DIGITAL DIRECTORS NETWORK

Bob Zukis
Chief Executive Officer
[redacted]
[redacted]

March 3, 2023

National Institute of Standards and Technology (NIST)
Gaithersburg, MD USA

Re: **NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework**

Ladies and Gentlemen of the NIST CSF 2.0 Working Group,

We are pleased to provide our comments on the proposed NIST CSF 2.0 Concept paper**.**

We are a curated network of over 1,100 U.S. technology executives and corporate directors working exclusively on advancing leading boardroom policies and practices in cyber governance. We are the leader in advancing these issues in America as this was our founding mission when we launched in October of 2017. Our executive network includes CIOs, CISOs, CROs, and corporate directors from some of America's leading public and private companies and boardrooms.

Our opinions reflect the most developed perspective and body of work on cyber governance in America.

Digital Directors Network (DDN) Comments on NIST CSF 2.0

The NIST Cybersecurity Framework (CSF) is an influential tool with wide private sector adoption. We believe that expanding CSF to create a *Govern* crosscutting function is not only a critical addition but a necessary step to strengthen America's collective security model. Along with helping cybersecurity teams, boardrooms and executives integrate governance throughout the complex cybersecurity system, CSF 2.0 must also help teams understand systemic risk within the complex digital business system to address the distributed nature of cybersecurity risk facings America's companies, investors and consumers.

Effective governance in complex information systems needs to fulfill several key objectives that works towards a goal of digital trust: Leadership, Transparency, Accountability, Assurance, Stakeholder Management and Effectiveness.

Foundationally, the opportunity with CSF 2.0 is to reframe digital governance as a collective security model that introduces a new paradigm that can address the nature of distributed risk that is inherent in the digital systems that power much of the modern world. Transparency and the proper understanding of the nature of issue is the starting point of the NIST CSF 2.0 emphasis on governance.

DIGITAL DIRECTORS NETWORK

Bob Zukis
Chief Executive Officer
[redacted]
[redacted]

Systemic cyber risk is an inherent aspect of complex digital systems and a core requirement of any governance framework that would comprise the foundation of NIST CSF 2.0. The importance of this is reflected in the just released National Cybersecurity Strategy.

The National Cybersecurity Strategy released by The White House on March 1, 2023 emphasizes the importance of this when it says:

> *Our goal is a defensible, resilient digital ecosystem where it is costlier to attack systems than defend them, where sensitive or private information is secure and protected, and where neither incidents nor errors cascade into catastrophic, systemic consequences.*[1]

Systemic cyber risk in complex digital systems is a material aspect of cybersecurity that is also underdeveloped as a management practice. This DDN working group recommends that NIST CSF 2.0 reflect the range of governance objectives previously mentioned, but that its initial focus be on *Transparency*, in order to frame the problem in the proper systemic context.

We have attached two papers that explain these issues in further detail that will also introduce the only framework that has been developed to address systemic risk in the complex digital system at the corporate board governance level. Please see "Systemic Digital Risk: Understanding And Overseeing Complex Digital Environments With The DiRECTOR™ And RISCX™ Frameworks" and "Digital and Cybersecurity Governance Around the World", which was published in the 'Annals of Corporate Governance: Vol. 7, No. 1, pp 1–92. DOI: 10.1561/109.00000032'.

The DiRECTOR™ and RISCX™ frameworks have been developed by practitioner leaders and have been taught to several hundred of America's digital and governance leaders. It is also beginning to be implemented into enterprise risk management practices for some of America's leading companies.

The DiRECTOR™ and RISCX™ frameworks provide a structured way to understand and govern risk within the complex digital business systems that power a growing proportion of economic output and competitive advantage. The other aspects of governance within NIST CSF 2.0 should build upon this foundation.

The application of the overall model can reveal significant gaps in understanding component and systemic risk throughout the digital business system. The model is intended to be applied at any level within an organization including project, objective, functional or enterprise. The model is designed to be applicable to any organization or industry to enable a deeper understanding of how systemic digital risk exists and threatens the ability to support and deliver business value.

[1] National Cybersecurity Strategy, The White House, March 2023 https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

DIGITAL DIRECTORS NETWORK

Bob Zukis
Chief Executive Officer
[redacted]
[redacted]

In the proposed NIST CSF 2.0 model, a *Govern* function will help the security teams that implement CSF manage the environment; however, without specific and well-understood level of transparency across and entire ecosystem, enterprise and complex digital system, it will not help identify and mitigate risk in a distributed risk environment.

The emergence of systemic cyber risk also requires every public and private company to strengthen their cyber governance, not just a few. Cyber risk that can start in one organization can rapidly move between companies as was experienced with the SolarWinds breach. Attackers are increasingly looking to exploit systemic cyber risk in this manner.

Effective governance over any issue also starts with the competencies of those with governance responsibilities. A useful model should also be able to be repurposed across multiple objectives in governance. The DiRECTOR™ framework is also a strong competency model that reflects the domain knowledge needed from the corporate boardroom and beyond needed to fulfill the Accountability objective of digital governance.

In summary, we reiterate our strong support for the broader concept paper and are pleased to provide our initial comments. We've already been working to advance this issue over the last five years and our support and comments come from our depth of experience and informed insights on this issue. We are America's leader in digital and cyber risk governance, and your proposal, along with our recommendations, has the strong support of the more than 1,100 technology and cyber leaders who are our members.

America's investors, consumers, and stakeholders expect and deserve the companies they do business with to have a secure infrastructure, cyber competent boardrooms, and a comprehensive approach to governing systemic risks in the complex digital systems that serve them that is reliable and trustworthy. NIST CSF 2.0 needs to fulfill this objective, and it begins with Transparency into the complex system.

Thank you for your attention and please contact me if you would like to discuss these views.

Sincerely,

Bob Zukis
CEO, Digital Directors Network