April 25, 2022

Laurie E. Locascio, PhD
Director of NIST and the Under Secretary of Commerce for Standards and Technology
The National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Submitted electronically via www.regulations.gov

Dear Dr. Locascio:

On behalf of the Healthcare Information and Management Systems Society (HIMSS), I am pleased to provide written comments in response to the Request for Information on Evaluating and Improving NIST Cybersecurity Resources. HIMSS applauds the work of the National Institute of Standards and Technology (NIST) in evaluating and improving its cybersecurity resources, to account for the changing landscape of cybersecurity risks, technologies, and resources.

HIMSS is a global advisor and thought leader supporting the reform of the global health ecosystem through the power of information and technology. As a mission-driven non-profit, HIMSS offers a unique depth and breadth of expertise in health innovation, public policy, workforce development, research, and analytics to advise global leaders, stakeholders, and influencers on best practices in health information and technology. Through our innovation engine, HIMSS delivers key insights, education, and engaging events to healthcare providers, governments, and market suppliers, ensuring they have the right information at the point of decision. Established in 1961, HIMSS serves the global health information and technology communities with focused operations across North America, Europe, the United Kingdom, the Middle East, and Asia Pacific. Our members include more than 115,000 individuals, 480 provider organizations, 470 non-profit partners, and 650 health services organizations across 86 countries.

We offer the following thoughts and recommendations for ensuring that the revisions to the Cybersecurity Framework include the valuable and necessary updates necessary to reflect advancements in cybersecurity and current threat landscape. Additionally, we encourage NIST to refer to "Appendix A" of this document for a list of recommended references that should be considered for inclusion within NIST's Online Informative References Program.

Usefulness of the NIST Cybersecurity Framework

The NIST Cybersecurity Framework ("CSF") is highly useful to healthcare organizations of all types, sizes, and kinds. The CSF is widely used by many healthcare organizations as a way for healthcare organizations to manage cybersecurity risk more effectively. The five functions of Identify, Detect, Protect, Respond, and Recover provides a practical outline for organizations to navigate data protection in cyberspace. Organizations should understand that this is a continuous cycle. Cybersecurity is not a "one and done" proposition, but rather a cycle of continuous improvement.

The cybersecurity landscape is quickly and vastly changing. Every organization has a different set of risks, risk tolerances, capabilities, and metrics. Many organizations of all types, sizes, and kinds can significantly benefit from information sharing with others regarding policy, business, and technological approaches to reduce cybersecurity risks.

Information sharing partners should include other similarly situated organizations, as well as others that may have more sophisticated, agile, and/or mature cybersecurity programs. It is vital for healthcare organizations to share information with peers, and others that may be outside of the relevant geographic locale. Additionally, information sharing should occur both in the intra-sector and inter-sector sense. There is much to learn from one's peers as one can learn from others, especially those either within or aligned with other critical infrastructure sectors. It is also vital to share information with upstream and downstream providers, business associates, and others. Of course, such information sharing should occur with vetted, trusted partners. It is also important for market suppliers to keep the channels of communication open with customers and partake in coordinated vulnerability disclosure programs.

Now, more than ever, there is a significant volume of cyber-attacks, whether from nation states, non-state actors, cybercriminals, hacktivists and others. Often, these cyber-attacks use simple and/or old techniques to infiltrate systems and networks. For example, a nation state sponsored group may use an old remote access Trojan that is well-known but highly effective because people are simply not patching systems and/or identifying and detecting potential threats.

According to the results of the 2021 HIMSS Healthcare Cybersecurity Survey, relatively few organizations are implementing a full complement of basic security controls. For instance, network monitoring tools may not be in place and so visibility into one's network traffic may be practically non-existent. Additionally, there are some healthcare organizations that are still not encrypting information, whether in transit or at rest.
If anything, the CSF should be expanded to include examples of how organizations can grow in their cybersecurity capabilities from one tier to another across functions. Some

steps may seem very basic, but granular guidance may be warranted especially for those organizations that need to significantly improve their respective cybersecurity programs. As such, it would be helpful to have additional guidance on how organizations can move from one tier to another to improve their capabilities with appropriate metrics and other tools.

Current benefits of the CSF

While there is no universally adopted framework, the CSF is one of the most implemented frameworks within the healthcare and public health sector. Our stakeholders have greatly benefited from adoption of the CSF. Consistent with the language of Section 405 of the Cybersecurity Act of 2015, now codified at 6 U.S.C. §1533, we recommend the CSF as the key element of the "voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes." As a result, many stakeholders are now moving away from a compliance-based approach to a holistic risk management approach to better address risks. The CSF has been a catalyst of change.

While we acknowledge other frameworks could be adopted to fit the healthcare and public health sector's needs, we recommend the NIST Cybersecurity Framework, the associated industry-led, collaborative efforts of the 405(d) program, and the best practices as recommended by US DHS CISA and HC3. We encourage all healthcare stakeholders to adopt and implement the CSF to help strengthen our collective security posture.

A significant challenge that many healthcare organizations face is ensuring that its business associates, other covered entities, market suppliers, health information exchanges, data aggregators and data trading partners are on the same page. Numerous breaches and security incidents have occurred due to inconsistencies in applied frameworks and associated practices. The CSF can be used to normalize these variations.

The CSF also provides a common language for healthcare providers, suppliers, vendors, and others to better manage cybersecurity risk. It can be used to communicate risk and serves as a reminder that the protection of assets and information is indeed a continuous improvement process. Indeed, the CSF can be used as a communication tool within organizations so that various stakeholders can more effectively communicate cybersecurity risks and assess and manage these risks. More effective and frequent information sharing is recommended within healthcare organizations and also peer-to-peer to stay ahead of threats and to keep educated and informed about evolving best practices.

The CSF should be based upon voluntary, industry-based standards, guidelines, and best practices and the CSF should be a voluntary tool for which industry can suggest improvements on a regular basis. Now is the time for healthcare and public health sector stakeholders to step up their efforts, especially in light of increasing asymmetric threats from within healthcare organizations and outside of organizations. Our healthcare and public health stakeholders must achieve greater information superiority regarding their systems, networks, and software and hardware components. Not only do we champion better technical practices, but also more effective governance and training of our cybersecurity personnel and the workforce at large.

Challenges using the CSF

The CSF is a voluntary, free tool that can be readily adopted and implemented by any type of organization. However, as previously noted, there are certain organizations that need more granular guidance (a "how to" if you will) in terms of implementing and adopting the CSF.

In terms of information sharing restrictions, one significant one is that legal counsel often restricts sharing of cyber threat indicator information between and among entities. But this is likely because the nature of cyber threat indicators may not be well understood. It is doubtful that there are laws and regulations that may restrict the actual sharing of cyber threat indicator information.

Changes, Additions, or Removal – CSF

The CSF should ideally be used as a tool for an organization to evaluate its cybersecurity capabilities, meaningfully communicate to others its cybersecurity capabilities, and, ultimately, better manage risk. Overall, the CSF can be a robust communication tool, but it should be understandable to both cybersecurity professionals and laypeople. Various forms of media (e.g., video, audio, visual illustrations, and otherwise) can be explored to enhance the understanding of those who wish to use the CSF.

Further, the CSF should more substantially address cloud computing, edge computing, phishing, and the protection of operational technology and information technology and operational technology assets. Given the current threat landscape and state of infrastructure, stakeholders should be more aware of intra-sector and inter-sector dependencies, in addition to assessing and managing risk within the organization. Ultimately, supply chain security should inform the scope of security risk assessments.

The Framework should also emphasize the importance of having an inventory of data, data flow, as well as IT and OT assets. It should also speak to the unauthorized use of shadow IT and how shadow IT can be a source of unnecessary exposure to risk. While the NIST cybersecurity framework profiles, such as NISTIR 8374 (ransomware), provide information on what the outcomes could look like based upon the business needs of an organization, it would be also helpful to have a visual illustration or mapping of this information and additional context.

Inventory

A significant challenge that organizations have is keeping an accurate and thorough inventory of IT, OT, and mobile device assets. This can be an impediment to conducting an accurate and thorough risk assessment. Further, many organizations do not have a complete picture of what data they have, who has access to it, and where the data flows (whether it is inside or outside of the organization).

Another challenge is knowing what is within these assets in terms of hardware and software components. To this end, the Framework should address the Software Bill of Materials ("SBOM"). Not only will the SBOM benefit those who may be procuring assets, but also those who manufacture and operate such assets. The SBOM will provide a greater degree of awareness in terms of supply chain security and integrity for all stakeholders. Indeed, we need greater transparency not only in terms of the software supply chain but also the hardware supply chain. While risk assessments may be the foundation of any cybersecurity program, knowing what you have is the essential footings of that foundation.

Often, stakeholders do not know what they have because of the lack of visibility into their inventory. For example, when WannaCry occurred, many stakeholders were unaware that they had assets at risk. With greater visibility into the supply chain, we will have better tools to assess and, ultimately, mitigate risk.

Governance

The success or failure of a cybersecurity program may depend upon how well it is governed. Cybersecurity should not exist in a vacuum (or otherwise in a silo) at any organization. This is why many cybersecurity programs fail – due to a lack of support from the organization. Leadership at the highest levels of the organization should be strong advocates of the cybersecurity program and they should be equally well informed. In healthcare, robust cybersecurity is needed to ensure patient safety, especially in our connected world.

The section of the CSF on governance of cybersecurity risk should be expanded to include stakeholders from all relevant departments and units. Cybersecurity should

always be a priority. Cybersecurity is indeed a shared responsibility and key stakeholders should be informed of what is happening and also be involved in the decision-making process, as appropriate. (Indeed, governance of cybersecurity risk should go way beyond privacy and security personnel.) All too often, cybersecurity programs are broken due to a lack of "buy in" from leadership and/or communication between or among key departments (such as human resources, legal, procurement, facilities, etc.).

Further, policies and procedures that are poorly crafted and developed – without multi-stakeholder input and buy-in – will likely fail. According to the 2021 HIMSS Cybersecurity Survey, compliance with policies and procedures is a significant challenge for many organizations. This is likely due to policies and procedures being out of date at the organization. Far too often, formal policies and procedures to do not reflect actual practice. Organizations often grant many exceptions to established policies and procedures, which leads to inconsistent enforcement and weaker security.

Finally, governance programs should address normal times and abnormal times (e.g., weather hazards, ransomware attacks, or otherwise); steps should be taken to establish a chain of command; and appropriate open channels of communication / information sharing within the organization must encouraged.

Identity and Access Management & Privileged Access Management
The CSF should be updated to include more of a focus on identity and access management as well as privileged access management. A weakness of many healthcare organizations is that accounts are not timely provisioned and de-provisioned, nor do these accounts necessarily ensure the appropriate levels of access (namely, least privileged access) for respective roles.

Identity and access management is not just a technical issue, but also a people issue. The human resources department may not necessarily be tightly integrated with the information technology department. Accordingly, access may not be revoked at just the right time – prior to termination of an employee, contractor, or other individual and/or entity.

Further, multi-factor authentication should be implemented whenever and wherever possible throughout the organization. Plus, multi-factor authentication technologies will evolve over time to incorporate more advanced factors, such as dynamic biometrics (e.g., voice, face liveness detection, etc.). Simply put, multi-factor authentication, which is now increasingly embedded within off-the-shelf hardware, should be part of every organization's identity and access management program.

Encryption

Encryption is also a topic that needs to be addressed within the CSF. Encryption, too, evolves over time. It is important for all organizations, including those in healthcare, to deploy encryption for data at rest, in transit, and archived data. Encryption is useless, though, if it can be broken. Factors for weak encryption include low entry randomness, weak keys, weak ciphers, and inaccurate time sources.

Even with robust encryption, however, poor key management can undermine strong encryption measures. It is important for all organizations to implement encryption key management best practices as well.

Zero Trust

The security of an organization is no longer at the organization's perimeter. Rather, with remote work, cloud computing, and the distribution of people and assets in geographically distinct places, the traditional network perimeter has ceased to exist. Zero trust is more adaptable to the modern workforce and the fluidity of the modern technology ecosystem, compared to traditional/legacy controls.

While zero trust technology is nascent to many organizations, it is best implemented when organizations have a strong foundation of security controls in place. This foundation includes robust identity and access management as well as robust encryption measures. CSF should include up-to-date information about zero trust technology. With zero trust, a breach is always assumed as opposed to the grant of unfettered access once a user (or application or device) has successfully authenticated.

Implementation Tiers

Given the velocity and impact of today's cyber-attacks, we believe that the implementation tiers should be revisited. While it may have been tenable previously to encourage organizations to walk before, they can run, it is generally advisable for all organizations now to strive for being Tier 4: Adaptive organizations. It is not enough for organizations to have repeatable processes. Rather, organizations must have adaptive processes so that they can indeed revamp their programs in light of the post-incident analysis and lessons learned.

Standards

Prospectively, too, Appendix "A" of the CSF should also refer to the cryptocurrency security standard ("CCSS"). Further, the CSF and/or collateral NIST documents should be updated to address blockchain and the security (and attendant risks) thereof.

Modifications or Changes to CSF and Impact to Usability or Backward Compatibility

From the inception, one of the greatest strengths of the CSF is that it has been acknowledged as a living, breathing document that will adapt and change with input and involvement from a wide variety of stakeholders. We encourage NIST to continue this approach.

To the extent that CSF is modified or changed, there should be a clear roadmap regarding such changes. In addition to specifying by way of text what has changed, it will be helpful to have a variety of ways to communicating the nature of such changes. For example, visual illustrations showing how the CSF has changed in whole or in part would be quite helpful, as well as videos and/or infographics regarding the nature of such changes and any other essential information.

Additional Pathways for Improvement

It would be helpful for NIST to publish successful use cases of organizations across all critical infrastructures – including in healthcare – regarding adoption and use of the Framework. Additional insights and know-how can be shared in terms of how organizations can advance in terms of the implementation tiers. Providing visibility into the organizations' adoption and use of the Framework during normal times and also times in response to significant security incidents would be most helpful to others. There should be an examination about how organizations of different types, sizes, and kinds deal with normal vs. abnormal scenarios.

Further, it would be helpful for each sector's use case to ask relevant assessment questions based upon relevant compliance requirements, industry guidance (e.g., NIST or otherwise), frameworks, and provide visual mappings to relevant standards and controls, such as ISO 27001 and 27002.

It would also be valuable for NIST to address how the NIST Cybersecurity Framework and NIST Privacy Framework can be used as complementary tools for managing privacy and cybersecurity risk at the enterprise level with the use of the catalog of controls from NIST Special Publication 800-53 Rev. 5. On another note, entities would greatly benefit from a more detailed understanding of supply chain risk management – not just simply cyber supply chain risk management.

Managing supply chain risk should start with the careful selection and vetting of the vendor. Too many organizations do not adequately select and vet the vendors whom they ultimately retain. As a result, vendors may be retained that have poor security postures and/or that may not have the financial wherewithal to be around in the long-

term. Appropriate business and technical due diligence are required to select the best vendor that can meet the business needs and requirements of the organization. Unfortunately, this aspect of the procurement process is often neglected and, as a result, the organization may be exposed to unnecessary risk. Vendors offering the lowest price and/or claiming benefits that may not be realized in practice might not be the best choice for the organization that is in search of a solution.

Cybersecurity risk is a complex, multi-dimensional problem. Indeed, our organizations do not exist in a vacuum. Healthcare organizations exchange information with multiple partners and depend upon many other critical infrastructure sectors to function. There is no other sector that is more vulnerable. The healthcare and public health sector has touchpoints to just about every other sector. Indeed, the lives and well-being of individuals depend upon the healthcare sector and safety is of the utmost importance. Accordingly, NIST would greatly assist the various critical infrastructure sectors, including the most vulnerable, by helping stakeholders with granular guidance on how to manage risk effectively in a multi-dimensional, highly dependent and interwoven world.

On a related note, while the subject matter of the CSF relates to, obviously, cybersecurity, organizations must also be prepared to address physical risks as well as technical risks. The CSF does address in a few places physical risk, but additional explanation would be beneficial, as robust cybersecurity also requires robust physical security.

Additionally, while CSF does lightly mention risk vis-à-vis people, it does not seem to mention insider threat. Insider threat is on the rise. Insider threat activity can be significantly more damaging than a cyber-attack. Many organizations do not have formal insider threat programs in place. Thus, insider threat is often left undetected until significant damage or harm has occurred. However, all organizations struggle with negligent insider threat activity and malicious insider threat activity is always a possibility. Accordingly, we recommend that a substantive resource on insider threat mitigation be provided to users of the CSF.

Moreover, although prevention of security incidents can sometimes be achieved, incident response plays more of a critical role than ever. Know-how from the National Incident Command System (NIMS)/Incident Command System (ICS) should be leveraged during incident response. The CSF should address resources from FEMA such as NIMS and ICS.

Finally, NIST has a bevy of useful resources and there are numerous other references as listed in Appendix A of the CSF. However, rather than having a laundry list of the various references, it would be helpful to have a visual guide to show how various components

of the CSF and the relevant standards and other guidance documents interrelate. These are indeed integral pieces of the puzzle, but unless we can actually see how the puzzle is put together this valuable knowledge is, at best, obscured.

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

It would be helpful to further integrate the Framework with NIST Cybersecurity Supply Chain Risk Management CSRM (NIST SP 800-161 Rev. 1 – Draft), Digital Identity Guidelines (NIST SP 800-63B), Guidelines for Media Sanitization (NIST SP 800-88), Securing Wireless Infusion Pumps in Healthcare Delivery Organizations (NIST SP 1800-8), Securing Picture Archiving and Communication System (PACS): Cybersecurity for the Healthcare Sector (NIST SP 1800-24), Securing Electronic Health Records on Mobile Devices (NIST SP 1800-1), Securing Telehealth Remote Patient Monitoring Ecosystem (NIST SP 1800-30), and An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (NIST 800-66 Rev. 1), among others. Several of these publications, however, have not been updated in several years and it is recommended that these publications be brought up to the present time given the current technology and threat landscape, as well as the present legal and regulatory environment.

Use of non-NIST frameworks or approaches in conjunction with the NIST Cybersecurity Framework

Other non-NIST frameworks, such as the Payment Card Industry Data Security Standard ("PCI DSS"), have been mapped to the NIST Cybersecurity Framework. In the healthcare and public health sector, the HIPAA Security Rule has been mapped to the CSF. Also, the HITRUST Common Security Framework has been mapped to the CSF.

Overall, it would be helpful to see, in more granular detail, about how other non-NIST frameworks, especially those for risk management, may be mapped to the CSF in practice. The CSF is an excellent means for helping organizations communicate their cybersecurity risks and expectations to their suppliers and other stakeholders. Risk management frameworks, however, are more granular and technical. To this end, it would be helpful to have sector-specific guidance on how to bridge this gap so that the security culture and practice of suppliers and stakeholders are aligned with the organization.

Updates NIST should consider regarding international use of the Framework

Use cases of stakeholders who implement the CSF both domestically and internationally would be helpful. Cybersecurity programs are informed by legal and regulatory requirements, as well as the current threat landscape and future concerns.

An opportunity for international engagement includes United States, along with Canada, Japan, the Republic of Korea, the Philippines, Singapore, and Chinese Taipei participating in the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) system. Notwithstanding legal complexities in cross-border data transfer, there needs to be a meeting of the minds in terms of the promotion of interoperability with other data protection and privacy frameworks, including CSF and the NIST Privacy Framework and, also consistent with the goals of the Global CBPR Forum, the periodic review of data protection and privacy standards to ensure that Global CBPR and Privacy Recognition for Processors (PRP) program requirements align with best practices.

Amplify Overall Awareness of the CSF to Encourage Stakeholder Engagement, Use, and Understanding of the Significance of the Updates

Good cybersecurity practices help ensure that data will remain confidential, have integrity, and be available on demand. Cybersecurity, a key responsibility of data stewardship, is a necessary predicate to data privacy, access, and usage. Data should be protected, not just to preserve privacy but also to protect the patient and maintain safety.

Recognizing the value of such data, we need to have robust cybersecurity policies and corresponding practices to ensure healthcare data interoperability. People, processes, and technology must work in tandem to facilitate data privacy. Therefore, there must be a more significant push to educate potential users on the NIST Cybersecurity Framework and its content.

HIMSS welcomes the opportunity to be a resource to NIST on innovative, forward-thinking steps to educate the public about the value of this its cybersecurity resources as well as how the broader healthcare community should think about better leveraging its content.

We look forward to the opportunity to discuss these issues in more depth. Please feel free to contact Lee Kim, Senior Principal Cybersecurity & Privacy at [redacted] with questions or for more information.

Thank you for your consideration.

Sincerely,

Harold F. Wolf III, FHIMSS
President & CEO

Appendix A - Recommended References That Should Be Considered for Inclusion Within NIST's Online Informative References Program

HIMSS Resource Guide on Cybersecurity in Healthcare
HIMSS Resource Guide on Blockchain in Healthcare
HIMSS Cybersecurity Frameworks Explained
2021 HIMSS Healthcare Cybersecurity Survey Findings
HIMSS Security Incidents in Healthcare Infographic
Phishing: Don't be Phooled!
A Lifeline: Patient Safety & Cybersecurity
Protecting and Defending Hidden Treasures

Cybersecurity & Infrastructure Security Agency (CISA): Insider threat mitigation resources
Cybersecurity | ASPR TRACIE
Health Sector Cybersecurity Coordination Center (HC3)
HHS 405(d) Aligning Health Care Industry Security approaches
Health Industry Cybersecurity Practices (HICP) Quick Start Guide
HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework
OWASP Top 10 Web Application Security Risks
Cloud Security Technical Reference Architecture
Known Exploited Vulnerabilities Catalog
DHS CISA Shields UpICS-CERT
International Medical Device Regulators Forum
Insider Threat Mitigation Guide
The Minimum Elements for a Software Bill of Materials (SBOM)
Vulnerabilities MITRE ATT&CK Framework
Ransomware Prevention and Response for CISOs