November 4, 2023

Laurie E. Locascio, Ph.D.
Under Secretary of Commerce for Standards and Technology and
Director, National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Submitted electronically to: cyberframework@nist.gov

Dear Dr. Locascio:

On behalf of the Workgroup for Electronic Data Interchange (WEDI), we write today in response to the publication on August 8, 2023, of the *NIST Cybersecurity Framework 2.0* and the *Discussion Draft: The NIST Cybersecurity Framework 2.0 Core with Implementation Examples*. WEDI appreciates NIST developing these important resources and providing an opportunity for stakeholders to submit public comments.

WEDI was formed in 1991 by then Department of Health and Human Services (HHS) Secretary Dr. Louis Sullivan to identify opportunities to improve the efficiency of health data exchange. WEDI was named in the HIPAA legislation as an advisor to the Secretary of HHS. Recognized and trusted in that role as a formal advisor to the Secretary, WEDI is the leading authority on the use of health information technology (IT) to efficiently improve health information exchange, enhance care quality, ensure confidentiality, and reduce costs. With a focus on advancing standards for electronic administrative transactions, and promoting data privacy and security, WEDI has been instrumental in aligning the industry to harmonize administrative and clinical data.

As we are all well aware, there has been an increase in the number and types of threats targeting health care and other critical sectors of the U.S. economy as cyber criminals are deploying more sophisticated techniques every year. At the same time, while organizations understand the need to deploy security resources that can reduce exposure and decrease the chance that patient data will be compromised, many entities, especially smaller ones, often operate on razor thin margins. Access to high-quality, actionable, security resources that can be deployed by organizations of all types and sizes is critical if health care and other sectors are to adequality protect themselves from cyber-attacks.

General comments

We applaud the NIST staff for their excellent work on the *Cybersecurity Framework 2.0* (CSF 2.0) and for the many other resources the agency has developed to assist critical sector organizations meet cybersecurity challenges. WEDI also commends NIST for engaging with the private sector and continuing to augment this important resource. For the health care sector, the CSF 2.0 represents the benchmark for those seeking to develop a comprehensive HIPAA security compliance program.

With the publication of this draft, NIST is seeking feedback to assist in evaluating and improving one of the most important cybersecurity resources publicly available to the health care industry and other critical areas of the nation's infrastructure. We will focus our comments on the opportunities NIST has to augment the contents and applicability of the CSF 2.0.

Inclusion of the Govern Function

We recognize the importance the integrating NIST's Privacy Framework and emphasis on people, processes, and technology are particularly significant improvements to the document. Most importantly, we strongly support including "Govern" into the Framework Core of the CSF 2.0. This Govern function highlights the significance of governance in overall enterprise risk management. For many organizations, effective governance policies form the backbone of a successful security framework that includes structure, transparency, and accountability. It ensures responsible decision-making and protects against potential cyber dangers. We do note, however, that while the CSF 2.0 discusses almost exclusively of Cybersecurity Risk Governance (CSRG) and Cybersecurity Risk Management (CSRM), these terms are never fully defined in the document and recommend the final version include these definitions.

Specific Comments on the CSF 2.0

The following are our specific comments and recommendations on modifying the CSF 2.0 to make this already excellent resource stronger. We urge NIST to expand the CSF 2.0 to describe in more detail significant cybersecurity threats to health care and other sectors of the economy. In conducting risk management and risk mitigation, organizations need to know both what assets need protection and what can threaten those identified assets.

We recommend NIST consider the following areas for CSF 2.0 augmentation:

Address the security challenge presented by third-party applications. While we recognize that application (app) security was not contemplated when the HIPAA Security Final Rule was released in 2005, the issue is a critical one in today's health care environment. Many health plans, physician practices and inpatient facilities have already built or have contracted with business associates to develop patient access Application Programming Interfaces (APIs) and apps and are actively promoting their use.

Specifically, these apps deployed by providers and health plans are typically required to

adhere to HIPAA provisions and therefore the individual's accessing data has assurances that their information is being kept private and secure. We are concerned, however, regarding the lack of robust privacy standards applicable to the large percentage of third-party app developers not directly associated with covered entities (CEs) and therefore not covered under HIPAA. Due to the potential for Protected Health Information (PHI) gained via the apps to be inappropriately disclosed to the detriment of patients and their families, we recommend NIST incorporate the issue of how CEs can address app security directly into the final version of the CSF 2.0.

Include the issue of insider threats. Insider-based threats fall into two broad categories-intentional (malicious) and unintentional. While unsettling, some cybersecurity incidents are the result of specific and intentional acts on the part of a current or former employee. Employees with knowledge of network setup, vulnerabilities, and access codes pose an enormous threat to a health care organization. Employees with malicious intent could alter, destroy, or hold ransom critical and sensitive patient information. With so much attention and money surrounding cybersecurity in the health care industry, disgruntled current or former employees may decide to purposefully disclose patient information out of spite or for the potential of financial benefit.

As well, data breaches caused by employee mistakes, such as a lost laptop, are also a common threat to organizations. In the health care sector, the need for proper device management and monitoring, as well as the protection of sensitive information is equally as important to providing medical care for patients.

Another threat to health care organizations through their employees is phishing attacks. A phishing attack is an attempt to trick users into revealing passwords or personal information. These cyber-attacks are a form of social engineering and are commonly transmitted via email. An employee may receive an email from a hacker posing as a platform used by the organization and say that their account password is no longer valid. If the employee is not properly trained on how to recognize these phishing emails, their 'click' to reset the password, for example, could be all that a hacker needs to put an organization at risk. Each of these insider issues represents significant challenges for health care organizations. We recommend NIST address these in the final iteration of the CSF 2.0.

Expand the discussion of workforce awareness and training. The cybersecurity weak link for many organizations is its workforce. We encourage NIST to expand the discussion of workforce awareness and training in the final iteration of the CSF 2.0. Awareness and training steps for organizations should include: (i) Conduct educational campaigns specific to phishing and other cybersecurity issues; (ii) Leverage simulated phishing campaigns as part of the workforce training regimen and offer additional training to those that fail the phishing test; (iii) Ensure that workforce training is instituted on an ongoing basis and (iv) Include senior management in the education campaign and demonstrate to the entire workforce the critical nature of security awareness training.

Include a specific focus on ransomware. We appreciate the CSF 2.0 including the issue of "cybersecurity attacks" in the document. However, the ransomware issue should be specifically addressed in the document. The immediate and persistent threat of

ransomware attack is driving significant resource allocation on the part of health care and other sectors and by incorporating the ransomware issue directly into the document will expand the reach and impact of this resource.

When a health care entity is hit with a ransomware attack, there can be a devastating impact to operations. For example, if a cloud-based electronic health record vendor is attacked, their client base of physician practices, hospitals, and other care settings could experience a loss of functionality that could significantly impact care delivery. Options for incorporating ransomware into the CSF 2.0 include integrating case studies of a variety of health care organizations that have experienced a ransomware attack and focusing on contingency planning, execution, and recovery. As well, outlining contingency planning strategies based on the type of health care entity hit with the attack would also be beneficial and highlighting how various types of organizations have mitigated these attacks and deployed contingency plans to minimize impact on business operations and patient care. Finally, incorporating disaster recovery operations that organizations have deployed following a ransomware attack would be highly beneficial.

Incorporate additional best practice guidance. For health care CEs, revisions to the Health Information Technology for Economic and Clinical Health (HITECH) Act requires HHS to consider efforts by CEs and BAs to implement "recognized security practices" when assessing fines or penalties under the HIPAA Security Rule. The statute provides that if a CE or BA can demonstrate compliance for the previous twelve months with "recognized security practices," then that entity may benefit in the following scenarios: (i) mitigation of fines related to a HHS investigation resulting from a security incident; (ii) an early and/or favorable termination of an audit brought under section 13411 [of HITECH]; and (iii) mitigation of remedies agreed to in any agreement with respect to resolving potential violations of HIPAA Security Rule.

Under this new law, HHS may reduce fines and penalties for certain violations for HIPAA CEs that have adopted cybersecurity best practices. These best practices and standards are those developed under the NIST Act and under 405(d) of the Cybersecurity Act of 2015. Considering the recent legislative requirement that HHS take into account an entity's deployment of "recognized security practices" before taking any enforcement action, we urge NIST to develop CSF 2.0-based set of specific action steps that organizations can leverage.

Promote improved organizational cyber hygiene. Although it is unlikely that an organization can fully eliminate completely the threat of data breaches and phishing attacks, appropriate security policies can minimize risks. For example, the CSF 2.0 could encourage organizations to improve their cybersecurity hygiene by emphasizing the following steps:

- Create a security-focused culture. Stressing the importance of deploying appropriate security hygiene throughout an organization is an important step toward protecting patient data. Instituting regular cybersecurity training and education courses for every full and part-time employee, both in administrative and clinical departments underscores the point that each team member is responsible

for protecting patient data.

- Allocate appropriate security budgets. Creating this security culture also requires allotting an appropriate budget for employee training and deployment of security technology. Security must be seen as an organizational priority and security leaders need to be part of the overall leadership structure.

- Require strong passwords from workforce members. As inconvenient as it is for employees to implement, health care organizations must require the use of strong passwords. Strong passwords are typically 12-14 characters and include a combination of numbers, symbols, capital letters, and lower-case letters. Maintaining good password hygiene starts with a good structure and ensure employees understand the difference between strong and weak passwords. Incentives and disincentives should be implemented to ensure employee compliance.

- Leverage multifactor authentication. Over the next few years, we expect more of the industry to embrace the use of multifactor authentication (MFA)—particularly token-based authentication, which can significantly reduce the risk of compromised accounts. Health care organizations should be encouraged to use MFA.

- Employ risk-based access controls. Enforcing access policies based on risk will improve an organization's overall security posture and reduce employee resistance to strong authentication technologies, such as password management and MFA. Risk-based authentication can often make it easier for users to access data from their normal locations by eliminating the need for any form of authentication.

- Protect all devices-especially mobile. Health care and other critical sector organizations, including smaller ones, have become more reliant on mobile devices, laptops, tablets, and other devices. It is critical that these devices employ encryption solutions and incorporate other protective measures to guarantee information security.

- Install and regularly update anti-virus software. A powerful line of defense for all health care organizations is the use of anti-virus software. With the constantly changing cyber threat environment, it is essential that anti-virus software is regularly updated to ensure your healthcare organization is always protected and against the newest threat attempts.

- Review cloud storage solutions. Not all cloud-based solutions support good security posture. Popular cloud-based platforms leveraged by organizations may not meet the data security, privacy, or sovereignty, making them an easy target for hackers. All cloud-based storage solutions should be reviewed for their security features and protocols.

- Perform regular data backups. Data loss does not only occur when end users accidentally delete a file, but can be the consequence of hardware issues, power failure or malware attacks. All organizations need to deploy policies and

procedures that ensure important data are backed up in a regular basis. Automated backup procedures should also be considered to maintain a regular backup schedule.

- Recognize and report phishing activity. Organizations need to know when an outside actor is attacking their systems. An organization's workforce should be encouraged and incentivized to recognize and report any instances of phishing.

- Deploy strong controls to protect physical and network access. Protected data should not be readily available for any employee in the organization, but only available to those that have a legitimate need to access it. Organizations must establish a zero-tolerance policy and enforce breaches, even if it involves senior staff.

Work with WEDI and other industry groups such as 405(d) to promote awareness and use of the CSF 2.0. Utilizing conference sessions, webinars, and other educational vehicles, we recommend NIST continue to work with WEDI, 405(d) and other key health care stakeholders to educate our industry specifically on how the CSF 2.0 can be leveraged by health care organizations and other stakeholders. Educating organizations on how to identify security threats, how to mitigate threats, how to develop effective contingency plans and how to successfully recover from a security incident would be extremely beneficial to health care organizations of all types and sizes.

We thank NIST for partnering with WEDI on past educational events aimed at educating the health IT community. We recommend that NIST staff experts and agency resources be further leveraged to acquaint the industry with the many NIST resources and educate them on action steps to improve security hygiene. In addition to continuing our successful partnership, we encourage NIST to reach out to organizations representing various stakeholders in the health care sector and partner on security education.

Conclusion

Allocating sufficient resources to address security issues if often a significant challenge for health care organizations. Recognizing this, the role of the federal government is to identify and make available to the industry the best possible protocols, policies, and procedures. We urge NIST to continue to promote improved security hygiene tactics through every available communication channel, with an emphasis on smaller health care organizations.

We appreciate the opportunity to share our perspective regarding the draft CSF 2.0 and incorporate the new and expanded cybersecurity threats facing health care and other critical industry sectors. WEDI believes the CSF 2.0 and other NIST cybersecurity tools represent some of the best security resources available today. We hope our comments and recommendations will serve to improve the content of the CSF 2.0 and offer opportunities to expand NIST's outreach and impact on the health care sector. We must all work together to ensure patient data is being securely maintained and exchanged throughout the health care ecosystem and provide patients with increased confidence that their health information is being kept confidential.

Please contact Charles Stellar, WEDI President & CEO, at [redacted] to discuss these recommendations or explore future opportunities to work together to educate health care stakeholders.

Sincerely,
/s/
Ed Hafner
Chair, WEDI

cc: WEDI Board of Directors