[redacted] [redacted]
Subject: NIST CSF 2.0 Draft Core - Comments from Forcepoint
Date: Wednesday, May 3, 2023 8:51:05 AM

To the NIST team,

Forcepoint is grateful for the opportunity to provide feedback on the NIST 2.0 Draft Core. Below are comments with special consideration for organizations that must operate and protect multiple independent security domains.

Table 2: Discussion Draft NIST Cybersecurity Framework 2.0 Core: Sample of Implementation Examples

Comment: Forcepoint supports the use of notional implementation examples that organizations can relate to their operational architecture. Each of the Examples outlined in the 2.0 core draft is applicable to any security domain, including classified security domains. A significant number of US government organizations operate multiple independent security domains with unique identities, security stacks, workloads, infrastructure, etc. To achieve the desired outcomes stated in CSF 2.0, organizations must understand how to implement Cybersecurity protections that can span multiple security domains. For example, routine patching is often implemented separately and inconsistently across each security domain which has previously resulted in negative Cybersecurity outcomes. Organizations can leverage existing Cross Domain technology to enable automation and standardization of Cybersecurity functions across many security domains. Cross Domain Solution (CDS) technology is widely used within US government agencies to support the movement of information, access to information, and to enable mission critical functions and thus should be an integral component in Cybersecurity implementation.

Table 3: Discussion Draft NIST Cybersecurity Framework 2.0 Core: Functions, Categories, and Subcategories

Comment: Forcepoint believes that the updates provided in 2.0 improve clarity and actionability. As noted previously in comments regarding Table 2, it is Forcepoint's position that the multiple security domain aspect of many US government organizations should be considered within the context of various Functions, Categories, and Subcategories. Below is a list of such areas where Cross Domain considerations are highly applicable.

Category	**Subcategory**	**Cross Domain Applicability**
Identity, Management, Authentication, and Access Control (PR.AA)	PR.AA-01: Identities and credentials for authorized users, processes, and devices are managed by the organization (formerly PR..AC-1)	Organizations operating across multiple security domains must contend with the unique challenge of managing multiple unique identities for each person. There is not currently a widely accepted solution for federating identities across

		multiple security domains. This results in a negative impact to Cybersecurity outcomes and therefore should be of special consideration for any government organization with a substantial user base that operates in multiple security domains.
Platform Security (PR.PS)	PR.PS-04: Log records are generated for cybersecurity events and made available for continuous monitoring.	Log records generated for cybersecurity events from all security domains should be consolidated to support continuous monitoring.
Adverse Event Analysis (DE.AE)	DE.AE-02: Adverse events are analyzed to find possible attacks and compromises.	Adverse events should be consolidated across all security domains.
	DE.AE-06: Information on adverse events is provided to cybersecurity and incident response tools and staff (formerly DE.DP-4)	Adverse events should be consolidated across all security domains.
Continuous Monitoring (DE.CM)	DE.CM-02: The physical environment is monitored to find adverse cybersecurity events	Definition of the physical environment to encompass all security domains is important.
	DE.CM-03: Personnel activity and technology usage are monitored to find adverse cybersecurity events (formerly DE.CM-3 and DE.CM-7)	Personnel activity often spans multiple security domains – attribution of activity is key to effective monitoring and should apply across all domains on which the user is active.

Very respectfully,

Chris Finch
Senior Principal Solutions Architect, CISSP, CCSP
Global Governments Critical Infrastructure

Forcepoint
[redacted]
www.forcepoint.com

[redacted]

[redacted]