From: **Mari Savickis** <msavickis@chimecentral.org>
Date: Mon, Apr 10, 2017 at 12:51 PM
Subject: CHIME / AEHIS Comments on NIST Cybersecurity Framework draft
To: "cyberframework@nist.gov" <cyberframework@nist.gov>

Attached, please find CHIME & AEHIS' comments on NIST's draft Framework. Please let me know if you have any questions.

Mari

Mari Rose Savickis, MPA
Vice President, Federal Affairs
College of Healthcare Information Management Executives (CHIME)
20 F Street NW, Suite 700 | Washington, DC 20001 | 202.294.3828

[Attachment Below]

April 10, 2017

Kent B. Rochford, PhD
Acting Director
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Dear Acting Director Rochford:

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 Comment (RFC), “Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity,” (hereafter referred to as the Framework) published in the Federal Register on January 27, 2017.

CHIME membership consists of more than 2,300 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 almost 600 chief information security officers and provides education and networking for senior IT security leaders in healthcare. CHIME and AEHIS offered comments to NIST in 2016 on the previous Framework draft and are pleased to see that NIST took many of our suggestions into consideration for the current draft. Our members are generally supportive of the NIST framework, the seven step process that has been laid out, and NIST’s efforts to seek stakeholder feedback to improve upon the existing Framework. Below, we have offered comments on eight different areas, as well as answered the questions specifically posed by NIST (see Appendix).

To summarize our discussions and feedback, there is a strong unified desire for a “common” or “standard” accepted framework with a corresponding standard model to measure maturity and compliance. The current model with many frameworks and models for measurement is resulting in inconsistent and incomplete risk assessments with inconsistent remediation. Today, Healthcare is using NIST, International Organization for Standardization (ISO), the Health Information Trust Alliance (HITRUST) and Control Objectives for Information and Related Technologies (COBIT). This issue of inconsistency in standards and measurement is forcing Healthcare providers to seek multiple certifications resulting in higher Healthcare costs and fractured security models. Some organizations are verifying security using, HIPAA, 27001:2013, SSAE-16, SOC 1, SOC 2, FISMA, PCI, FedRAMP, FedRAMP+, or HITRUST. The objective of a common framework should be to create a standard goal or target and to improve the cyber infrastructure and resiliency. In practice, the confusion surrounding frameworks and guidelines is creating misdirection, increased cost and resulting in inconsistent treatment of security risk and remediation.

I. Terminology Used in the CSF and Maturity Models

At the outset, we'd like to draw a distinction between cybersecurity compliance and cybersecurity maturity, as the two are vastly different concepts. Compliance, from a healthcare perspective, is intended to depict whether an affected entity is meeting the privacy and security standards either under the Health Insurance Portability and Accountability Act (HIPAA) as outlined by the U.S. Department of Health & Human Services' (HHS) Office for Civil Rights (OCR) or under the Post-Market Management of Cybersecurity in Medical Devices as outlined by the Food and Drug Administration's (FDA). On the other hand, maturity refers to the journey an entity takes to continually evaluate risk, measure and benchmark implementation, and improve their cybersecurity posture. While compliance measure completion of a task, maturity measures processes, policy, ongoing measurement of the implementation and efforts to provide continuous improvement.

There is some confusion within the industry if the Framework is intended to serve as a maturity model. Despite NIST explicitly stating that the Framework is not intended to be used as a maturity model, many of our members still perceive that it as such. Several other members believe NIST's framework is aimed more at describing the "what" rather than detailing the "how." Meaning, the Framework allows a provider to secure their network without detailing how it has done so. This framework or architecture-only perspective has resulted in a level of abstraction that leaves out many critical implementation details, and has caused some to adopt other frameworks or standards that are more prescriptive. The NIST document communicates that this is a framework / architecture conveying "what" needs to be done. It also communicates that the Framework CSF is not a process (the "how") and is not a "maturity model" (the "continuous process improvement" dimension).

We recognize NIST's desire to allow for sufficient flexibility with how the document can be used by a variety of entities in different industries, but we believe the healthcare industry also needs more detailed information to strengthen the resilience of our healthcare infrastructure. At this time, we believe use of such tools should continue to be voluntary, however, we recognize the utility in consistent use of the Framework across the industry and envision widespread use to be highly desirable. We do not wish to see the Framework become yet again another "controls checklist."

Recommendations:
1. NIST should include a recommended information risk management process (e.g., NIST SP800-39, -30, -37, etc.) in the Framework.
2. NIST should develop a maturity model using resources already in existence today which could serve as a foundation for this. Two examples of this include: The Program Review for Information Security Management Assistance (PRISMA), a NIST-developed tool based on NIST guidelines and other recognized security best practices; and, the Capability Maturity Model Integration (CMMI) developed by Carnegie Mellon.

II. A Standard for Measurement

A common concern from our membership is the need to consistently measure a provider's cybersecurity readiness. There is significant variability in how healthcare entities currently measure their cyber security readiness / hygiene.

Our members are very concerned with the effect that a lack of a measurement standard has on both compliance and actual program performance, present and future. Understanding the standard for measurement is extremely challenging for healthcare entities when they perform risk assessments and when they get audited because there is no clearly delineated standard. Providers find this type of environment not only unfair, but increasingly challenging as cyber threats increase. Moreover, the way an entity perceives how well they are doing as compared to how OCR views them seems to vary substantially; many entities appear to think they are doing better than OCR thinks they are doing. One security expert we spoke with reported he has surveyed several of chief information security officers (CISOs) and it always astounds him that people assess themselves highly and then he speaks with OCR and they assess them at 1 or 2 with respect to a maturity scale of 1-5.

This ambiguity has more sophisticated organizations now measuring maturity and smaller organizations measuring compliance. Some are turning to third-party organizations for their certification of compliance that does not assess maturity and resiliency. Further, OCR does not recognize such certifications even as they relate to compliance. They state, "It is important to note that HHS does not endorse or otherwise recognize private organizations' certifications regarding the Security Rule, and such certifications do not absolve covered entities of their legal obligations under the Security Rule. Moreover, performance of a certification by an external organization does not preclude HHS from subsequently finding a security violation."

Using the NIST framework as a STANDARD by all healthcare entities, to advance cybersecurity efforts, to improve the healthcare infrastructure maturity and resiliency, and to facilitate better measurement across the healthcare sector from a compliance standpoint should be a priority. Naming the NIST standard for healthcare entities will bring more certainty, consistency, and will focus more attention on driving towards a stronger overall state of heightened readiness. We believe it is also worth noting that other industries (Maritime Bulk Liquids and Manufacturing) are already using the Framework as a standard and several have developed industry-specific implementations.

Furthermore, we believe that under no circumstances should commercial frameworks / certifications be mandated for use. Some are costly and many providers – even some of the more well-resourced ones – cannot afford these. Furthermore, many perceive a proprietary, commercial standard poses a conflict of interest. We detail our concerns with the use of certified products in greater detail later in our letter.

Recommendations:
1. Framework should be the named cybersecurity framework standard for use across the healthcare industry and entities should be encouraged to measure maturity using a preferred model from a recommended set of maturity models including PRISMA and CMMI.

2. As noted above, NIST should develop a maturity model using resources already in existence today which could serve as a foundation for this. Two examples of this include: The Program Review for Information Security Management Assistance (PRISMA), a NIST-developed tool based on NIST guidelines and other recognized security best practices; and, the Capability Maturity Model Integration (CMMI) developed by Carnegie Mellon.
3. While we recognize that NIST cannot dictate their framework as the named standard for healthcare entities, we urge NIST to continue working closely with HHS, OCR and the FDA to communicate these concerns and to push for a consistent standard.
4. Once the Framework is recommended as a standard, it should be regularly reviewed and updated based on implementation lessons learned through a continuous improvement process.
5. No commercial frameworks / certifications should be mandated for use.

<u>III. Guidelines for Industry-specific Adoption</u>

AHEIS and CHIME continue to believe that healthcare-specific guidelines for using the NIST framework are needed to best utilize and benefit from the use of the framework. We believe that the NIST crosswalk to the HIPAA Security Rule is very helpful, however, healthcare users also need guidelines for each function of the Framework (Identify, Protect, Detect, Respond, Recover) for each of these areas: policy, procedures, testing, and integration. One member noted that they struggle with cybersecurity testing, stating it's very hard to know whether your policies and procedures are effective. For example, if a hospital system has implemented encryption, it could argue that it's compliant with OCR's rules. However, by monitoring daily compliance with the encryption policy, one healthcare entity noted 7-8% of devices move in and out of encryption daily for maintenance, configuration and updates. Implementation of encryption in this use case is a compliance effort and could be reported as 100%, while the daily testing of compliance produces maturity and improves infrastructure resiliency by understanding, measuring, and monitoring deviation.

There are many similar examples of actual best practice implementation in healthcare that could improve the healthcare industry in a specific set of best practice guidelines for adoption and implementation.

Recommendations:
1. NIST, working in conjunction with affected stakeholders, should develop guidelines for use of their cyber framework for each industry, including healthcare. To help implement this recommendation, AEHIS and CHIME members, if required, are willing to volunteer to develop these guidelines for the acceptance and adoption by the healthcare industry.
2. NIST should continue to work with the critical infrastructure industries to develop implementation toolkits to support Framework adoption and productive use. We view NIST's sponsorship of the Cyberchain Initiative and the Baldrige Cybersecurity Excellence Builder, for example, as indicators that NIST recognizes this importance as well. Continued investment in this area, broadly and within each critical infrastructure industry, may serve to accelerate adoption, productive use, and initiate alignment with a maturity model that will increase the probability of achievement of the Framework's founding purpose as outlined in Executive Order 13636.

IV. Access Management

On page 32 of the redlined version of the draft Framework we note that NIST has added "identity proofing" to "access control." We strongly support this addition. In fact, the feedback we received was that there was too much attention placed on identity proofing and not enough on access management which continues to be a challenging issue for our members. We would also note that while the topic of minimum necessary is referenced in the training section of the report it needs greater attention in the actual Framework; it would appear that category PR.AC would be the appropriate location for additional content of this nature. More discussion and guidance on unauthorized access will be needed if the Framework is deemed the standard for the industry. Subcategories that should be included are: minimum necessary; privileged account management; role-based access; unauthorized access; and unauthorized activities.

Related to this, we also believe that there needs to be a discussion and guidance on privileged users. In the training section (page 33) there is discussion of users, though it is in the area of identity management. We believe more focus on identity management is warranted. Today in healthcare, identity management is fractured with the patient identity contained in the electronic health record, the employee identity contained in the Enterprise Resource Planning system, the member identity in the claims processing system, the affiliated Physician identity in the credential management system, consumer identities in the consumer portal. Most healthcare systems have identities spread through an average of 10-12 different systems. Guidance on identity management needs to include the critical need to have a master view of all identities and all the entitlements. Finally, we are unsure why NIST removed mention of concept of Separation of Duties (SOD), a common IT general control.

Recommendations:
1. Finalize the addition to the change which includes "Identity Management" along with "Access Control," and consider making Identity Management its own section.
2. Place more emphasis on the principles of minimum necessary including adding a subcategory on page 32.
3. Add a subcategory on "Privileged User" under the "Identity Management and Access Control" function.
4. Ensure there is crossover between what is addressed in the training section and the "Identity Management and Access Control" section.
5. Provide more background for users in both the Framework and ideally in a companion guide to expand upon the intent of this section as we believe many users of the Framework do not have a strong background in this area.
6. Retain the concept SOD.

V. Certification

Certification is another area of concern for our members. Some in the industry have argued that using a certification model could help with compliance efforts and with goal-setting. Others say it can also help with budgeting for cybersecurity. We understand these arguments, but we believe requiring certification is the wrong approach. We fear that requiring the use of a certification will result in a check-the-box mentality. Further, we fear if healthcare entities are required to use a certified cybersecurity tool, this will drive the end-state of compliance. To quote one member, “Cyber maturity should become the vision but if certification is where we start and end we will fail.” Another member also reflected on the concerns with a checklist approach stating, “It becomes difficult to explain to an auditor about why you are managing risk in a different way.”

Many experts raise concerns about certification programs such as the Payment Card Industry Data Security Standard (PCI DSS) requirement. In May 2016, the National Retail Foundation petitioned the Federal Trade Commission (FTC) in a letter and white paper raising concerns about “PCI, a proprietary organization formed and controlled by a single industry sector—the major credit card networks—that is not an open organization built on standard-setting principles recognized by the United States Standards Strategy (published by the American National Standards Institute, better known as ANSI).” The concerns raised in the letter and white paper sent to the FTC closely parallel concerns raised by healthcare CIOs and CISOs about a similar requirement in healthcare.

We also worry use of a certification could bring a false sense of security to healthcare providers and their patients. Certifications tend to be ‘snapshots’ in time; cyber risk management programs need to be ‘videos’ with a drive to continuously frame, assess, respond and monitor.

Recommendations:
Do not require a certification for the Framework or other frameworks or tools as this can have the unintended effect of driving compliance rather than maturity as an end state. Further, a certified tool would equate to “check the box” compliance mindset and undermine the holistic risk management approach in a dynamic cybersecurity threat landscape.

VI. Protecting Information Outside the “Four Walls”

Our members continue to express concerns with the growing challenges they face in securing patient information they deem outside their four walls and thus outside their control. For instance, with the growing reliance on a cloud environment, there is much that is outside the control of healthcare providers. Other industry dynamics such as the formation of accountable care organizations (ACOs), increased partnering, and the medical home models are demanding an increase in information sharing. This makes it difficult for them to identify, let alone protect, information assets not within their four walls. Providers have been pushed from a cost pressure standpoint to rely more heavily on cloud-based solutions, but in doing so they acknowledge that this has significantly challenged their ability to detect and respond to cyber threats.

Breaches of patient information that occur in these externa” environments can result in fines, reputational harm, and threats to patient safety. These threats will only grow as the healthcare system becomes more interconnected and dependent on connected devices and cloud storage. Some of our members have said they are experiencing challenges with some entities refusing to sign HIPAA business associate agreements (BAAs), placing in jeopardy a provider’s responsibility for shouldering compliance failures.

We also need to look no further than to some of OCR's most recent resolution agreements to appreciate the fact that providers - as HIPAA covered entities - have been saddled with the financial consequences of a breach that resulted from the implementation of inadequate safeguards by a business associate (BA). We acknowledge that some of these findings resulted from the covered entity not having a BAA in place, but the lack of such documentation was not the root cause of the breach and the presence of such an agreement would not have provided the covered entity any protection against the financial and reputational costs associated with the breach. Further, based on information published by the OCR or communicated informally throughout the industry, heavier fines on HIPAA covered entities as compared to BAs have been reported. Several of our members have reported they are addressing these concerns with their vendors, however, the regulatory environment continues, from our perspective, to be too lopsided. We continue to believe cybersecurity should be a shared responsibility.

Recommendations:
NIST should work with healthcare stakeholders and HHS to address how providers can respond to issues outside their control in a manner which embraces a culture of shared cybersecurity responsibility.

VII. Supply Chain Management

We appreciate the added attention NIST has placed on the supply chain area of the framework; this was something we recommended in our comments on the previous draft. That said, we believe additional changes, if made, will improve this piece of the Framework even more. Notably, we'd like to highlight the fact that there are several more relationships that are much broader than just the supply chain in the healthcare sector (and other sectors for that matter), and thus the scope of entities with whom users of the Framework are contending is indeed larger.

Additionally, there are many relationships that are not HIPAA-addressable or part of the supply chain but are still needed to understand the flow of patient information. An entity still needs to understand the flow of its patient information and all of the entities that are part of that "information sharing ecosystem" need to be aligned in their shared responsibility for protecting the data / information that defines that sharing relationship. If we adopt the de facto definition of "supply chain" particularly as it is operationalized in other industry sectors, we fail to capture what we believe was NIST's intent on introducing this new provision in the 1.1. release.

The other issue raised by our reviewers is many users will interpret this section as calling for the use of specific technologies which we do not believe should be the recommended approach. For instance, on page 31 of the draft under subcategory ID.SC-3 it says, "Suppliers and partners are required by contract to implement appropriate measures designed to meet the objectives of the Information Security program or Cyber Supply Chain Risk Management Plan." First, we worry that could be interpreted as requiring provider organizations to renegotiate business associate agreements down to a technology, or specific technical control level rather than at a control process level which we believe is far preferable. Second, this could foster a climate where healthcare entities are forced to be more prescriptive with their HIPAA BAAs.

To elaborate on this further, healthcare BAs have taken exception to even the most innocuous efforts on the part of covered entities to introduce clarifying language around “adequate security measures, controls or safeguards” in the BAA, often leading to significant delays in contract negotiations that impact healthcare operations and, at worst, patient safety. In addition, if the Framework calls for more prescriptive contract language, contracts and BAAs will need to be revisited with even greater frequency which is simply operationally burdensome and unsustainable. As one member reflected, it took fifteen months to address the specifics around a contract with a difficult supply chain partner. This BAA was at a control process level and not to the level of detailed technologies. Multiplied by hundreds or thousands of vendors this becomes unsustainable. And, as another member noted, they feel compelled to re-write existing contracts with their physician groups around service agreements as a result of a recent OCR settlement action.

Recommendations:
1. Expand the scope of the “Supply Chain Management Section” to reflect the wider array of parties with whom users of the framework are encountering who touch patient PHI.
2. Rename this section from “Supply Chain Management Section” to reflect the broader array of entities with whom users do business (i.e. “Relationships with Third Parties”)
3. Clarify the language to reflect that the intent is not aimed at defining the use of specific technologies in contracts.

<u>VIII. Incentives</u>

While outside the scope of NIST, incentives were discussed in Executive Order 13636, Section 8, paragraph (d): “(d) The Secretary (of DHS) shall coordinate establishment of a set of incentives designed to promote participation in the Program.” We feel it is important to raise the need for increasing incentives for driving better cyber resiliency, maturity and hygiene among healthcare entities. Harkening back to the need for a shared culture of responsibility for good cyber hygiene, we feel it is imperative that NIST work collaboratively with other federal agencies and departments like HHS and FDA, the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) to identify and promote ways by which healthcare providers and other healthcare stakeholders can be incented to make greater investments and get credit for work already underway to engage in good cyber hygiene.

Recommendations:
1. NIST should urge the Centers for Medicare and Medicaid Services (CMS) to include among its “Improvement Activities” under the Medicare-based Incentive Program (MIPS), credit for engaging in good cyber hygiene.
2. An interagency taskforce should be established to explore an entire suite of incentive options which could be leveraged by the healthcare sector.

<u>Conclusion</u>

AEHIS and CHIME appreciate the opportunity to comment, and acknowledge the great effort that is being made by NIST. We stand as ready and willing partners to help execute on the recommendations we have made and to participate in collaborative discussions and actions aimed at furthering a culture of shared responsibility when it comes to improving the cyber hygiene within the healthcare sector. Should you have any questions about our comments please do not hesitate to contact Mari Savickis, Vice President, Federal Affairs at.

Sincerely,
Russell Branzell, FCHIME, CHCIO
CEO & President, CHIME
Liz Johnson, MS, FAAN, FCHIME,
FHIMSS, CHCIO, RN-BC
Chair, CHIME Board of Trustees
CIO, Acute Care Hospitals &
Applied Clinical Informatics
Tenet Healthcare Corporation
Deborah Stevens
Chair, AEHIS Board of Trustees
CSO, Tufts Health Plan

APPENDIX – Sampling of Responses to the NIST Question Set

Response Legend:

- Response 1: Rehabilitation Provider (i.e. outpatient, skilled nursing, home care).
- Response 2: Security and HIPAA consultant whose customers are providers.
- Response 3: EHR vendor whose customers are providers.

<u>IX. Experience of our Members Using the NIST Framework</u>

We asked several of our members to provide us input on their experience with the NIST framework working off a short series of questions. Below are some excerpted quotes from members on their experience with the NIST Framework, as well as response to specific questions posed by NIST. As you will see, our members' use of the NIST framework varies widely.

Q1. Do you have a risk management framework in use?

Response 1: Our current program is homegrown and pieced together from multiple standards and frameworks. We are however considering a greater adoption of NIST framework."

Response 2: In a previous life, used ISO since we were a global organization. Today, our organization uses the NIST CSF in our own business and we assist organizations in adopting the NIST CSF through the proscribed 7- step process. It is important continue to differentiate the NIST CSF or any Framework from the cyber risk management Process. At the risk of oversimplifying, the Framework communicates WHAT needs to be done whereas the Process (think NIST SP800-39 and related documents) communicates HOW to do it.

Response 3: Yes.

Q2. Do you have a risk inventory?

Response 1: We do maintain a Security Risk Inventory that includes project prioritization, vulnerability assessment output and general concerns. Albeit not using a formal approach from any framework.

Response 2: Yes. A.K.A., Risk Register or Risk Rating Report. Developed per the HHS/OCR Guidance of Risk Analysis which in turn is based on NIST SP800-30.

Response 3: Yes.

Q3. Do you have a risk assessment?

Response 1: We do regular self-assessments that feed into our risk management approach and we do an annual 3rd party assessment focused on HIPPA, but using the NIST framework as the foundation of the assessment.

Response 2: Yes, as above. Developed per the HHS/OCR Guidance of Risk Analysis which in turn is based on NIST SP800-30.

Response 3: Yes.

Q4. How do you think the NIST framework is / could help you better manage your risk?

Response 1: It provides a comprehensive tool that helps to avoid paying too much attention in one area or missing an area of risk. The challenge is adopting it for our specific environment. At first glance is can be overwhelming, however it is more clear than many other frameworks. It's also a good foundation to establish a consistent view of risk and a common way to communicate. As it is more used within the organization as a communications tool, stakeholders will get used to it and start focusing on the content.

Response 2: In our experience assisting organizations in adopting the NIST CSF, one of the single biggest benefits is that it creates a common language for information / cyber risk management. This common language can serve all internal and external stakeholders. As one example, we've seen the quality of the conversations between the executive team/Board and the CIOs/CISOs improve dramatically. It expressly calls for senior management and Board understanding of cyber risk.

It is risk-based and not controls-checklist-based. It helps organizations understand that the challenge at hand is about saving their assets, not adopting someone else's checklist. The NIST CSF can also provide a standard measurement that organizations can use to measure risk and improve security Currently voluntary, but likely the de-facto standard in event of a breach.

Response 3: We are currently leveraging the NIST CSF version 1.0 for our security program. We are looking at what gaps there may be between our current risk framework, which is based off of ISO31000 with the security extensions in ISO27005, and NIST to determine if there are items that need to be adjusted or added.

Q5. Are there any topics not addressed in the draft Framework Version 1.1 that could be addressed in the final?

Response 1: No.

Response 2: I would like to see more coverage of the difference between the Framework and the Process (as above). Based on OCR data (Out of 47 Settlement Agreements/CAPs with 37 involving ePHI, 33 organizations (89%) have had adverse findings related to conducting a bona fide risk analysis), we know healthcare organizations are confused. I fear the "subcategories" will be used as yet again another checklist! I know NIST SP800-39 etc. are referenced under Authoritative Resources, but I think more needs to be done to emphasize and clarify the difference.

I would also like to have NIST address the matter of all threat source categories (accidental, adversarial, structural and environmental) as they do in NIST SP800-39 etc. The word cyber can be interpreted narrowly to mean only threats related to nefarious bad actors. Our job in information risk management must consider what amount to dozens of threats that roll-up under those four categories.

Version 1.1 continues to discourage the use of Tiers as an indication of maturity when, indeed, the Tier labels suggest maturity levels (Partial, Risk Informed, Repeatable and Adaptive). I would prefer to see NIST encourage the use of Framework Implementation Tiers or suggest / develop an alternative. I believe robust information risk management programs comprise three key components:

- A Framework – NIST CSF Core serves this need very well
- A Process – NIST SP800-39 etc. serves this need very well
- A Maturity Model – NIST CSF Framework Implementation Tiers could serve this purpose very well.

Response 3: I think this covers 2 key missing pieces of the framework. Supply chain risk management and metrics to measure effectiveness. Most mature organizations have implemented their own version of Supply chain risk management, but, having it tied to the NIST CSF can provide a level of structure that can be consistent across organizations. The challenge with the framework has always been around measurement. I think this is a good start to including that in the framework but feel it is still lacking some detail and clarity.

Q6. How do the changes made in the draft Version 1.1 impact the cybersecurity ecosystem?

Response 1: I think the addition of the SCRM section has the biggest impact. I'm not sure I like the "Supply Chain" nomenclature, but the concept of managing partner relationships better is critical to the cybersecurity infrastructure. For smaller entities, non-profits, and those with budget constraints, often outsourcing is the best economic option. Extending not only your supply chain, but extending your security operations outside the organization is critical to managing in these environments. Manage partner and vendor risk is one area that needs to be continued to be developed.

Response 2: The Cyber Supply Chain Risk Management (SCRM) expansion is a hugely positive addition affecting the entire healthcare ecosystem. This should be enable all stakeholders up and down and across the supply chain to use the same terminology, set mutually agreeable objectives around the Framework Core, the Tiers and the Profiles AND measure against these objectives.

This version 1.1 underscores the importance of building security into our services, solutions and information assets. To wit, “The Framework can be applied in design, build/buy, deploy, operate, and decommission system lifecycle phases.” It is very important for healthcare organizations to move from our current “Tactical-Technical- Spot-Welding” approach to a more “Strategic-Business-Architectural” approach.

Response 3: As I said above it may provide a level of consistency for SCRM and measures of effectiveness.

Response 4: Since this was just released they haven’t had a chance to incorporate this and they are waiting for final version to come out. Likes that they added supply chain and identity pieces.

Response 5: The business vernacular as opposed to being in the weeds – helps them be able to communicate better with their clients. And the communication goals also helped the CISOs she is working with; they are using some of the communications categories to bring empowerment to the CISOs that they don’t see in HIPAA. So better communication and relationships. Starting in late quarter of last year they started folding in Version 1.0.

Response 6: We adopted (NIST Version) 1.0 and have begun to makes changes to their organization to the 5 pillars - identify, detect, protect, respond and recover - in the past their focus has been on regulatory compliance which has not helped them from a maturity standpoint. He has a consultant to look at regulatory compliance vs their maturity.

Q7. For those using Version 1.0, would the proposed changes impact your current use of the Framework? If so, how?

Response 1: NA.

Response 2: Only to reinforce its use.

Response 3: For those using Version 1.0, would the proposed changes impact your current use of the Framework? If so, how? No real impact. We can leverage the SCRM and measures of effectiveness to compare against what we are doing today and determine the gaps and potential improvements we can make to our program.

Q8. For those not currently using Version 1.0, does the draft Version 1.1 affect your decision to use the

Framework? If so, how?

Response 1: I've already been a fan of the NIST framework, but just haven't gotten around to fully adopting it. The 1.1 update only enhances that further. The SCRM is probably the best addition. SCRM however makes it sound more industrial. Being in Healthcare, I would like to see this section be a little more generic and speak to partner relationships. From a supplier standpoint but also, BA's, staff augmentation, functional outsourcing of security operations, etc.

Q9. Does this proposed update adequately reflect advances made in the Roadmap areas?

Response 1: I believe it does, but it's trying to address a broad perspective. I'm wondering if there should be a variation by industry. A framework specific to Healthcare? Although our individual adoption does just that I suppose.

Response 2: Yes.

Response 3: I am not sure that it does but, it does start to address to major gaps in the framework.

Q10. Is there a better label than "version 1.1" for this update?

Response 1: I have no opinion.

Response 2: No specific thoughts.

Response 3: We do not feel the naming structure is a problem.

Q11. Based on this update, activities in Roadmap areas, and activities in the cybersecurity ecosystem, are there additional areas that should be added to the Roadmap? Are there any areas that should be removed from the Roadmap?

Response 1: I believe it is very comprehensive. The SCRM is a great addition but I would rename it to be more geared towards partner and vendor risk management and not make it so industrial.

The "Federal Alignment" section really reminded me that was originally geared towards the federal government and if the intent is to make this more widely used and adopted, maybe moving further away from Federal Government specific section would help.

Section 4 on Measures and Metrics is a great addition, however the table and the explanation lost me. I believe this is a great addition and VERY important, however it need to be more clearly explained. I would suggest taking another shot at rewriting that one.

Overall the additions are helpful and enhance the possibility of its broader adoption. Within healthcare, we need a standard beyond HIPAA, but as long as HIPAA is our minimum guiding principal for Privacy and Security, we are going to have to find the right marriage between it and the NIST framework. We will use 3rd party risk assessors to help with that over the next year and see if bringing in experienced consultants who have done that will help. The struggle is always, “How do you adopt a comprehensive framework on a budget with limited resources?”

Finally, we talked about government incentives. I think this is an important discussion to continue. Being Post- Acute, Not-for-profit and a growing company is the perfect storm for not having the resources to focus on Governance and Framework adoption. A little support and incentive would go a long way.

Response 2: I would like to see more coverage of the difference between the Framework and the Process (as above). Based on OCR data (Out of 47 Settlement Agreements/CAPs with 37 involving ePHI, 33 organizations (89%) have had adverse findings related to conducting a bona fide risk analysis), we know healthcare organizations are confused. I fear the “subcategories” will be used as yet again another checklist! I know NIST SP800-39 etc. are referenced under Authoritative Resources, but I think more needs to be done to emphasize and clarify the difference.

I would also like to have NIST address the matter of all threat source categories (accidental, adversarial, structural and environmental) as they do in NIST SP800-39 etc. The word cyber can be interpreted narrowly to mean only threats related to nefarious bad actors. Our job in information risk management must consider what amount to dozens of threats that roll-up under those four categories.

Version 1.1 continues to discourage the use of Tiers as an indication of maturity when, indeed, the Tier labels suggest maturity levels (Partial, Risk Informed, Repeatable and Adaptive). I would prefer to see NIST encourage the use of Framework Implementation Tiers or suggest / develop an alternative. I believe robust information risk management programs comprise three key components:

- A Framework – NIST CSF Core serves this need very well
- A Process – NIST SP800-39 etc. serves this need very well
- A Maturity Model – NIST CSF Framework Implementation Tiers could serve this purpose very well.

Response 3: Most organizations probably combine the activities around respond and recover. Most of these are so closely tied together that it may make sense to combine them into one section of the framework.

[i] HHS Website FAQs

[ii] Payment Card Industry Data Security Standards: Federal Standard-Setting and Competition Policy Concerns

[iii] https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructurecybersecurity