Establishing the clear mandate
Alignment between NIST CSF, CISA, and others

The attackers got into the company's digital network through the help of a publicly exposed password of a VPN account. After the attackers got entry into the company's network system, they stole 100GB of the data within the next 2 hours. After the data theft, the attackers infected the digital network with ransomware, affecting many other systems, such as billing and accounting.

Unfortunately, many U.S. Government Departments/Agencies reported the Cyber matter as: a Cyberattack, Cybersecurity Breach, Ransomware Cyber-Attack, Ransomware Incident, an Attack, a Hack, Ransomware Attack, and Data Breach. [The above is the 2021 Colonial Pipeline Company matter.] And while they are similar, they don't have the same meaning and therefore don't elicit the same response. So, we return to NIST Computer Security Resource Center terms and definitions for a Cyber Attack: "Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself." (OR) "An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information."

NIST CSF 2.0 cannot solve the many IT/Cybersecurity resource challenges, but it can continue emphasizing the need for a structured approach to a Cybersecurity Program. The National Institute of Standards and Technology's (NIST) 's creation of the Cybersecurity Framework (CSF) has been incredible for Critical Infrastructure Systems and precious to public and private organizations around the globe. CSF is the onramp to considering and developing a Cybersecurity Program, and it provides structure to establishing, managing, and maturing an organization's Cybersecurity Program through five functions, 23 categories, and 108 subcategories. NIST did a tremendous service to many organizational departments and functions from Information Technology (IT), Information Systems (IS), Information Security or Cybersecurity ('Cybersecurity'), Risk Management, and Audit by including Informative References, Resources (e.g., Presentations, Training, Crosswalks, Mappings), and various Baldridge Cybersecurity Excellence assessments.

The NIST CSF Informative References and mappings have significantly aided more mature organizations and IT/Cybersecurity Departments/Functions ('functions') in their adoption of broader IT, Security, and Privacy control sets from ISO, NIST, ISACA, CIS, and the consideration of regulations and laws from GDPR to CCPA, and others. And while it may be apparent for some that the NIST CSF is the "what," while NIST Special Publication 800-53 rev4/rev5 ('SP 800-53'), Security and Privacy Information Systems and Organizations and the other standards are the "how," the reality is that the under-resourced organizations and IT/Cybersecurity functions cannot transition from the day-to-day tactical matters of vulnerabilities, patches, and incidents to being able to strategical consider the adoption of a standard or framework.

The SP 800-54 standard is voluminous at 1189 spreadsheet rows of current or retracted Control (or Control Enhancement) statements, and the Control Texts read more like detailed action plans. The depth and detail are phenomenal, especially for public and private organizations looking to solidify their Cybersecurity footprint further. For under-resourced organizations and IT/Cybersecurity functions, SP 800-53 is another set of considerations that requires a significant amount of time and is, unfortunately, a low priority. And the organizations and IT/Cybersecurity functions that adopt SP 800-

53 tend to implement a standard set of Security and Privacy controls without providing the necessary relevance for their organization.

Fundamentally, most organizations and IT/Cybersecurity functions are challenged to identify, assess, document, and continuously manage their information and security practices, from categorizing systems to prioritizing and implementing security and privacy controls that meet their mission and business objectives. Such activities are deemed not a high priority, less valuable, unsustainable, irrelevant to more systemic matters, incidents, and threats, and lacking commitment from the Board, Executive Management, and Senior Leadership. Here in lies the opportunity for NIST and CSF 2.0. In coordination with other U.S. Government Departments/Agencies, translate the many recent Cybersecurity events into activities that could have mitigated the associated risk.

In addition, here are some additional steps:

1. Modify the subcategories language into principle statements. Such an approach is similar to how the Committee of Sponsoring Organizations (COSO) Internal Control-Integrated Framework (ICIF) 2013 includes five components of internal controls, 17 principles, and 81 points of focus that provide the structure to this framework. The form is neither control objectives nor statements but mere characteristics and considerations to define a system of internal controls.
2. Use the five functions of the NIST CSF to align and collaborate with Cybersecurity & Infrastructure Security Agency (CISA) and the sector-based Information Sharing and Analysis Centers (ISACs).
3. CISA, as America's Cyber Defense Agency, serves "a single resource that provides you with access to information on services across CISA's mission areas."
4. Unfortunately, the NIST CSF is not 'actively' communicated on the CISA website or how materials available via the website are labeled. The NIST CSF is mapped to CISA Cyber Resilience Review (CRR). However, any user will find it difficult to distinguish why CRR, an operational resilience and security practices assessment method, is not modeled entirely on the NIST CSF 1.1.
5. The CISA states that the NIST CSF "which provides a holistic perspective of the core steps to a cyber risk assessment." This is a somewhat confusing statement considering that is why CISA promoted the CRR.
6. The CISA's 2022 Cross-Sector Cybersecurity Performance Goals state the following: "It became clear that even with comprehensive guidance from sources like the NIST Cybersecurity Framework, many organizations would benefit from help identifying and prioritizing the most important cybersecurity practices along with support in making a compelling argument to ensure adequate resources for driving down risk. Ultimately, prioritized investment will help meaningfully address serious risks to the safety, health, and livelihoods of the American people." 2 And recommends using NIST CSF or ISA 624433.
7. National Council of Information Sharing and Analysis Centers (ISACs) and the 26 sector-based ISACs should be utilized to promote the core concepts of NIST CSF "Profiles," "Tiers," and measuring and assessing against the NIST CSF.
8. While most sector-based ISACs embrace the NIST CSF, the Center for Internet Security (CIS), which houses the Multi-State Information Sharing and Analysis Center (MS-ISAC) and Elections Infrastructure ISAC (EI-ISAC), has for years produced the CIS Critical Security Controls Top 18 (formerly known as the CIS Top 20), a different framework of 153 safeguards. The CIS Controls are publicly available and have been formally mapped to the NIST CSF. Unfortunately, the CIS Controls version 8 introduces implementation groups to ease adoption to SLTT and non-SLTT entities.

9. Use the NIST CSF 2.0 to align communication and messaging around NIST Special Publications and NIST Internal Reports (NISTIR). The SP 800-53 Security and Privacy Controls for Information Systems and Organizations has only been mapped to the NIST CSF.
10. NIST CSF 2.0 is an opportunity to demonstrate how an organization establishes its Cybersecurity Program and how it is not a one-size fits one. Still, it must be tailored to the organization.
11. For the more mature Cybersecurity Programs - Begin with one of the five function areas and the related categories and subcategories; the organization must determine current controls. And then whether the organization's controls satisfy SP 800-53 control (or control enhancement) statements by utilizing the applicable control texts. For an even more mature Cybersecurity Program, consider applicable NISTIR Profiles and the organization's adoption of other potentially applicable NIST Special Publications.
12. For the less mature Cybersecurity Programs – Begin with one of the five function areas and the related categories and subcategories. Then, begin an internal dialogue on the activities or documentation available to frame the organization's response to the subcategory. For each subcategory, determine the basics:
13. Does the organization have a policy that addresses this subcategory or category?
14. Does the organization have a procedure, process, or general notion of activities to address this subcategory or category?
15. If XYZ asked the organization to demonstrate our approach to date, would the organization do ABC? Reinforcement of each subcategory should be coupled with SP 800-53 example control texts to assist with identifying and defining controls.
16. For the moderately mature Cybersecurity Program – Begin with the sector-based ISACs to determine whether 'what' is being performed today aligns with the sector-based ISAC guidance and the NIST CSF. Determine whether the shortfalls to maturity are people, processes, or technology. Consider SP 800-53 example control texts to assist with assessing and improving controls.

In summary, the NIST Cybersecurity Framework 2.0 is how anyone in any size organization across any sector begins to understand how the organization handles security and protection of IT. The continual adoption, performance, and evolution of IT require sufficient structural boundaries defined within the organization by executives, boards, state and local governments, educational departments, and tribunal communities. Unfortunately, tomorrow's IT investment decisions are made without a sufficient understanding of today's security and risk challenges, especially regarding assets, networks, users, data, resources, suppliers, training, continuity, redundancy, incident response, etc. Therefore, Cybersecurity Framework 2.0, at its core, is about establishing IT governance and not another function or role.