Katherine MacFarland
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Dear Ms. MacFarland,

Thank you for the opportunity to comment on ways we can evaluate and improve the NIST Cybersecurity Framework.

The Internet Security Alliance (ISA) is a multi-sector coalition comprised of Fortune 500 companies representing virtually every critical infrastructure sector. ISA's board of directors consists of the top cybersecurity professionals (typically chief information security officer) from these companies (see attached list). ISA sells no products or services. ISA's sole mission is to integrate advanced technology with public policy and business economics to create a sustainable system of cybersecurity.

As we begin this review of the utility and enhancement of the NIST Cybersecurity Framework (NIST CSF) it is important to understand that the United States is under significant, constant, and successful cyber-attacks. Criminals and nation states routinely compromise our cyber defenses – both industry and government—with substantial impact. Cybercrime costs over $2 trillion a year in economic damage. Yet we currently prosecute less than 1% of cyber criminals. The Solar Winds attack was not discovered by the US government which needed to rely on the private sector to identify the attack nearly a year after it had compromised both government and industry systems.

Nearly a decade after the promulgation of the NIST CSF we are far worse off in terms of our overall all security than we were before it was promulgated. We need to understand that what we have been doing for the last decade is not working sufficient to our needs, in fact, some elements of what we have done, as we will explain below, are counter-productive to our nation's overall security.

The notion that all we need is some minor repairs and technical modifications to the NIST CSF and overall, our cyber strategy is tragically naive. The NIST CSF is a fundamental element of our cyber security strategy, but it needs to be enhanced significantly with comprehensive analysis and modification based on a new appreciation for the public private partnership and a rigorous documentation of its effectiveness.

The Internet Security Alliance's History with the NIST CSF

The ISA initially called for creating, what eventually became the NIST Cybersecurity Framework as part of a broader proposal to enhance our nation's security in its 2008 Cybersecurity Social Contract[1]:

"[I]n order to provide the stability and predictability that ISA agrees must be present… Federal incentives must be associated with those standards that are widely recognized and have broad endorsement… Information security procedures that are established and maintained pursuant to applicable standards published by recognized standards organizations. Specific organizations which could be recognized by the enabling legislation would be… [the} National Institute of Standards and Technology."

ISA's 2008 proposal called for developing NIST's framework standards and practices but coconsciously embedded it into the economic model which the private sector operates under. ISA has always believed that to create a model without accounting for the economics of the issue would fail to adequately service our emerging cyber crisis. In fact, an appropriately designed model, including the economics, would enable faster and more agile defense in the face of rapidly changing threats.

"This model has multiple advantages. First, it allows for multiple 'standards' to be rewarded and, thus, avoids the one size fits all problem of a single standard… The standard-setting entities themselves are enhanced by the larger number of organizations that adopt their standards. As a result, there is a built-in economic social benefit, motivated by a profit incentive that can move with far greater speed and which can easily stay abreast with ever-changing technologies, their vulnerabilities and threat vectors that can the traditional regulatory mechanisms that move far too slowly to keep pace with this continuing evolution, a system motivated by the profit motive can move with far greater speed."

Although Executive Order 13636, which designated NIST as the standards body to carry out this proposal, called for the Framework to be flexible (which it is) but also cost effective, prioritized, and supported by incentives. These critical aspects have never been conscientiously developed by NIST. These omissions have led to under-utilization of the framework which in turn has limited its impact. ISA suggests that these omissions need to be corrected in the 2.0 version of the framework. By fulfilling the mandates embedded in the Executive Order 13636, NIST will unlock the potential the framework possesses and would substantially enhance our nation's security

Some may argue that demonstrating the cost effectiveness of the CSF which would enable private companies (especially smaller companies) to prioritize its use and design incentives for its voluntary use are outside NIST's purview. However, the EO is quite clear that these qualities are essential elements of the full framework NIST was charged with creating. In addition, while

[1] https://isalliance.org/isa-publications/social-contract/

the sector Risk Management Agencies can be expected to have more substantive knowledge in the sectors subject area, there can be no greater authority on how to best use the NIST CSF than NIST itself. Moreover, as will be demonstrated below, the current fractured approach the federal government has taken for the past decade wherein agencies are asked to use the NIST CSF without any guidance from NIST as to how to fulfill the requirements that it be cost effective, prioritized, and supported by incentives not only is not providing adequate security, but it is also quite likely undermining national security efforts through disjointed, duplicative and even conflicting federal systems.

Perhaps most importantly, while the idea that cybersecurity was simply an “IT” issue that could be addressed simply with a technical framework may have been conventional wisdom – mistakenly so – a decade ago, the cybersecurity field has now moved past this narrow construction. Perhaps there is no clearer demonstration of the insight that in order to construct an effective framework to enhance our nation’s security, economics must be directly injected into the framework than the bipartisan letter cosigned by seven different Congressional Committee and Subcommittee Chairs and their Ranking Members that “stressed” “cybersecurity is not just an IT issue, but an economic issue with national security implications.”

ISA urges NIST coordinate with the new Office of the National Cybersecurity Director to take a more pro-active role in managing the use of the framework by its government partners including fully integrating the economic factors called for in EO 13636 as core elements of the 2.0 version of the NIST CSF.

As NIST looks to update the Framework to Version 2.0, we encourage NIST to continue using the successful public-private partnership model it used for the Framework’s development and subsequent updates. In fact, NIST’s approach has aligned with many of the best practices for public-private partnerships as identified by the IT Sector Coordinating Council and the Department of Homeland Security. These include:

- Senior level commitment to the partnership process communicated to staff & upper echelons
- Involvement at the priority/goal & objective phases of projects, not just implementation
- Use of the process identified in the NIPP for involving industry
- Reaching out to stakeholders early on, ideally at the "blank page" stage
- Continuous and regular interaction between government and industry stakeholders
- Providing adequate time for stakeholder review (equivalent to government review)
- Establishing co-leadership of programs
- Consensus partnership decision making
- Communicating genuine interest in stakeholder input e.g. via co-drafting
- Adequate engagement from federal agencies beyond DHS
- Government follow through on partnership related decisions
- Adequate and competent support services

Section 1 – Use of the NIST Cybersecurity Framework

Section 1, Subsection 1 – What is the current usefulness of the NIST Cybersecurity Framework for aiding organizations in organizing cybersecurity efforts via the five functions?

Although the NIST CSF has been a watershed contribution to our overall cybersecurity efforts, nearly a decade after its development, and continual promotion by the federal government -- and notwithstanding various publicized examples of use by various companies -- overall use of the framework is limited. A 2022 study By ThoughtLab found roughly a third of large organizations (32 percent) surveyed use the NIST CSF. As will be noted below, other research suggests use of NIST CSF by smaller companies is far lower than the ThoughtLab study found.

The comparatively limited use of the CSF may be due to a lacking empirical data that demonstrates that its use substantially enhances security. A 2020 study from ThoughtLab found that the relationship between companies who use the NIST CSF and effectiveness in actual security is weak[2]. A minority (42 percent) of companies found to be leaders in terms of NIST CSF compliance were also leaders in terms of overall cybersecurity effectiveness.

ThoughtLab noted that chief information security officers generally acknowledge that while following the NIST CSF is a fundamental element of effective cybersecurity, its use alone is insufficient to protect against advanced threats. Specifically, the study noted "Firms need to go beyond NIST and other frameworks to secure their enterprises from escalating cyber-attacks."

The 2022 study asked these companies to rank their progress on key activities under each NIST Framework function, ranging from 1 (undefined with no plans in place) to 5 (optimized and ahead of industry peers)[3]. The five levels were defined as follows:

- **Level 1:** Undefined – starting to think about this, but no plans in place.
- **Level 2:** Ad hoc – beginning to put plans and processes in place. Taking action, but not consistently.
- **Level 3:** Defined and repeatable – have defined processes and plans. Making progress but not fully aligned with the business yet.
- **Level 4:** Managed – continuous monitoring, with metrics in place, and seeing considerable benefits.
- **Level 5:** Optimized – fully acted on this activity. Ahead of most industry peers and seeing significant benefits.

Companies that use the Framework often use it as their core benchmark and track progress against the categories and sub-categories for program capabilities and services. Frequently, these organizations do not use strict framework mapping, as they are often too abstract and do

[2] https://econsultsolutions.com/driving-cybersecurity-performance/

[3] https://thoughtlabgroup.com/cyber-solutions-riskier-world/

not align with modern services. While organizations benefit from using the Framework – primarily due to its directional and flexible guidance – progress among the five functions – identify, protect, detect, respond, and recover – has been mixed.

Among the 32% of companies using the Framework, ThoughtLab discovered the following on organizations' progress in using the five functions:

- **Identify:** 51 percent of the organizations using the CSF are either in the managed or optimized stages of cybersecurity governance, and 50 percent of those surveyed are in managed or optimized stages of risk assessment. 46 percent of organizations are in managed or optimized stages of supply chain risk management, and 44 percent are in managed or optimized stages for risk management strategy. Organizations ranked lowest in business environment and asset management, with only 38 and 35 percent of organizations being in managed or optimized stages, respectively.
- **Protect:** More than half of all organizations are in managed or optimized stages for protective technology (55 percent) and data security (52 percent). However, progress falls off sharply for maintenance, awareness and training, identity management, and information protection processes vital for safeguarding networks and data. Only 40 percent of organizations are in managed or optimized stages for maintenance, and those numbers drop significantly for awareness and training (36 percent), identity management and access control (35 percent), and information protection processes (35 percent).
- **Detect:** Most organizations using the framework need to do more to catch up in detection activities as they face more complicated perils. 58 percent of organizations are in managed or optimized stages for detection processes. However, while this is good progress, most organizations are doing far less well in basics such as continuous security monitoring (41 percent) and anomalies and events detection (39 percent).
- **Respond:** Many organizations fall short with adequate response planning, mitigation, and communications. Less than half of the organizations surveyed (47 percent) are in the managed or optimized stage for most response areas. Specifically, communications are weak (only 37 percent of organizations were in managed or optimized stages), despite the criticality of reaching out to stakeholders and law enforcement agencies to contain a breach. Mitigation, analysis, and improvements ranked poorly as well, with 46 percent, 45 percent, and 44 percent of organizations being in managed or optimized stages, respectively.
- **Recover:** More than half of the organizations surveyed (54 percent) are advanced in recovery planning and just under half in communications (49 percent). Only 38 percent have progressed in improvements post-breach, failing to apply lessons learned to prevent future events.

The report also stresses that proactive cybersecurity management requires going beyond the NIST Framework and drawing on advanced analytics and continuous surveillance to counter emerging complex threats. The alternative models suggested below map to NIST CSF but also facilitate these advanced functions by folding in the critical economic aspects of cyber risk management.

The findings in the ThoughtLab report underscore that many organizations still are struggling with how to implement the five functions of the Framework. ISA believes that much of this confusion could be addressed through systematic evaluation of the framework which would document what uses are most cost beneficial to defined categories of organizations. It is time to finally move on from the use of self-report testimonials as illustrative of the Frameworks utility and move to an empirical basis for how the framework can best be used by defined categories of organizations. Such, research must, include the construct of cost-effectiveness. as called for in the 2012 EO 13636 which gave rise to the framework,

As the National Infrastructure Protection Plan NIPP) correctly points out, private sector organizations appropriately make investments on a commercial economic basis. For a voluntary government program, such as NIST CSF, to have its maximum impact it needs to address the real-world economics that are an inherent part of private sector security investment.

Such research is fully consistent with the voluntary nature of the NIST CSF. Organizations will quite naturally deploy programs that are empirically proven to be cost effective. This research will have the added benefit of helping to define what former CISA Chris Krebs has referred to as the "delta" between commercial security and national security. This research would not only enable identifying what uses of the CSF are cost effective, but also may illustrate uses that are needed – but not cost justified. Such findings would enable government to define adequate market incentives which would enable critical infrastructure to invest in non-commercially justified security procedures while maintaining their economic viability to provide needed consumer services.

Section 1, Subsection 3 – What challenges prevent organizations from using the NIST Cybersecurity Framework or using it more efficiently and extensively (e.g., resource considerations, information sharing restrictions, organizational factors, workforce gaps, or complexity)? How can we address those challenges?

Despite robust efforts to promote the Framework's use since its inception in 2013, research underscores room for improvement among large as well as smaller organizations.

A joint industry-Department of Homeland Security white paper noted that "many small and medium-sized businesses (SMBs) are still unaware of the Framework[4]." Moreover, a 2021 US Telecom study found that only 13 percent of small businesses in critical infrastructure sectors rely on government advice – such as the NIST Framework – in developing their cybersecurity programs[5].

[4] https://www.it-scc.org/uploads/4/7/2/3/47232717/the_collective_defense_white_paper_12.19.pdf

[5] https://www.ustelecom.org/research/2021-cybersecurity-survey-critical-infrastructure-small-and-medium-sized-businesses/

As noted above, in order to maintain viability private organizations must make security decisions based not purely on threat assessments but threat assessments in context of their economic needs. Because of this fact private entities often must be more risk tolerant than government might be. For example, everyone knows that retailers tolerate x percent of their inventory to "walk out the back door." The reason they don't hire more guards or other security process to prevent the pilferage is because they have determined such security spending would be some form of x +1, or 2, or 3 …. While private entitles are obviously interested in securing themselves – from cyber-attack as well as other threats – of necessity this is an economic calculus. Pragmatically speaking, the questions private entities have to address is, how much security can I afford to buy?

This process is particularly important for smaller companies who often operate with less economies of scope and scale as well as smaller profit margins. Especially for this critical element of the cybersecurity eco-system the question is what marginal dollar I can afford to devote to security – as opposed to other priorities such as sales and marketing. As documented in the US Telcom study these decisions are typically not based on government advice, More typically they are based on data.

If NIST could identify which elements are most effective and cost-effective for organizations of a defined size and or sector it would become much easier to persuade smaller organizations – limited in time and resources – to adopt the Framework to bolster their security.

Advanced analytical models now exist to help document the effectiveness and cost-effectiveness of cybersecurity controls. Using these tools, NIST can document what variations of the Framework (and there are many possibilities) show cost-effectiveness for specific user populations.

NIST should enlist the assistance of the Sector Risk Management Agencies (SRMAs) working with the Sector Coordinating Councils (SCCs) to design and undertake a systematic evaluation process to measure the NIST Framework's impact and cost-effectiveness when adopted by defined segments of the sector.

Armed with empirical data jointly produced through an industry-government partnership further outreach, backed by empirical data, will likely have greater impact on overall use of the framework while simultaneously enhancing the needed industry government partnership on cybersecurity. Now is the time for NIST to follow up on that task, leveraging new tools for a sophisticated assessment based on economics. Research that documents the use of specific elements of the CSF to security outcomes would be a strong lever for increasing the voluntary use of the NIST CSF.

Organizational factors may also be an inhibiting factor in fuller NIST CSF use. Initial drafts of the 1,0 version of the NIST CSF did attempt to contextualize the framework into the governance structures of enterprises. NIST representatives have since commented publicly that they abandoned this aspect of the 1.0 CSF based on comments suggesting this was inappropriate. Subsequent research indicates that NIST's original inclination was probably right.

Existing reporting structures and decision-making processes in many enterprises are legacies of a siloed operating model. In these instances, each department and business unit makes decisions and manages risk relatively independently, without fully taking into account digital interdependency – a fact of modern business.[6] The World Economic Forum conducted research on cybersecurity in enterprises, finding that "strong and effective cybersecurity adds value to the business. Controlling cyber risk means coordinating and collaborating with business units throughout the enterprise including the CEO and the board. Ensuring the entire enterprise, not just the IT department, is addressing cyber risk furthers the organization's culture of cybersecurity."

NIST can help organizations adopt this kind of enterprise-wide approach by harmonizing the with popular standards and models already being used in the private sector facilitating enterprise-wide cybersecurity.

For example, NIST should align the CSF with its Integrating Cybersecurity and Enterprise Risk Management guidelines, which mirrors the popular enterprise risk management approaches being adopted by private sector corporate boards. NIST's Enterprise Risk Management guidelines view cybersecurity as more than an IT issue, aligning with the predominant model used in the private sector.

The National Association of Corporate Directors' Cyber-Risk Oversight Handbook outlines these same principles, identifying cybersecurity as a strategic enterprise risk. It urges organizations to establish an enterprise-wide cyber-risk management framework with adequate staffing and budget. These approaches have been adopted globally through organizations such as the Organization of American States, the European Confederation of Directors Associations, the Japanese Business Federation, the World Economic Forum, and more.

Moreover, these guidelines have been assessed and determined to be effective at improving overall enterprise cyber-risk management in the private sector.

An independent study from PricewaterhouseCoopers found that adopting the NACD model led to meaningful security improvements: "Boards appear to be listening to this guidance. This year we saw a double-digit uptick in Board participation in most aspects of information security. Respondents said this deepening Board involvement has helped improve cybersecurity practices in numerous ways. It may be no coincidence that, as more Boards participate in cybersecurity budget discussions, we saw a 24% boost in security spending. Other notable outcomes cited by survey respondents include identifying key risks, fostering an organizational

[6] https://assets.ey.com/content/dam/ey-sites/ey-com/en_us/topics/cbm/ey-how-boards-are-governing-disruptive-technology.pdf

culture of security, and better aligning cybersecurity with overall risk management and business goals.”

NACD’s 2020 Public Company Governance Survey, further corroborated the advancement of Enterprise Risk Management maturity among boards, with 79 percent of directors saying their board’s understanding of cyber risk had significantly improved compared to two years prior.

By harmonizing the NIST CSF with the Enterprise Risk Management guidelines, which align private-sector NACD principles, NIST can speak with a consistent voice to approaches that are effective at enhancing security. These principles have been adapted to numerous international markets, taking a consistent approach can expand international use and interoperability, enabling organizations to integrate new technologies and services more effectively and securely to support their digital transformation efforts. Moreover, these approaches are being adopted at the management level as well. Textbooks – such as *Cybersecurity for Business: Organization-Wide Strategies to Ensure Cyber Risk is Not Just an IT Issue* – are now being adopted in business courses, bringing these paradigms of cybersecurity into the management level of enterprises.

Section 2 – Relationship of the NIST Cybersecurity Framework to Other Risk Management Resources

Section 2, Subsection 8 – Are there commonalities or conflicts between the NIST framework and other voluntary, consensus resources? Are there commonalities or conflicts between the NIST framework and cybersecurity-related mandates or resources from government agencies?

Harmonizing Regulatory Adoption of the NIST Cybersecurity Framework

Since the Framework’s inception, the federal government has promoted aligning regulatory models with the NIST Framework, and regulatory agencies have stepped up to that task. Unfortunately, these regulatory models, even if based on NIST CSF, are ill-suited for the dynamism of the cyber threats we face today. Thus this “leveraging” of the NIST CSF undermines its voluntary nature and, with its ongoing expansion promotes a security system that has not been shown to be enhancing security and may well be compromising collective security by encouraging wasteful use of scarce cybersecurity resources.

At core the traditional regulatory system is a backward looking, check-the-box pass-fail system primarily designed to detect and punish corporate misfeasance and mal-feasance.
Effective cyber risk management is almost the polar opposite of these regulatory models.

Effective cyber risk management is not a backward-looking process to see if you have met a pre-determined criterion. Instead, effective cyber risk management is a forward-looking process – focused on assessing what attacks are most likely and proactively designing a defensive posture. In addition, unlike regulatory compliance, which is pass-fail (you are either in compliance or not), cybersecurity is a spectrum. Organizations are no secure vs insecure.

They are on a spectrum of relative security and the appropriate level of security can only be understood within the context of the threats that particular entity faces.

Finally. Traditional regulation is essentially an adversarial system premised discovering an organization that is negligent or corrupt. Contrary to early conceptions, still present in some circles, that the existence of a breached cyber system is the result of organizational failure (which in some cases is probably true of both the private and publish organizations that have been compromised) the more typical problem is that the attacker – motivated by the enormous profits cybercrime yields and the almost total lack of effective law enforcement --has found one of the innumerable vulnerabilities in the system and exploited it. Relying on a system that results in blaming the victim (be it industry or government which has been compromised) is unhelpful.

Notwithstanding the awkward fit of traditional regulation into the cybersecurity domain, federal agencies have been building the Framework into these outdated compliance regimes with no clear evidence that these efforts enhance security as intended.

In his book, *How to Measure Anything in Cyber Risk*, Douglas Hubbard evaluated the standard measurement techniques for existing cybersecurity regulation and determined "there is not a single study indicating that the use of such methods actually helps reduce risk."

Moreover, a 2020 MIT report notes that standards such as NIST provide limited protection capabilities against sophisticated threat actors like nation-states. The report quotes a former official from one government agency that "Compliance [with standards] does not mean security. Certified compliance is a joke. We were constantly violating systems that were supposedly compliant." The report also conveys that government and private sector experts worry these standards are well below the existing capabilities of the largest firms in key sectors, so codifying these standards as regulation or conducting audits based on those standards would not enhance security at the companies whose failure presents the most significant systemic risk.

However, in doing so, redundancies and conflicts have become rampant.

According to a 2020 GAO review of cyber regulation, the percentage of total requirements with conflicting parameters ranged from 49 percent to 79 percent[7]. These variances, according to GAO, were primarily due to the lack of coordination between agencies. Similarly, a private-sector study found that chief information security officers spent upwards of 40 percent of their time and resources dealing with conflicting or redundant compliance exercises.[8]

Current duplication and conflict across federal agency guidelines based on NIST have drained scarce cybersecurity resources with duplicative exercises that provide no additional security

[7] https://www.gao.gov/products/gao-20-123

[8] https://www.hsgac.senate.gov/imo/media/doc/Testimony-Feeney-2017-06-21.pdf

benefit. Lack of cybersecurity personnel has already been a challenge, and conflicting and redundant compliance exercises are only making it worse. According to job aggregator CyberSeek, 522,000 cybersecurity jobs in the U.S. are currently unfilled[9], and that number could increase by 31 percent by 2029, according to the Bureau of Labor Statistics.[10] Plus, while there has been no evaluation of the Framework's effectiveness and cost-effectiveness.

NIST should look to the private sector's approach to evaluating cybersecurity decisions. Private organizations have found the lack of clear metrics as a challenge for the Framework, especially due to the lack of granular data to be able to tell the difference in maturity between the four risk tiers of the Framework.

Private organizations make empirical decisions based on economic data to set their cyber risk tolerance and set priorities for cybersecurity. These assessments primarily revolve around the economic cost of implementing controls versus the risk of economic loss as a result of a breach.

While the traditional compliance checklist models were the primary methods of evaluating cybersecurity at the Framework's inception, it is time to move toward these more advanced, empirical tools. Models such as Factor Analysis of Information Risk (FAIR) and X-Analytics are far more scientific and effective approaches to cyber risk assessment, translating cyber risk management into economic terms. NIST should leverage these tools as it looks to enhance the Framework in Version 2.0.

It is fair to conclude that the generic regulatory models that have grown up around NIST CSF are not the appropriate model for creating an effective and sustainable use of NIST CSF or creating a sustainable cybersecurity system. Instead, to the extent an organization is subject to cyber regulation, that regulation should assure the entities are using one of modern risk management models, such as X-Analytics and FAIR, which enable the organization to establish appropriate cyber risk management based on the unique threat posture and the economics of the organization. Fortunately, both X-Analytics and FAIR already map to NIST which should facilitate this evolution as to how NIST is used in the regulatory environment.

By evaluating the Framework on effectiveness and cost-effectiveness, we can begin to home in on what elements of the Framework can provide the most effective security.

Moreover, the federal government and NIST could go a long way in boosting our nation's overall cybersecurity by unifying and streamlining the federal government's approach to cybersecurity. A more unified government voice around the Framework's use across government could make the Framework more consistent and easier to use.

[9] https://threatpost.com/wiley-the-remote-work-transition-shifts-demand-for-cyber-skills/162019/

[10] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwj6mq2IyOn2AhVJSjABHZJDATYQFnoECAcQAQ&url=https%3A%2F%2Fwww.neit.edu%2Fblog%2Fcyber-security-job-outlook&usg=AOvVaw2ZOE5DzdKVv4C37nDj5vL7

Harmonizing the NIST Framework for Cloud Environments

Another area NIST should consider as it updates the Framework is the rapid adoption of cloud technology in the private sector.

As cloud adoption increases, the NIST Framework must become less datacenter/perimeter focused and more cloud/digital-native. While these concepts are similar, there is too much translation between the NIST requirements defined today and what security teams manage daily.

Section 2, Subsection 9 – What steps should NIST consider ensuring any update increases international use of the Framework? How can the Framework better align with international standards and models for cybersecurity, allowing organizations to more easily and effectively integrate new technology and services?

As outlined above, NIST could go a long way by helping harmonize the Framework's use across government agencies. Similarly, NIST could help advance the use of the Framework in the private sector by harmonizing it with popular standards and models already being used in the private sector.

Aligning International Approaches to Enterprise Risk Management

For example, NIST should align the CSF with its Integrating Cybersecurity and Enterprise Risk Management guidelines, which mirrors the popular enterprise risk management approaches being adopted by private sector corporate boards. NIST's Enterprise Risk Management guidelines view cybersecurity as more than an IT issue, aligning with the predominant model used in the private sector.

The National Association of Corporate Directors' Cyber-Risk Oversight Handbook outlines these same principles, identifying cybersecurity as a strategic enterprise risk. It urges organizations to establish an enterprise-wide cyber-risk management framework with adequate staffing and budget. These approaches have been adopted globally through organizations such as the Organization of American States, the European Confederation of Directors Associations, the Japanese Business Federation, the World Economic Forum, and more.

Moreover, these guidelines have been assessed and determined to be effective at improving overall enterprise cyber-risk management in the private sector.

An independent study from PricewaterhouseCoopers found that adopting the NACD model led to meaningful security improvements: "Boards appear to be listening to this guidance. This year we saw a double-digit uptick in Board participation in most aspects of information security. Respondents said this deepening Board involvement has helped improve cybersecurity practices in numerous ways. It may be no coincidence that, as more Boards participate in cybersecurity budget discussions, we saw a 24% boost in security spending. Other notable outcomes cited by survey respondents include identifying key risks, fostering an organizational culture of security, and better aligning cybersecurity with overall risk management and business goals."

NACD's 2020 Public Company Governance Survey, further corroborated the advancement of Enterprise Risk Management maturity among boards, with 79 percent of directors saying their board's understanding of cyber risk had significantly improved compared to two years prior.

By harmonizing the NIST CSF with the Enterprise Risk Management guidelines, which align private-sector NACD principles, NIST can speak with a consistent voice to approaches that are effective at enhancing security. These principles have been adapted to numerous international markets, taking a consistent approach can expand international use and interoperability, enabling organizations to integrate new technologies and services more effectively and securely to support their digital transformation efforts. Moreover, these approaches are being adopted at the management level as well. Textbooks – such as *Cybersecurity for Business: Organization-Wide Strategies to Ensure Cyber Risk is Not Just an IT Issue* – are now being adopted in business courses, bringing these paradigms of cybersecurity into the management level of enterprises.

Mapping the NIST CSF to ISO and Sector-Specific Needs

An area NIST should focus on is mapping the NIST CSF to the ISO standard, as it is the preeminent standard used internationally. Moreover, NIST should develop more detailed templates aligned to each of the critical infrastructure sectors.

The IT sector is unique from the Manufacturing sector, which is unique from the Telecom sector, and so on. While some work has been done in this area, the CSF in its current form is more an idea translated by third parties into how someone "feels" about their program, rather than a stronger instrument that can be used to truly verify and validate cybersecurity activity (e.g., SOC reports, ISO audits, etc.). NIST should undertake a more robust effort to develop detailed profiles and templates to help each of the critical sectors adapt the Framework to their specific needs.

Conclusion

ISA applauds NIST for moving the needle forward on the NIST Cybersecurity Framework by emphasizing the effectiveness of the Framework and identifying ways to streamline and harmonize disparate standards.

If you have any questions or want more information on the ISA's approach, please do not hesitate to reach out at [redacted]. We look forward to maintaining a robust public-private partnership with NIST to further improve the NIST Cybersecurity Framework.

Sincerely,

Larry Clinton
President and CEO
Internet Security Alliance