Tausight™

April 25

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

Tausight welcomes the opportunity to submit comments in response to the National Institute of Standards and Technology Request for Information: Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management published in the Federal Register on February 22, 2022.

Tausight was founded in 2018 with the vision of reducing healthcare specific cybersecurity incidents in the information sharing age by simplifying the way hospitals and healthcare systems detect and manage Protected Health Information (PHI) risk. Applying breakthroughs in ML/Federated Learning and NLP, and a detailed understanding of clinical workflows, we have developed a revolutionary and affordable situational PHI awareness platform that identifies, tracks and analyzes PHI activity and risk, in real-time, in any workflow in today's decentralized care delivery ecosystem.

Prior to starting Tausight, in 2002, I founded Imprivata, where I served as Chief Technology Officer for 15 years, working closely with hospital Chief Information Officers (CIOs) and Chief information Security Officers (CISOs) to develop Identity and Access Management solutions designed for the unique workflow requirements in healthcare. In 2016 I was appointed to the Department of Health and Human Services Healthcare Industry Cybersecurity Task (HCIC) Force, the group that co-authored the Report on Improving Cybersecurity in the Healthcare Industry in 2017. It was during this time that it became clear to me that once the adoption and meaningful use of technology in healthcare became a reality, and information was being shared between providers, patients, payers, public health practitioners, technology developers, researchers, and other stakeholders, a new approach to protecting PHI would be required.

Tausight is a CHIME and AEHIS Foundation Partner, and we agree wholeheartedly with the comments submitted by Russ Branzell on behalf of the organization. In particular, we support the recommendation that NIST work with 405(d) to leverage the *Healthcare Industry Cybersecurity Practices (HICP)* to educate providers on concrete steps that can be taken to protect data and patient safety. The healthcare sector faces distinctive challenges caused by the increasingly decentralized nature of care, the open working environment, concerns for delaying the clinical workflow, patient safety issues in the response/recovery phase and the desire to roll back the entire system to a known backup state, etc. The 405(d) practices and metrics have been developed with these healthcare specific characteristics in mind and would be valuable to healthcare organizations implementing the NIST Cybersecurity Framework.

We appreciate NIST seeking suggestions for improvements to the CSF. In addition to endorsing the comments submitted by CHIME/AEHIS, Tausight would like to present the following comments for consideration.

Use of the NIST Cybersecurity Framework

1. The usefulness of the NIST Cybersecurity Framework for aiding organizations in organizing cybersecurity efforts via the five functions in the Framework and actively managing risks using those five functions. –

CSF offers a standardized vocabulary and framework for building cybersecurity resiliency in a thorough and comprehensive manner, but it has proved overwhelming for many in the healthcare industry to implement. The guidance from the 405(d) task group on "Healthcare Industry Cybersecurity Practices" (HICP) is more practicable for healthcare providers by narrowing the lens on what is critical for patient care delivery. HICP also provides clear and actionable guidance for organizations of various sizes, whereas the NIST CSF requires a substantial security team in order to produce an actionable and practical program.

The challenges for applying it in the healthcare industry is the nature of what is critical for supporting the supply chain used today in delivering patient care across a distributed network of service providers. Patient information is now being sent and used in more business associates or covered entities than ever before creating the need for customized cyber boundaries that are established based on the patient care regime.

Some of the challenges we've seen in applying the CSF in healthcare include:

***Identify** – ePHI is the core asset that drives digital health and the ability to deliver patient care. It is a high-valued, transient digital asset that can be arbitrarily created by a clinician whenever and wherever on behalf of the patient such as sending a referral note to another provider. The "identify" requirement of the CSF has to account for the nature of the clinician's workflow and the need to inform the healthcare industry that ePHI is an intangible, yet critical asset that must be considered the same as any other asset such as servers, endpoints, etc. Identifying and inventorying these assets is difficult as new instances of ePHI are created anytime Personal Identifying Information (PII) is blended with medical information in healthcare, this occurs anytime medical correspondence is involved such as in a consult or referral email.*

***Protect** – Healthcare IT currently takes the perspective that the majority of the critical assets lie within the perimeter and on secured servers that manage the bulk of the ePHI. As provider organizations of all sizes have experienced, ransomware and theft of medical records are not limited to just the servers but are notorious for attacking endpoints as well. The boundary for what must be protected must extend to the edge of the network and cover all potential locations where clinicians can create, store, transmit and use ePHI. Protecting ePHI is mandated by the HIPAA Security Rule but due to the large number of endpoints inside and outside of the hospital environment, it is extremely difficult to ensure, as often, there are disparate lines of responsibility for ensuring adequate security. Use of personal machines at home or shared endpoints in a clinical setting increase the challenges of protecting ePHI and the applications used by clinicians to access it.*

***Detect** – Healthcare IT has a high ratio of endpoints to clinicians as many of the machines are distributed throughout a hospital. The lack of a clear ownership relationship between a clinician/user and an endpoint means the only way IT gains visibility to what is happening on a computer is either* *through feedback from clinicians, the help desk or remote system monitoring. The lack of situational awareness related to the critical aspects of the ePHI lifecycle – where it is being created, stored, transmitted and used means it is extremely difficult to model or establish baselines for "normal" operating circumstances. These models are also highly correlated to clinical workflows which vary depending on the different roles clinicians take, especially if they have teaching or research responsibilities. There is an understanding and desire to be able to detect changes in the system that may affect how the system addresses the Confidentiality, Integrity and Availability around ePHI, but currently the sophistication is mostly around the technical infrastructure with strict change management policies.*

***Respond** – In healthcare, if business stops, human lives are at risk. Lacking a means to understand the extent of damage, and not willing to endanger patients, during an incident, healthcare systems rely on paper records using archived records from air-gapped machines. The decision to stop relying on the EMR and go to paper is not easily made, but unfortunately the choice is often made without sufficient information pertaining to the cause, or with the lack of situational awareness. Going to paper records means not only reconciling the information post-incident but also the inability to use the EMR decision support systems for such things as drug dosage, drug-drug interactions, etc., which poses a serious risk to patient safety.*

***Recover** – The ability to recover an IT infrastructure is dependent on having an accurate inventory of all the critical assets, the ePHI content, critical applications used by clinicians, the configurations for medical devices and the ability to compare and contrast what was changed during an incident. Having access from a trusted (immutable) source to accurately capture pre-incident snapshots of what the data and the system looked like before the incident is critical to timely isolation and recovery of the system. Most logging information on endpoints and servers will likely be wiped by the attacker. Lacking a means to understand the extent of damage and the ability to isolate changes means the most common recovery method for healthcare is complete system restoration – servers and endpoints from their backup archives. This is an expensive and time-consuming process for most hospitals.*

2. Current benefits of using the NIST Cybersecurity Framework. Are communications improved within and between organizations and entities (e.g., supply chain partners, customers, or insurers)? Does the Framework allow for better assessment of risks, more effective management of risks, and/or increase the number of potential ways to manage risks? What might be relevant metrics for improvements to cybersecurity as a result of implementation of the Framework?

Between Cybersecurity, Privacy and IT the CSF becomes a tool and vocabulary for sharing principles and approaches. While it was intended for all verticals, most healthcare professionals understand them conceptually but need to convert the principles to a clinical setting and more importantly, understand them from the perspective of the clinical workflow. The 405 (d) guidelines' interpretation of the CSF simplifies actions from a healthcare point of view. More importantly, it accommodates for the size of the organization to allow for a better assessment of risks, more effective management of risks, increased number of ways to manage risk.

3. Challenges that may prevent organizations from using the NIST Cybersecurity Framework or using it more easily or extensively (e.g., resource considerations, information sharing restrictions, organizational factors, workforce gaps, or complexity).

DifficultyIdentifying PHI given the decentralized nature of work - clinicians working at home, in the clinic, each receiving, using and producing more patient records.

The requirements of The 21st Century Cures Act to broaden the formats to receive/send data, in whatever format requested by patients, increases the challenges of finding PHI, much less securing it. Problems with Shadow IT and the potential for privileged users with administrative credentials inadvertently installing malware on a single click.

The concern that security slows down the clinical workflow and efforts to subvert them make deploying CSF more challenging especially around detect/respond. Perpetual use of "break the glass" by clinicians bypassing security to (correctly) address patient care needs. The challenge is "how do you inventory PHI in a dynamic manner?"

The framework allows for comprehensive risk assessment and coverage but it requires too many resources for most small and mid-sized healthcare organizations today. There needs to be a simplified pathway to assist healthcare organizations to quickly develop and implement a "cybersecurity sprint."

4. Any features of the NIST Cybersecurity Framework that should be changed, added, or removed. These might include additions or modifications of: Functions, Categories, or Subcategories; Tiers; Profile Templates; references to standards, frameworks, models, and guidelines; guidance on how to use the Cybersecurity Framework; or references to critical infrastructure versus the Framework's broader use.

Clear reference should be made to the guidance from the 405(d) task group on "Healthcare Industry Cybersecurity Practices" (HICP).

5. Impact to the usability and backward compatibility of the NIST Cybersecurity Framework if the structure of the framework such as Functions, Categories, Subcategories, etc. is modified or changed.

6. Additional ways in which NIST could improve the Cybersecurity Framework, or make it more useful."

A road map that makes it clear where organizations should begin their "cybersecurity sprint" would be useful as they will not be able to tackle everything on the first round of effort.

Thank you for the opportunity to contribute suggestions for improving the NIST CSF. Please don't hesitate to reach out if I can be of assistance.

Sincerely,

David Ting
Founder and Chief Technology Officer