[redacted]

March 17, 2023

Cybersecurity Framework Team
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

RE: Cybersecurity Framework NIST 2.0: Recommended Updates

On behalf of the Network Perception team, I would like to express our sincere gratitude for your efforts in reaching out and seeking input from the market in updating the Standard NIST 2.0. I believe that this new version will play a crucial role in emphasizing the importance of cybersecurity governance, supply chain risk management, strengthening cybersecurity practices, and helping organizations protect their sensitive data from various cyber threats.

As a leading provider of OT network security and compliance solutions, Network Perception appreciates the opportunity to share our thoughts and suggestions with you regarding the NIST 2.0 update. I recognize that the standard results from extensive research and consultation with industry experts. Network Perception is honored to be part of this collaborative effort.

I strongly believe that the updated standard should continue to focus on risk-based approaches to cybersecurity, with an emphasis on cyber resiliency and automation. Therefore I recommend that the standard highlights the importance of continuous verification and assessment of networks and systems, which is essential in protecting against and recovering from cyber attacks.

The two areas of the Jan. 19, 2023 Concept Paper for which Network Perception would like to provide input are the following:

- Section 2. CSF 2.0 will remain a framework, providing context and connections to existing standards and resources
    - 2.6 Remain technology- and vendor-neutral, but reflect changes in cybersecurity practices
- Section 4. CSF 2.0 will emphasize the importance of cybersecurity governance
    - 4.1 Add a new Govern Function

Feedback on subsection 2.6 "Remain technology- and vendor-neutral, but reflect changes in cybersecurity practices"

We fully agree with the statement from subsection 2.6 that CSF 2.0 has to remain technology- and vendor-neutral while recognizing that the technology landscape is evolving. To that end, we would like to highlight recent technology innovations that enable organization to improve the comprehensiveness of their IT / OT network visibility.

network perception

[redacted]

Background

Organizations worldwide are maturing their cybersecurity program and the concept of cyber resiliency is now well accepted. NIST publication SP.800-160v2r1 on developing cyber-resilient systems defines visibility as maintaining useful representations of mission and business dependencies and the status of resources with respect to possible adversity. In the context of critical infrastructure, this requires an understanding of dependencies among cyber systems and critical operations:

- On which cyber systems critical operations depend,
- How those systems connect, and
- How communications are controlled.

NIST publication SP.800-160v2r1 defines two techniques under the objective of visibility and understanding:

- *Analytic Monitoring: Monitor and detect adverse actions and conditions in a timely and actionable manner*. Analytic monitoring means understanding which assets are connecting to which services in near real-time. It relies on network instrumentation such as TAP or SPAN to collect live traffic and dissect protocols through deep packet inspection. Network traffic monitoring is beneficial for identifying compromised assets and exploited vulnerabilities, as well as detecting whether sensitive information is being exfiltrated or a connected service is misconfigured.
- *Dynamic Representation: Keep the representation of the network current*. Enhance understanding of dependencies through network access modeling. This means understanding which assets can connect to which services. This technique relies on configuration files from firewalls, routers, and switches to model the network topology and analyze connectivity paths. Network access modeling enables the proactive verification of network segmentation and understanding if critical vulnerabilities are exposed on the network. It's also vital to measure remote access risks and simulate possible network attack paths.

NIST CSF currently covers parts of those two techniques under:

- *DE.CM-1: The network is monitored to detect potential cybersecurity events* (Analytic Monitoring)
- *ID.AM-3: Organizational communication and data flows are mapped* (Dynamic Representation)

Feedback

We invite the drafting team to connect the two techniques defined above as fundamental building blocks to improve visibility and understanding. Those techniques, also called the two sides of network visibility, are crucial and complementary to each other. Through a direct understanding of network segmentation, network access modeling (*Dynamic Representation: which assets can connect to which services*) provides the contextual information needed to assess the risk of a suspicious connection (*Analytic Monitoring: which assets is connecting to which services*). We also invite the drafting team to take under consideration the technology

[redacted]

innovation of **dynamic network access modeling** that enables ID.AM-3 to become continuous as opposed to point-in-time.

Feedback on subsection 4.1: "Add a new Govern Function"

We welcome the addition of a new govern function in the NIST CSF. We believe that it will greatly contribute to elevating the importance of cybersecurity at the highest level of decision-making within organizations of all sizes.

Background

We would like to point out a couple key considerations for governance that could be useful to the NIST drafting team, especially in the context of industrial control systems:

- **First, information security policy drives a set of coherent security requirements throughout the organization.** In this context, a security policy should support safety, reliability, resilience, privacy, and other related concerns. Within this context, grid components are cyber-physical systems (CPS), composed into a more complex, networked cyber-physical system of systems. NIST CPS Public Working Group (PWG) Framework provides a set of relevant concerns. An organizational and informational security policy should address OT and IT environments and how they integrate, the complexity of external partnerships, and cover both traditional and modernized environments. Because the grid is a large cyber-physical system, governance and risk management processes should address all risks, not just cybersecurity.
- **Second, the governance teams today tend to be resource and technology limited.** As a result, they faced multiple challenges such as 1) having to promote and enforce a non-mandatory framework, and 2) relying on a large group of different stakeholders to collect data and assess situations.

Feedback

In light of those challenges, we invite the NIST drafting team to take the following items under consideration:

- Adding governance to all the core functions will require much thought on measurement, assessments, and the people (cybersecurity group, internal/external audit group, and regulatory audit groups) required to support these activities. We recommend the CSF to include this functionality at the control level and put together specific requirements and expected outcomes. In particular, clear ownership for each governance-supporting functions should be established.
- Today's networks are very complex, and many governance team members do not maintain specific vendor-specific technology skills as those managing the infrastructure functions of the networking/infrastructure teams. We recommend the CSF to emphasize the role of technology that embrace automation and ease-of-use to collect supporting data. The governance teams should be equipped with tools that are easy to deploy while requiring minimum training and time-consuming efforts.
- Governance cannot succeed without a strong culture of cybersecurity and the proper budget. We invite the drafting team to reference business practice guides that ensure

[redacted]

governance organizations have the budget, and accountability to manage to the agreed upon program, policies and procedures. Those guides should take into account the constraints of small, medium and large companies.

I want to thank the cybersecurity framework drafting team for providing Network Perception with this opportunity. As a business and as individuals, we highly value the ability to have a voice and impact the future of critical standards and regulations. I look forward to continuing our collaboration with you and contributing to developing effective cybersecurity practices.

Please let us know if you have any questions or need additional information. We look forward to maintaining our effective public-private partnership with NIST and other relevant stakeholders.

Sincerely,

Robin Berthier
CEO/Co-Founder
Network Perception