From: Robin Regnier
Sent: Friday, January 19, 2018 6:41 PM
To: cyberframework <cyberframework@nist.gov>
Subject: Comments on Draft 2 of Version 1.1 of the Cybersecurity Framework

To Whom It May Concern,

Thank you for the opportunity to submit comments on Draft 2 of Version 1.1 of the Cybersecurity Framework.

The Center for Internet Security (CIS) is a not-profit organization that works with the global IT community to safeguard private and public organizations against cyber threats.

CIS is home to the CIS Critical Security Controls, the CIS Benchmarks, and the Multi-State Information Sharing and Analysis Center (MS-ISAC), the go-to resource for cyber threat prevention, protection, response, and recovery in state to tribal governments.

CIS appreciates being called out as an informative reference in the Framework, and appreciates the opportunity we have had to work with NIST to ensure a correct and consistent mapping between the Framework and the CIS Controls. We are fully committed to the adoption and evolution of the Framework and to creating a body of knowledge and complementary working aids that allow our constituency to successfully implement the Framework.

Comments

For the information on Informative References, we suggest that a note be included that sends them directly to the original source/reference for a current and authoritative mapping before use, since any of these references could be updated on a timeline independent of the Framework document. For example, we anticipate releasing an update top Version 7 of the CIS Controls in early spring 2018.

We appreciate specific inclusion of Cyber-Attack Lifecycle as an essential topic in the Roadmap, and have already contributed the CIS Community Attack Model to the cyberdefense literature. We believe that any such activity should clearly address both “tactical” and “strategic” understanding to be gained from such an approach. Most thinking (and products and services) about attacker lifecycle focuses on the use of specific indicators, and specific responses to attack stages and vectors. Equally important is the need to use such an approach to define the most effective control strategies, and to ensure that the basic infrastructure needed to take best advantage of indicators, etc. is identified and in place. We find it common that many enterprises cannot begin to take advantage of deep threat intelligence, as they do not have the basic machinery in place to execute on that information.

Comments on behalf of the MS-ISAC:

The mission of the MS-ISAC is to improve the overall cybersecurity posture of state, local, tribal and territorial governments through focused cyber threat prevention, protection, response, and recovery.

Aligned with its mission, the MS-ISAC administers the Nationwide Cyber Security Review (NCSR), which is a free, confidential, annual self-assessment survey that is based on the Framework and is sponsored by the Department of Homeland Security (DHS) and the MS-ISAC.

The NCSR evaluates cybersecurity maturity across the nation while providing actionable feedback and metrics directly to individual respondents in State, Local, Tribal & Territorial (SLTT) governments.

Using the results of the NCSR, DHS delivers a biyearly anonymous summary report to Congress providing a broad picture of the cybersecurity maturity across the SLTT communities. To access the summary report, please visit: https://www.cisecurity.org/white-papers/2016-nationwide-cyber-security-review-summary-report/.

In response to the NIST Cybersecurity Framework Draft 2 Version 1.1, the Metrics workgroup, which is comprised of MS-ISAC members who volunteer their time and talent to assist with specific program areas and deliverables in support of the MS-ISAC's goals and objectives believe there would be value in adding the proposed core updates at the category and subcategory levels.

In closing, CIS strongly believes in the need for the "Community-First" approach to cyber security. The vast majority of attacks and threats facing enterprise are universal, which implies a strong need for a social expectation of basic security practices (a principle embodied in the CIS Controls). This establishes a basic social expectation of good security behavior, which simplifies partner and supply chain discussions, and also does not require that every enterprise in the ecosystem do "the right job" in assessing their own risk. Note that this is about establishing a baseline or foundation of good security practices, not a one-size-fits-all solution.

We continue to appreciate the chance to work with NIST on the evolution of the Framework and to keep all mappings to the CIS Controls current and relevant.

Best regards,

Robin Regnier, GCCC
Controls Coordinator
Critical Security Controls