To the NIST team,

CyberArk is honored to provide feedback on NIST CSF 2.0 Concept paper. Listed below are comments across several key sections of the concept paper for your consideration.

For any questions please feel free to reach out to the following individuals:

- Amita Potnis: [redacted]
- Ernie Rhyne: [redacted]
- Troy Grubbs: [redacted]

Warm regards,

CyberArk team.

CyberArk feedback on NIST CFS 2.0 Concept paper	
NIST CSF 2.0 Concept Paper Sections	**CYBR Feedback**
1.2. Scope the CSF to ensure it benefits organizations regardless of sector, type, or size	• The federal agencies/government may already have a cybersec framework for certain sectors, like for Fintech. Other than international collab, a tool that can map their controls with CSF functions and categories will be helpful
2.1. Retain CSF's current level of detail	• A new category under 'Protect' function can be 'Data Privacy'. This will provide more visibility rather than being covered under 'Data Security'
2.5. Use Informative References to provide more guidance to implement the CSF	• Sometimes the implementation steps are abstract. While the new mappings will help, an exhaustive checklist sample of implementation steps can be handy
2.6. Remain technology- and vendor-neutral, but reflect changes in cybersecurity practices	• "Identity management" is mentioned. In the context of this paper (cyber security), we can suggest Identity security (which is unlikely to be accepted) or securing identities throughout their lifecycle • We need to keep an eye on this paper and feedback - https://csrc.nist.gov/publications/detail/sp/800-63/4/draft , https://csrc.nist.gov/News/2022/nist-draft-revision-4-of-sp-800-63 • As part of the controls under ZTA, how can risk scoring (context based, real time and available as part of technology) be measured, standardized, and integrated into the guidance in the future? • Suggestion to NIST that the revised paper includes more examples of hybrid-Cloud models. In many cases, recommendations are given in a vacuum (e.g., OT, On-Prem, and Cloud) but most organizations today fall into an increasingly homogenous blend of the above environments creating the need to blend recommendations
4.1. Add a new Govern Function	• It is good to see "Govern" is considered as an additional Function. It makes sense to move the sub-categories ID.GV-1 - : Organizational cybersecurity policy, ID-GV.2 - Cybersecurity roles and

	responsibilities, ID.GV-3 - Legal and regulatory requirements and ID.GV-4: Governance and risk management processes to elevate as new categories under Govern function. We can consider adding following categories. A. **Exceptions management or whitelisting of resources.** In real adoption of cloud security, there are often cases where customers define the exceptions or whitelist certain resources to exclude from the cybersecurity policies. And in majority of the time this gets un-managed. It is good to have some process defined around this area. **B. Notification and Alerting:** As part of governance, it is crucial to define the appropriate notification and alerts for the right set of policies. **C. Continuous Monitoring.** One of the key items under governance is continuously monitor the security hygiene. **D. Incident Response & business continuity.** It is crucial to define incident response plan and continuity plans as part of governance.
5.1. Expand coverage of supply chain	• One item in the proposal is critical— expanding pursuant to the SSDF publication, guidance around first-party supply chain risk. We have seen a few cases where the teams responsible for implementing the first party controls are not the same ones diving deep into supplemental NIST publications, so repetition here is exceptionally good. • Thinking about first-party developers got me noodling on it— somewhere in this publication (likely zero-trust) there should be some mention of extending controls that are commensurate with the level of risk. All too often security teams will implement the controls through constraint for dev work which, while looking good on paper, ends up creating developer fatigue and animosity, leading to other common practices being ignored.
6. CSF 2.0 will advance understanding of cybersecurity measurement and assessment	• Suggest that examples are given for how security capabilities can be achieved by configuring or enabling security features within a technology stack. For example, by enabling the policy engine, audit, recording, and analytics feature of a ZTA based tool, can an auditor conducting security assessments mark the NIST ZTA controls as complete? Is there a need to provide specific evidence or will the proof of enabling the technology and the feature pack suffice?

About CyberArk:

CyberArk applies intelligent privilege controls to all identities – human & machine – with continuous threat detection and prevention across the entire identity lifecycle. With CyberArk, organizations can enable Zero Trust and least privilege with complete visibility, ensuring that every identity can securely access any resource, located anywhere, from everywhere – with a single Identity Security Platform.

CyberArk is the pioneer of Privileged Access Management, CyberArk has the most advanced and secure technology and enables the same privilege controls across the entire identity lifecycle. With thousands of deployments & a vast partner ecosystem, CyberArk has the technology, experience, expertise and innovation track record to address the broadest range of Identity Security requirements.