From: **Kathryn Burns**
Date: Mon, Apr 10, 2017 at 5:07 PM
Subject: Comments on the update to the Cybersecurity Framework
To: "cyberframework@nist.gov" <cyberframework@nist.gov>

To Whom It May Concern,

Thank you for the opportunity to submit comments on draft 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 NIST Framework. According to surveys by Tenable Network Security, Inc. users of the NIST framework are often using more than one framework to guide their security programs and a majority of CIS Critical Security Controls adopters also use the NIST Framework. As such, 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 on behalf of CIS Controls:

Please change all references to the Council on Cyber Security to the Center for Internet Security (pages 27-45, 50, and 56).

The CIS Critical Security Controls endorse the specific definitions of “measurement” and “metrics” used in this version of the Framework. CIS has previously adopted the same definitions, from the same source, in the “Measurement Companion to the CIS Controls”.

We think more care is required in the use of terms like “accurately monitor cybersecurity risk” (line 402). While you might be able to accurately and reliably monitor and measure Key Risk Indicators, or “measurements” (as now defined in the CSF), this does not necessarily mean you are accurately monitoring/measuring actual risks. The step from “measurement” to “metrics” inherently involves the subjective value judgement of “good enough”. Secondly, we also feel that it is important to specifically address the use of measurements and metrics from both an absolute and relative perspective.

We appreciate specific inclusion of Supply Chain Risk Management as a topic. While it is a key risk management process, is not necessarily a unique process onto itself and it could be incorporated into the other Tier components instead of a stand-alone topic. For example, we have experience working with very large companies who have integrated use of the CIS Controls as a key component of Supply Chain Risk Management. For them the CIS Controls provide a relatively speedy, cost-effective and reliable operational framework to assess the risk of supply chain partners. While Version 1.1 of the Framework suggests that a Target Profile be used to drive this discussion, we believe that starting from the CIS Controls provides a more flexible way to manage this problem, as suppliers typically want to be supporting many upstream companies, each with potentially a different Target Profile.

We find the discussion on how to connect security practices to business outcomes somewhat confusing, and perhaps not practical. A more effective approach might be to tie security practices to either specific business principles desired by the enterprise (e.g., consumer confidence, reliability of performance) or key attributes of the business/mission which influence the cyber security threat model, and so the priority of controls (e.g., safety first, avoiding loss of life).

<u>Comments on behalf of the MS-ISAC:</u>

The MS-ISAC administers the Nationwide Cybersecurity Review (NCSR). The mission of the NCSR is to provide meaningful security metrics to our State, Local, Territory, and Tribal Community in support of the missions of the Department of Homeland Security and the Multi-State Information Sharing and Analysis Center.

In short, the NCSR is a free annual voluntary self-assessment survey that is aligned to the NIST Cybersecurity Framework and is designed to evaluate cybersecurity management. This marks our third year using the NIST CSF as the question set for the annual self-assessment. Using the NCSR results, DHS and MS-ISAC continue to work with our partners in State, Local, Tribal and Territorial Governments to identify actionable steps for improving the security of the nation’s critical cyber infrastructure.

In response to the NIST Cybersecurity Framework Draft 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 and or incorporating information <u>sharing</u> and <u>collaboration</u> to the framework.

The mission of the MS-ISAC is to improve the overall cybersecurity posture of state, local, tribal and territorial governments. Collaboration and information sharing among members, private sector partners and the U.S. Department of Homeland Security are the keys to success. The MS-ISAC is designated and funded by DHS as the key cybersecurity resource for State, Local, Tribal, and Territorial governments in the Unites States. The MS-ISAC offers free membership to all public entities which includes free monitoring of your IP ranges and domains, access to the HSIN Secure Portal, a no cost incident response team for any attack that you may be the victim of, free educational materials for your own use in educating staff and the public, weekly reports of the top malicious IP addresses and malware sites, monthly webcasts on a variety of topics, as well as regular advisories regarding internet security incidents in other parts of the country. We currently have over 1,100 State, Local, Tribal, and Territorial governments as well as other types of public entities among our membership.

We welcome the opportunity to further discuss the mission of the NCSR and the MS-ISAC and encourage you to share this information with the SLTT community. The Metrics workgroup is also looking for ways to become more involved with NIST and the Framework, and are open to any ideas you may have.

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 our work with NIST on the evolution of the Framework and our efforts to keep all mappings to the CIS Controls current and relevant.

Thanks again and please let us know if you have any questions.

Kathryn Burns
Sr. Director
CIS Controls Program

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.