June 12, 2023

COMMENTS ON NIST CYBERSECURITY FRAMEWORK 2.0 CORE DRAFT

SUBMITTED TO:
National Institute of Science and Technology

SUBMITTED BY:
Peraton Inc.
[redacted]
Scott Cooper, VP of Strategic Advocacy
[redacted]

Thank you for the continued work to update the Cybersecurity Framework 2.0. Peraton is excited to provide written feedback on the CSF 2.0 Core Draft after participating in the NIST's CSF 2.0 in-person workshop at the National Cybersecurity Center of Excellence (NCCoE) in Rockville, MD. Listed below are comments across key sections of the draft for your consideration. Please do not hesitate to contact us if further discussion is warranted, we are happy to continue partnering with NIST in this effort.

PERATON COMMENTS ON NIST CSF 2.0 CORE DRAFT

NIST CYBERSECURITY FRAMEWORK 2.0 CORE DRAFT SECTIONS	PERATON SUGGESTIONS	DISCUSSION
All six Core Functions	Incorporate an Operational Technology (OT) cybersecurity category or subcategory across each of the six Core Functions to ensure OT issues are reflected throughout the framework.	With the heightened concern around the United States' Critical Infrastructure cyber vulnerabilities, OT is noticeably absent from the CSF 2.0 Core Draft. While NIST solicited comments on the Draft Guide to OT Security, the two documents should not live separately. Rather, the CSF 2.0 Core Draft should incorporate key takeaways from the Guide to OT Security throughout each of the six Core Functions.
All six Core Functions	Incorporate the expanded use of Cloud Native cybersecurity capabilities across all six CSF Core Functions	The CSF 2.0 Core Draft makes no mention of Cloud Capabilities in the document. While the IDENTIFY function contains a "Platform Security" category, there is no connected "Infrastructure Security" that encapsulates Cloud Native capabilities.
Protect (PR)	Add a new category under the Protect function "Zero Trust Architecture (ZTA)."	Zero Trust is becoming the standard across government and industry. Following CISA's "Secure by design, secure by default" concept paper, it is important to reiterate the need for ZTA throughout government and industry based on NIST Special Publication 800-207, or other NIST research.
Protect (PR)	Add a new category under the Protect function "Cyber Threat Intelligence (CTI)."	Users should have plans in place for what to do with the immense amounts of cyber threat data collected through enhanced cybersecurity and threat monitoring. The CSF 2.0 Core Draft should provide simple outline and examples of the intelligence cycle as it pertains to CTI.