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

120 Holger Way, San Jose, CA 95134 USA
www.zscaler.com

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

120 Holger Way, San Jose, CA 95134 USA
www.zscaler.com

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.

120 Holger Way, San Jose, CA 95134 USA
www.zscaler.com

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.

120 Holger Way, San Jose, CA 95134 USA
www.zscaler.com