On February 22, 2022, NIST called for public comments to the "Framework for Improving Critical Infrastructure Cybersecurity" (the "NIST Cybersecurity Framework," "CSF" or "Framework") and a variety of existing and potential standards, guidelines, and other information, including those relating to improving cybersecurity in supply chains.

The Alliance for Digital Innovation (ADI) appreciates the opportunity to comment upon these critical guidance policies.

ADI is a coalition of customer-centric commercial technology companies focused on empowering Federal agencies to deliver the modern, secure, effective digital experiences that citizens deserve. Our mission is to aggressively drive digital modernization within government by breaking down institutional barriers, advocating for necessary change, and generating tangible results – for policymakers, for agency leaders and, most importantly, for our fellow citizens.[1]

The NIST Cybersecurity Framework was last updated in April 2018 [2] and consists of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to reduce cybersecurity risks. It is used widely by private and public sector organizations in and outside of the United States and has been translated into multiple languages, speaking to its success as a common resource.

Industry comments are also requested on the launch the National Initiative for Improving Cybersecurity in Supply Chains (NIICS) to address cybersecurity risks in supply chains. [3]

[1] Our members represent some of America's leading technology and cybersecurity companies, all of whom have joined ADI because of their desire to see the government acquire and leverage commercial capabilities to drive mission outcomes. Our members take the Framework seriously and must constantly stay aware of and defend against threats to their national and global supply chains, including their large partner networks.

[2] As NIST correctly notes, since 2018, much has changed in the cybersecurity landscape in terms of threats, capabilities, technologies, education and workforce, and the availability of resources to help organizations to better manage cybersecurity risk. With those changes in mind, NIST seeks to build on its efforts to cultivate trust by advancing cybersecurity and privacy standards and guidelines, technology, measurements, and practices by requesting information about the use, adequacy, and timeliness of the Cybersecurity Framework and the degree to which other NIST resources are used in conjunction with or instead of the Framework

[3] NIST describes this wide-ranging public-private partnership as focused upon identifying tools and guidance for technology developers and providers, as well as performance-oriented guidance for those acquiring such technology. To inform the direction of the NIICS, including how it might be aligned and integrated with the Cybersecurity Framework, NIST is requesting information that will support the identification and prioritization of supply chain-

ADI commends NIST on its transparency and industry engagement. Our comments are divided into two sections- General Observations and Specific Member Feedback to individual questions.[4]

ADI General Observations:

NIST should maintain the focus upon risk management and mitigation and not try to dictate specific outcomes- Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, our members believe that organizations must understand the likelihood that an event will occur and the potential resulting impacts. With this information, organizations can determine the acceptable level of risk for achieving their organizational objectives and can express this as their risk tolerance.

With an understanding of risk tolerance, our members can prioritize cybersecurity activities, enabling them to make informed decisions about cybersecurity expenditures. Implementation of risk management programs offers our members the ability to quantify and communicate adjustments to their cybersecurity programs.

The Framework uses risk management processes to enable organizations to inform and prioritize decisions regarding cybersecurity. It supports recurring risk assessments and validation of business drivers to help organizations select target states for cybersecurity activities that reflect desired outcomes. Thus, the Framework gives organizations the ability to dynamically select and direct improvement in cybersecurity risk management for the IT and ICS environments.

NIST should continue to maximize flexibility by using business incentives to drive implementation and deployment of the Guidelines- All of our members noted that the Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances. They also will vary in how they customize practices described in the Framework. Using this Framework, our members can determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent. Ultimately, our members recognize that the Framework is aimed at reducing and better managing cybersecurity risks and welcome this important focus.

NIST should focus upon enabling innovation- Our members agree that the Framework remains effective and supports technical innovation because it is technology neutral, while also referencing a variety of existing standards, guidelines, and practices that evolve with technology.

related cybersecurity needs across sectors. Industry responses will inform a possible revision of the Cybersecurity Framework as well as the NIICS initiative.

[4] Our members responded to many of the individual questions, but not all. Those individual comments are set forth in the second part of this document.

While the framework is clearly designed to be technology agnostic, there are tools and baseline controls that are discussed in a way that would be supportive in making the framework more accessible, especially by green organizations.

NIST must minimize overlap with existing standards and frameworks- Our members were uniform in the view that by relying on global standards, guidelines, and practices developed, managed, and updated by industry, the tools and methods available to achieve the Framework outcomes have the potential to scale across borders and thereby acknowledge the global nature of cybersecurity risks. This will allow them to evolve with technological advances and business requirements.

Our members believe that the use of existing and emerging standards will also enable economies of scale and drive the development of effective products, services, and practices that meet identified market needs. Market competition also promotes faster diffusion of these technologies and practices and the realization of many benefits by the stakeholders in these sectors.

In summary, our members are of the view that leveraging existing standards and frameworks to ensure that the elements proposed do not duplicate or contradict existing guidance for federal contractors is a key program objective.

We should accelerate the adoption of existing international standard- As NIST looks to develop guidelines pertaining to vulnerability disclosure, NIST should ensure that guidelines do not require companies to unnecessarily disclose information that, if exposed, could put customers at risk.

There needs to be a focus on harmonizing disparate and often conflicting cybersecurity and supply chain frameworks- Cybersecurity and supply chain prohibitions have a laudatory goal. Our members are unform in not wanting to see American IT products and services riddled with foreign technologies that allow foreign surveillance or national security espionage.

However, as these various cybersecurity and supply chain regulatory regimes proliferate (CMMC/Section 889/FASC, etc.), they do so with inconsistent applicability standards, waiver procedures, and administrative compliance requirements.

We would strongly encourage NIST to continue taking a leadership role in promulgating a comprehensive cybersecurity and supply chain security and compliance regime that considers all necessary laws, regulations, and policies. Doing so would significantly improve the level of consistency across numerous Federal agencies each seeking to implement these new and oftentimes conflicting requirements and deadlines.

Further, such a comprehensive approach would greatly benefit industry, who is beholden to various and sometimes incomplete information from the various authorities in charge of these unique legal and regulatory programs.

Focus upon small business impacts and costs- In all these cybersecurity and supply chain rules, the administrative cost associated with compliance would disproportionately impact small business and stifle government's access to innovative technologies.

Further, any exclusion or removal orders that may be required of Federal agencies could have disparate impacts on businesses of all sizes that might work in a non-governmental capacity with any banned entity, further complicating business relationships for small businesses.

NIST should continue and expand the focus upon privacy and individual liberties- Recognizing the role that the protection of privacy and civil liberties plays in creating greater public trust, the Framework includes a methodology to protect individual privacy and civil liberties when critical infrastructure organizations conduct cybersecurity activities.

Many organizations already have processes for addressing privacy and civil liberties. The methodology is designed to complement such processes and provide guidance to facilitate privacy risk management consistent with an organization's approach to cybersecurity risk management. Integrating privacy and cybersecurity can benefit organizations by increasing customer confidence, enabling more standardized sharing of information, and simplifying operations across legal regimes.

Response of individual ADI members to specific questions by NIST

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.*

This Framework addresses a challenging area - companies must always look to balance cost pressures, legislative pressures, and risks. There is an opportunity for the NIST Framework to help articulate this better--- but also to push companies to the minimum acceptable baseline.

In general, our members believe that the Framework is an excellent document, but universally observe that while it is a good start on the journey-- but not the destination.

More specifically, one member notes the Framework, and its five categories lack guidance on widely recognized identity and access standards. While things like MFA and Zero Trust have been named in the Administration's executive orders, the Framework has left these gaps.

Specific areas where additional guidance would be helpful include:

- IDAAS
- AaaS
- RBAC (Role Based Access Control) this is a very changed concept from the way it's described in the CSF - which also ties into cloud below.

One member also asked about modern architectures such as identity-based architectures and asked, "Shouldn't these also be addressed?" An issue was also raised about contextual based access control, specifically what about zero trust and continual authentication?

Overall, our members suggested that there is a lack of cloud focus (hence the lack of SaaS, IDaaS etc.) and wondered how does using the cloud might change the NIST Framework overall?

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?

Our members addressed this question by highlighting the diverse nature of their architectures. They asked for additional clarity regarding "shared responsibility" architectures- specifically technologies and deployments that include architectures encompassing multi-tenant approaches and the impact on the concept of "least privilege."

Many of our members are invested in diverse architectures involving various types of tenants, and must accommodate issues surrounding tenants' allocation, multi-tenant cloud and other complex situations. They asked us "what are the pros and cons of these types of architectures and how does NIST change the risk assessment model in light of these structures?"

One member offered that the Frameworks' standardized and repeatable process allows agencies to orient themselves within the CSF process, use standardized terminology during inter-agency communication, and share best practices.

Furthermore, as cybersecurity risks increase for small to medium-sized businesses, federal agencies benefit from supply chain partners incorporating the CSF to address the cybersecurity supply chain weaknesses or key considerations regarding privacy, risk, supply chain risk management, or sensitive information.

2. *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).*

Most companies coming to the Framework are looking for a "baseline" that they can build a security program against. This baseline should consider the key elements needed and the Framework would benefit from greater organizational clarity in identifying these key elements in a succinct fashion.

Our members commented that the Framework is much more helpful if it is consumable. One member recommended that NIST should keep the Framework to 21 pages, thereby not making the Framework more complicated. Our members commented that there is room for NIST to improve its "consume ability." ADI, as a group, believes that there is a good opportunity here for our members to work with NIST to support make the framework more "consumable"

and we offer our participation with NIST to assist in this endeavor.

In this regard, one member suggested that we (ADI) work with NIST to identify and assign "CSF Ambassadors" who can help organizations adopt the principles. Our focus would be upon assisting bigger organizations to make the CSF more relevant to smaller organizations --who in combination make up a great impact to the economy.

Our members welcome the opportunity to guide smaller, less mature organizations to identify best practices in measuring their risk. For example, what are some best practice approaches? What are good maturity metrics - especially ones that can be used by smaller organizations?

This was an area of great membership interest.

3. *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.*

One recurrent comment from the ADI members was the omission of guidelines regarding data. Specific comments asked about data retention best practices, for example regarding logs and system audits. There is no directive to keep this data for longer than 30 days.

The average time to find a breach is more than 150 days and log data of 30 days would not be useful in the average incident.

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.

One member advocated for the following improvements to specific metrics:

● IDENTIFY Governance (ID.GV) category- consider updating the CSF to include considerations for accounting for organizational software and systems and the resources necessary to perform RMF. This consideration forces organizations to pause and institute capabilities that have already received federal accreditations or include automated tools for threat prevention or inheritance of security controls.

● IDENTIFY Risk Assessment (ID.RA) category- consider updating the Framework to include considerations for the organizational threat and risk threshold and mitigation capabilities and techniques. For instance, once an organization creates its threat, risk, and capability baselines, it

can perform a cost-risk analysis to identify organizational and capability vulnerabilities and learn about emerging threats and technologies.

● IDENTIFY Supply Risk Management (ID.SC) category- Updating and integrating the Framework with the SCRM framework would incorporate SCRM best practices and raise organizational awareness on which corporate software and systems will require internal teams to apply SCRM and mitigate risks from second and third-order security vulnerabilities.

These efforts would increase the organization's understanding of NIST's critical software and Software Bill of Material (SBOM) development.

Relationship of the NIST Cybersecurity Framework to Other Risk Management Resources

7. *Suggestions for improving alignment or integration of the Cybersecurity Framework with other NIST risk management resources. As part of the response, please indicate benefits and challenges of using these resources alone or in conjunction with the Cybersecurity Framework. These resources include:*

- *Risk management resources such as the NIST Risk Management Framework, the NIST Privacy Framework, and Integrating Cybersecurity and Enterprise Risk Management (NISTIR 8286).*
- *Trustworthy technology resources such as the NIST Secure Software Development Framework, the NIST Internet of Things (IoT) Cybersecurity Capabilities Baseline, and the Guide to Industrial Control System Cybersecurity.*
- *Workforce management resources such as the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity.*

One of our members offered specific observations in this regard.

They noted that throughout these various frameworks, aligning, considering, and integrating the specific practices and frameworks, were referenced over 400 times. They recommended harmonizing the following NIST Frameworks so that Federal agencies and companies can have a modernized Integrated Cybersecurity-RMF (IC-RMF):

● Zero Trust Framework1

● Risk Management Framework2

● Privacy Frameworks

● Cybersecurity Framework

● Supply Chain Risk Management Framework

● NISTIR 7621 Revision 14

- NIST SP 800-53 Rev.55

- CISA Zero Trust Framework 6

- Cybersecurity Maturity Model Certification (CMMC)

In this manner, the NIST Zero Trust Framework would act as the overarching strategy to incorporate the remaining frameworks to iteratively apply each framework to the Zero Trust Pillars.

Along with this evaluation methodology and criteria, there should be a maturity model like CMMC—not to just implement more controls—but on the methodology's ability to continuously improve, assess, and mature the organization's cybersecurity program. In this modern integrated cybersecurity framework, common security controls would include the evaluation methodologies, interpretations, and examples based on its organizational program, i.e., FedRAMP, CMMC, Private Sector, and self-attestation.

8. Use of non-NIST frameworks or approaches in conjunction with the NIST Cybersecurity Framework. 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? Are there ways to improve alignment or integration of the NIST framework with other frameworks, such as international approaches like the ISO/IEC 27000-series, including ISO/IEC TS 27110?

9. There are numerous examples of international adaptations of the Cybersecurity Framework by other countries. The continued use of international standards for cybersecurity, with a focus on interoperability, security, usability, and resilience can promote innovation and competitiveness while enabling organizations to more easily and effectively integrate new technologies and services. Given this importance, what steps should NIST consider to ensure any update increases international use of the Cybersecurity Framework?

10. References that should be considered for inclusion within NIST's Online Informative References Program. This program is an effort to define standardized relationships between NIST and industry resources and elements of documents, products, and services and various NIST documents such as the NIST Cybersecurity Framework, NIST Privacy Framework, Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53), NIST Secure Software Development Framework, and the NIST Internet of Things (IoT) Cybersecurity Capabilities Baseline.

Cybersecurity Supply Chain Risk Management

11. National Initiative for Improving Cybersecurity in Supply Chains (NIICS). What are the greatest challenges related to the cybersecurity aspects of supply chain risk management that the NIICS could address? How can NIST build on its current work on supply chain security, including software security work stemming from E.O. 14028, to increase trust and assurance in technology products, devices, and services?

Our members recommend that NIST continue to be as inclusive as possible when establishing the NIICS. Additionally, our embers recommend identifying technologies that enforce and support C-SCRM to mitigate supply risk and dependency on technologies that are developed or out-sourced by third parties and implementing an evaluation program that goes in depth into validating supply chain evaluation/management. One member identified Jason Weiss, former DOD Chief Software Officer, to be an advisor for software supply chain management.

Our members were also uniform in their view that the Framework provides opportunity to talk about supply chain risk. One recurrent them was to embrace the automation of access though to automation of code and CI/CD platforms. One persistent question was what are the types of supply chain risk? How do you evaluate supply chain risk? How does SBOM play into managing this?

Guidance from NIST is a welcome addition to these difficult issues.

12. Approaches, tools, standards, guidelines, or other resources necessary for managing cybersecurity-related risks in supply chains. NIST welcomes input on such resources in narrowly defined areas (e.g., pieces of hardware or software assurance or assured services, or specific to only one or two sectors) that may be useful to utilize more broadly; potential low risk, high reward resources that could be facilitated across diverse disciplines, sectors, or stakeholders; as well as large-scale and extremely difficult areas.

On this point, one member observed that there is an opportunity for NIST to identify "Baseline Tools"- such as the MITRE ATT&CK framework. These tools will help organizations greatly in identifying gaps. This is both an opportunity and needs to be covered in more detail by the Framework.

13. Are there gaps observed in existing cybersecurity supply chain risk management guidance and resources, including how they apply to information and communications technology, operational technology, IoT, and industrial IoT? In addition, do NIST software and supply chain guidance and resources appropriately address cybersecurity challenges associated with open-source software? Are there additional approaches, tools, standards, guidelines, or other resources that NIST should consider achieving greater assurance throughout the software supply chain, including for open-source software?

14. Integration of Framework and Cybersecurity Supply Chain Risk Management Guidance. Whether and how cybersecurity supply chain risk management considerations might be further integrated into an updated NIST Cybersecurity Framework—or whether and how a new and separate framework focused on cybersecurity supply chain risk management might be valuable and more appropriately be developed by NIST.

In general, our members discussed the fact that there are currently many content assets already exist for CSF, but the landscape is noisy. They discussed how can industry make this easier for our customers?

Is there room for “supporting tooling”? This does not need to be complex, just something that indicates what coverage an organization gets from customization.

On behalf of the Alliance for Digital Innovation, we appreciate this opportunity to offer our comments and suggestions.