April 25, 2022

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

RE: NIST Cybersecurity RFI [Docket No. 220210–0045]

Zscaler, Inc. respectfully submits these comments in response to the National Institute of Standards and Technology (NIST) Request for Information (RFI) on the Framework on Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework). As a FedRAMP-accredited Cybersecurity Service Provider, Zscaler delivers secure cloud computing services to many types of organizations, including US Federal agencies and Fortune 500 companies worldwide.

Zscaler's mission is to secure the cloud so that organizations can realize the full potential of the cloud and mobility by securely connecting users to applications anywhere, from any device. Zscaler provides user/mission experience (ZDX), cloud-to-cloud security (CSPM), and internet and private access (ZIA & ZPA) Security Service Edge (SSE) capabilities widely used across the Federal government to meet Federal Zero Trust mandates.

Zscaler Cloud Services

Zscaler's multi-tenant cloud security platform applies policies set by each agency to securely connect the right user to the correct application. Unlike traditional hub-and-spoke architectures, which backhaul traffic over dedicated Wide Area Networks (WANs) to centralized gateways, this solution routes traffic locally and securely to the internet over broadband and cellular connections.

- **Zscaler Internet Access-Government (ZIA GOV)** securely connects users to externally managed applications, including SaaS applications and internet destinations, despite location, device, or network. ZIA—Zscaler's "TIC in the Cloud solution"— is FedRAMP-Moderate authorized and in-process for FedRAMP-High.

- **Zscaler Private Access-Government (ZPA GOV**) offers authorized users secure and fast access to internally managed applications hosted in enterprise data centers or the public cloud. ZPA is our "Zero Trust Networking Access (ZTNA) solution," and is FedRAMP-High authorized.

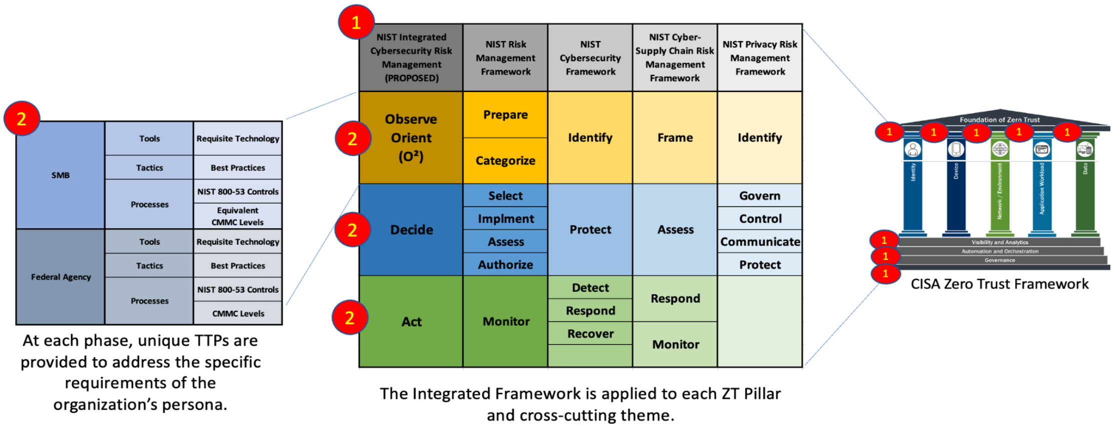
Zscaler General Comments

1. Modernized Integrated Framework.

Throughout the NIST RMF, CSF, SCRM, and Privacy frameworks, aligning, considering, and integrating the specific practices and frameworks, were referenced over 400 times. Zscaler recommends harmonizing the following NIST body of work so that Federal agencies and companies can have a modernized Integrated Cybersecurity-RMF (IC-RMF):

- Zero Trust Framework[1]
- Risk Management Framework[2]
- Privacy Framework[3]
- Cybersecurity Framework
- Supply Chain Risk Management Framework
- NISTIR 7621 Revision 1[4]
- NIST SP 800-53 Rev.5[5]
- CISA Zero Trust Framework[6]
- Cybersecurity Maturity Model Certification (CMMC)[7]

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. Additionally, since NIST RMF and CSF were tailored primarily for government and commercial audiences, the newly established 'IC-RMF' should earmark the best technology and practices for commercial businesses (SMB) and government entities.



SMB	Tools	Requisite Technology
	Tactics	Best Practices
	Processes	NIST 800-53 Controls
		Equivalent CMMC Levels
Federal Agency	Tools	Requisite Technology
	Tactics	Best Practices
	Processes	NIST 800-53 Controls
		CMMC Levels

At each phase, unique TTPs are provided to address the specific requirements of the organization's persona.

NIST Integrated Cybersecurity Risk Management (PROPOSED)	NIST Risk Management Framework	NIST Cybersecurity Framework	NIST Cyber-Supply Chain Risk Management Framework	NIST Privacy Risk Management Framework
Observe Orient (O^2)	Prepare	Identify	Frame	Identify
	Categorize			
Decide	Select	Protect	Assess	Govern
	Implment			Control
	Assess			Communicate
	Authorize			Protect
Act	Monitor	Detect	Respond	
		Respond		
		Recover	Monitor	

The Integrated Framework is applied to each ZT Pillar and cross-cutting theme.

CISA Zero Trust Framework

Figure 1: Proposed NIST Integrated Cybersecurity Risk Management

[1] NIST SP 800-27, Zero Trust Architecture, 2022
[2] NIST Risk Management Framework
[3] NIST Privacy Framework
[4] NISTIR 7621 Revision 1, Small Business Information Security: The Fundamentals
[5] NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations
[6] Memorandum for the Heads of Executive Departments and Agencies (M-22-09)
[7] Securing the Defense Industrial Base (CMMC 2.0)

2. Stronger Together.

Zscaler appreciates NIST’s continuous industry engagement and invitation to provide a diverse perspective. Only by viewing and approaching cybersecurity from different vantage points can Federal and commercial entities reinforce their security posture. No longer is it enough to have a strong perimeter. We must continuously learn from each other to protect our families, organizations, and nation from adversaries. Zscaler encourages NIST to continue prioritizing broad discussions on essential topics and establishing entities, e.g., NIICS, to develop stronger ties with industry partners who support a broad customer base.

3. Technologically Aware.

The Cybersecurity Framework should be vendor agnostic. However, Zscaler believes that cybersecurity, technology, and risk are at a nexus where modern frameworks should encompass, or at a minimum acknowledge, cybersecurity best practices, technological tools, and security controls.

4. Small Business Impact.

Zscaler has a genuine appreciation for NIST support for small businesses. Like larger organizations, small businesses must prioritize security against compliance costs but with smaller budgets. As such, Zscaler recommends NIST provide SMBs not only with the frameworks to achieve a more substantial level of cybersecurity but include recommended vendor-neutral resources like GSA.

5. International Partnership.

Establishing the National Initiative for Improving Cybersecurity in Supply Chains (NIICS) is a significant step toward addressing cybersecurity risks in supply chains. In addition, NIST should consider establishing an international version of NIICS that supports public-private partnerships to foster trust and knowledge transfer across various domains and mitigate supply chain risks. Such an effort could be a catalyst for developing an internationally integrated cybersecurity framework.

Zscaler Specific Responses to NIST Questions:

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.

(ZS) NIST's five functions provide organizations with a straightforward repeatable process for assessing an organization's current and target cybersecurity posture and a standardized way to communicate cybersecurity risk and mitigation progress to stakeholders (internal and external).

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 in the number of potential ways to manage risks? What might be relevant metrics for improvements to cybersecurity because of the implementation of the Framework?

(ZS) The CSF's standardized and repeatable process allows agencies to orient themselves within the CSF process, use standardized terminology during inter-agency communication, and share best practices. Since cybersecurity and its frameworks evolve from public-private collaboration, the cybersecurity community benefits from the CSF's unbiased, vendor-neutral approach to cybersecurity. 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.

(ZS) Relevant metrics for cybersecurity include detailed risks based on ratings developed by leadership and technical consensus (informational, thresholds that are low, medium, high). Upon reviewing the CSF, Zscaler noted the following relevant improvements:

- IDENTIFY Governance (ID.GV) category:
  - 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:
  - Updating the CSF 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. Zscaler has found that some customers or

industries are heavily prepared for specific cyber-attacks but vulnerable to others during our tenure.

- IDENTIFY Supply Risk Management (ID.SC) category:
    - Updating and integrating the CSF 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[8] and Software Bill of Material (SBOM)[9] development.

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).

(ZS) Despite NIST's ongoing industry outreach, challenges to extensive use of the NIST Cybersecurity Framework may be interpreting the CSF's purpose. CSF version 1.1 states: "While this document was developed to improve cybersecurity risk management in critical infrastructure, the Framework can be used by organizations in any sector or community.[10]" However, in light of the updated EO 14028, *Improving the Nation's Cybersecurity*, perhaps it would be worth removing the emphasis on Critical Infrastructure (CI) cybersecurity and aligning more closely to EO 14028, especially since EO 14028 reinvigorated numerous cybersecurity policies and initiatives.

(ZS) Along with reframing the CSF to EO 14028's context, another challenge to broader use of the NIST may be differing levels of expertise or experience personnel may have when utilizing the NIST CSF. Compounding this issue may be industries regarding NIST as a supplemental resource and using OMB guidance, DOD publications, etc., as their primary authoritative body of knowledge. To thwart misunderstanding and reach a broader audience, Zscaler encourages NIST to develop training on effectively applying the cybersecurity framework and its correlation and impact on other NIST frameworks.

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.

(ZS) Please see the following:

- General Comment 1: Modernized Integrated Framework
- Question Response 2: Relevant metrics using the NIST CSF

[8] NIST Critical Software Definition
[9] NIST Software Bill of Material
[10] NIST Framework for Improving Critical Infrastructure Cybersecurity

5. Impact on 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.

(ZS) Since the NIST CSF can be customized and tailored to each agency's unique environment, requirements, and threat profile, Zscaler recommends considerations be made regarding the usability and applicability of specific security technologies that close security gaps and achieve a Zero Trust Architecture.

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

(ZS) When evaluating potential improvements to the Cybersecurity Framework, NIST should continue maintaining vendor-neutral and performance-based approaches that encourage innovation, automation, and modern technologies. In particular, the Cybersecurity Framework should do its best to discourage the use of legacy technology solutions that carry greater potential for human error, false positives, and system and security control misconfiguration, versus more modern approaches.

(ZS) Incorporating an automation category within each CSF function would modernize the CSF so that Federal agencies consider and take advantage of security technologies to identify risks and optimize the risks management process in place. By taking advantage of Continuous Diagnostics & Mitigation (CDM)[11] security technologies, Federal agencies can utilize API integrations, platform dashboards, and tools to manage security, risk, and supply chain risk management practices for Federal Information Systems and organizations.

[11] Continuous Diagnostics & Mitigation (CDM) Program, 2022

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 the 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.

(ZS) Please see General Comment 1: Modernized Integrated Framework

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?

(ZS) Zscaler recommends the following non-NIST frameworks:

1. MITRE ATT&CK[12]
2. Cyber Kill Chain [13]

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 ensuring any update increases international use of the Cybersecurity Framework?

(ZS) At an international level, it would be great to establish a NIST-coalition to evaluate, pare down, and integrate the extensive list of frameworks, control listings, etc. into a clear, concise, and consolidated framework and information library so that implementers can develop a common understanding and applicability of cybersecurity practices.

[12] MITRE ATT&CK, 2022
[13] Cyber Kill Chain, 2022

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.

(ZS) Zscaler recommends adding NIST SP 800-207 - Zero Trust Architecture[14] and NIST Privacy Framework 1.0[15], as the NIST Supply Chain Risk Management and Cybersecurity Framework, intersect with the ZTA and Privacy framework at the strategic and tactical level, respectively. Each framework complements the other to achieve a higher level of security posture.

[14] NIST SP 800-27, Zero Trust Architecture, 2022
[15] NIST Privacy Framework

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?

(ZS) Like previous NIST groups, Zscaler recommends NIST continue to be as inclusive as possible when establishing the NIICS. Additionally, Zscaler recommends 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. Also, it would be great to have Jason Weiss, former DOD Chief Software Officer, as an advisor for software supply chain management.

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.

(ZS) As some of the vendor community has capitalized on the misunderstanding of common terminologies like cybersecurity and "Zero Trust," can NIST provide federal agencies a workshop or a more robust definition/standard around the "Zero Trust" approach and its correlation to cybersecurity?

(ZS) As federal agencies heavily invest their resources to vet and make available specific capabilities, can NIST harmonize its frameworks and best practices with the offerings of GSA and other federal programs? This blend of frameworks, best practices, and toolsets provides the cyber-community defense-in-depth with layered due diligence. For instance, Zscaler recommends using security technologies from GSA's Continuous Diagnostics & Mitigation (CDM) program when needing tools to monitor security vulnerabilities and supply chain risks continuously. Furthermore, Zscaler recommends utilizing StateRAMP or FedRAMP-accredited standardized platforms, as they adhere to NIST controls, Continuous Monitoring (ConMon), and Third-party assessments. Finally, Zscaler recommends leveraging Zero Trust Architecture security capabilities that enforce and support the MITRE ATT&CK and Cyber Kill Chain frameworks. These non-NIST frameworks allow Federal agencies to incorporate modern security frameworks throughout the CSF for an onion-style defense-in-depth security posture.

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?

(ZS) Upon reviewing the latest cybersecurity supply chain risk management guidance, Zscaler recommends developing guides—not additional frameworks—that explain how an organization can adopt new technologies. For example, an organization that decides to adopt IoT devices will have the nested guidance on incorporating the framework, identifying associated security controls, and evaluation methodology and criteria; all in accordance with the organization's unique requirements to establish specific controls to close or narrow the new security gaps. Concurrently, Zscaler recommends instituting a NIST technical team that actively lab, test, and challenge these "guides" with purple teams using a proven methodology like MITRE ATT&CK.

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.

(ZS) Because the NIST CSF and C-SCRM can be used in a modular fashion, Zscaler recommends the next iteration of the NIST CSF include recommendations for when the organization can utilize CSF or C-SCRM best practices within each publication.