemed in compliance with federal requirements around comprehensive risk management. While OCR and ONC have both published information on performing risk assessment, what is available and is widely viewed by many healthcare providers (especially larger ones) as being inadequate. As one member says, it is "very hard to take these things and implement them and say you are airtight," since the current federal guidance is incomplete. Furthermore, the challenge is magnified by the fact that this framework is built upon existing standards where the industry lacks adequately granular guidance. This has created a layered affect whereby providers are attempting to meet a series of requirements built upon one another where each layer lacks a sufficient amount of detail on how best to operationalize. A sentiment expressed by another member was that the further you get into trying to meet risk assessment mandates the more nebulous and complicated they become.

Nonetheless, our members recognize that OCR and ONC have tried to respond to this clamor for additional information such as through development and publication of the self-risk assessment (SRA) tool. Unfortunately, this is largely perceived as being designed for smaller organizations and regarded by large providers as primitive. Providers continue to feel challenged by the limited guidance released by OCR and ONC as they seem to scratch the surface, leaving many larger providers feeling vulnerable to cyber threats. Additionally, the absence of a comprehensive generally agreed upon set of security principles and framework standards leaves the healthcare landscape incredibly varied and thus introduces major risk due to the variability.

In conclusion, our members recommend NIST work with the healthcare industry to develop healthcare specific guidance.

#11 & #15. What portions of the framework (if any) should be changed or removed? What elements (if any) should be added to the framework? And, what is the best way to update the Framework while minimizing disruption for those currently using the framework?

NIST lays out a seven step process for "Establishing or Improving a Cybersecurity Program" (Section 3.2). Step 1 calls for prioritizing and addressing scope. Step 2 calls for orienting what related systems and assets, regulatory requirements, and overall risk apply to the identified scope. Step 3 calls for creating a current profile. Step 4 calls for conducting a risk assessment. Step 5 calls for creating a target profile. Step 6 calls for determining, analyzing and prioritizing gaps. Step 7 calls for implementing an action plan. We believe there could be some confusion around how the framework was laid out. Some could be reviewing it as though it is a linear document. Upon reflection we do not believe that was NIST's intent. We welcome clarification on this point and urge NIST to articulate more clearly which steps should be taken in which order. CHIME and AEHIS recommend NIST make the following changes:

1. Make section 3.2 “Establishing or Improving a Cybersecurity Program,” which includes the seven-step model, the first activity in using the framework. We believe that a framework core is a tool for characterizing an existing cybersecurity baseline and can’t be populated until you have gone through the process necessary to create a “current profile.”
2. Flipping steps 3 and 4 around under Section 3.2. The framework calls for developing a profile (Step 3) followed by conducting a risk assessment (Step 4). We believe that a profile is better arrived at after a risk assessment has been performed since performing a risk assessment is a broader task and requires taking into account all areas of potential risk; not just those involved in the framework.
3. The information gleaned from the first three (3) steps - prioritizing (Step 1), orienting (Step 2), and creating a profile (Step 3) - should be used to populate the information in the framework Core (Section 2.1), a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors (functions, categories and subcategories) which becomes the repository for establishing the Current Profile (Section 2.3). The Target Profile, as referenced in the Implementation Tiers (Section 2.2), can now be determined predicated on things like risk-tolerance, business drivers, regulatory compliance, etc.
4. Once the Target Profile is determined, a gap analysis should be done to determine how to move from the “as-is” state to the “to-be” state. This results in key tasks that can become a strategic IT risk roadmap that can be accomplished over time based on available resources and finances.
5. Further detailed examples of the programmatic action plan to achieve the Target Profile.
6. Creation of a step 8; measurement and metrics. There should be a common method for measuring the difference between Current, Target state, and the progress towards achieving the Target state. Providing consistent metrics will help organizations benchmark their progress, and add clarity to the path forward.

#16. Has information that has been shared by NIST or others affected your use the framework? If so, please describe briefly what those resources are and what the effect has been on your use of the Framework. What resources, if any, have been most useful?

Pursuant to comments made earlier, providers are challenged by finding a “complete” solution to address cybersecurity risk management today. Many providers are using NIST as one part of an overall solution to addressing cyber security threats. As one member reported, that they had been using the NIST framework, however when they were audited by OCR they were given specific interpretation by the OCR that the framework had not been implemented comprehensively enough and thus was insufficiently deployed to meet their security needs which led them to a more comprehensive private industry tool and one developed by ISO. Another member reported that many providers use NIST to help them meet certain pieces of risk management for cyber security, however, they feel challenged as it is not regarded by many as sufficient to meet all of their needs. Another member reported that they use a different framework than NIST’s to attempt to achieve compliance, however this member noted they look to the NIST framework to measure their maturity.

#17 & #18. What, if anything, is inhibiting the sharing of best practices and what steps could the U.S. government take to increase sharing of best practices?

There is a belief that healthcare providers are not talking about what they are doing to comply because they are concerned they are missing something or are out of compliance. They fear that sharing information could put them at risk for an audit or lead to reprisal from OCR. Further, there are vendors and consultants who are helping providers protect themselves against cyber threats, but are concerned that by sharing information that those intent on carrying out a cyber event will use this as an opportunity to do so. This lack of transparency makes the selection of tools and processes more difficult as providers look to find both appropriate frameworks and solutions. The lack of safe harbor provisions for best practice implementation and good faith efforts has also lead to a mentality among healthcare providers that has paralyzed them with fear and given the variety of interpretations to the NIST framework by regulatory agencies; the risk of not moving forward is less than the risk of potential misstep.

19. What kind of program would help increase the likelihood that organizations would share information about their experiences, or the depth and breadth of information sharing (e.g., peer-recognition, trade association, consortia, federal agency)?

We believe there needs to be a way to safely share information such that it does not incur added federal scrutiny, but instead is used to foster spreading information that can be used to further best practices and thwart cyber security threats. Further, our members recognize the importance of healthcare providers working together to share best practices and information on how to best safeguard patient information. To that end recognizing those providers who are leaders in their field could be helpful.

NIST should work with HHS and DHS to highlight best industry practice (i.e. wall of fame). Also, providers should be encouraged and incentivized to participate with their ISACs or ISAOs. In some cases the cost to join these information sharing communities can be prohibitively high; we recommend that subsidies be provided to increase participation and thus increase cyber security practices across this industry.

20. What should be the private sector's involvement in the future governance of the framework?

Many of our members are deeply concerned with frameworks that require a "pay to play" model and urge that any work NIST undertakes be done in a manner that is transparent and inclusive. While there are some private models that can be useful, they often come with hefty price tags hampering the ability for smaller providers to have access to these tools. Further, some expensive tools simply consist of existing public resources. The healthcare sector is further challenged by the critical importance of the data that must protect as well as the extensive list of technologies that support life safety functions such as patient monitors etc.

CHIME and AEHIS believe that there is a critical role for the private sector. We urge a public and private partnership is critical to help ensure providers of all sizes are able to further their risk management strategies. We recommend that NIST also pay particular attention to fostering an environment through its engagement with other federal stakeholders that moves away from the current environment where cyber risks are passed off to providers who in turn shoulder the entire burden under HIPAA as noted earlier. This includes working with the FDA and OCR to recognize that protecting against cyber threats is a shared responsibility.

Further, in order to move greater maturity in healthcare cybersecurity, engaging the private sector to help fill in the "gaps" on where more guidance is needed is crucial. Providers will be less willing to take certain actions if they feel they are not a partner in establishing what needs to be done and there is a "punitive" mentality. While providers are desperate for more granular guidance on the *minimum steps* to operationalize their risk management plans the appropriate balance must be struck such that being overly prescriptive does not have the opposite intended affect and innovation is stifled. One member reflected that his organization's privacy officer insisted that HIPAA calls for "use of passwords" and thus facial recognition was not permitted. Having specific technical and administrative guidance on what constitutes the minimum set of requirements for compliance will reduce the ambiguity for providers. Another member reflected that the providers really need "guardrails" and the issue with the lack of clear guidance for providers is a "really broken issue."

#21, #22, & #23. Should NIST consider transitioning some or even all of the framework's coordination to another organization, what might be transitioned, and what kind of organization could it be transitioned, and could it be self-sustaining?

We believe it would be acceptable to consider use a 3rd party to assist in updating the framework or transitioning the document in whole. However, we recommend NIST remain involved and that more discussion is needed prior to this occurring. At a minimum if this work is moved outside of NIST it must be done in a manner that has balanced industry representation. And, we strongly recommend against transitioning to a for-profit entity or a not-for-profit entity lacking strong governmental oversight.

Conclusion

CHIME and AEHIS appreciate the opportunity to comment and lend our perspective to the important work being done by NIST. We look forward to continuing to be a trusted stakeholder and lending our perspective on mitigating cyber security threats. Should you have follow-up questions to our comments please contact my staff Mari Savickis, Vice President, Federal Affairs at msavickis@chimecentral.org.

Russell Branzell, FCHIME, CHCIO
CEO & President, CHIME

Marc Probst, CHCIO
Chair, CHIME Board of Trustees
CIO, Intermountain Healthcare

Deborah Stevens
Chair, AEHIS Board of Trustees
CSO, Tufts Health Plan