March 2nd, 2023

National Institute of Standards and Technology
Applied Cybersecurity Division
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Sent via email to *cyberframework@nist.gov*.

M3AAWG Comments on NIST Cybersecurity Framework 2.0 Concept Paper

Introduction

The Messaging Malware Mobile Anti-Abuse Working Group (M[3]AAWG) submits these comments in response to the National Institute on Standards and Technology (NIST) Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework (CSF Concept Paper), released on January 19, 2023.

The NIST Cybersecurity Framework ("CSF" or "Framework"), released in 2014 and updated in 2018, provides critical infrastructure-focused guidance to organizations to better understand, manage, reduce, and communicate cybersecurity risks and build controls to mitigate these risks. The CSF Concept Paper outlines and seeks input on potential significant changes currently under consideration by NIST as it develops the 2.0 version of the CSF.

M[3]AAWG is a technology-neutral global industry association. As a working body, we focus on operational issues of internet abuse including technology, industry collaboration, and public policy. With more than 200 members worldwide, we bring together stakeholders in the online community in a confidential, open forum, developing best practices and cooperative approaches for fighting online abuse. Email, one of the key areas addressed by M[3]AAWG, is one of the most common initial attack vectors used by attackers.

As discussed below, M[3]AAWG generally supports the proposals outlined in the CSF Concept Paper. However, M[3]AAWG urges NIST to consider the impact of proposals that could potentially dilute the usefulness of a framework originally developed to focus on critical infrastructure cybersecurity risks and needs.

1.1. Change the CSF's title and text to reflect its intended use by all organizations

In Section 1.1, NIST proposes to change the name of CSF 2.0 from "Framework for Improving Critical Infrastructure Cybersecurity" to "Cybersecurity Framework," and to broaden the scope of CSF 2.0 to

> cover all organizations across government, industry, and academia, including but not limited to critical infrastructure. References to critical infrastructure in the CSF may be maintained as examples, but Framework text will be reviewed for broad applicability. Categories and

> Subcategories of the CSF Core that are specific to critical infrastructure, such as ID.BE-2 and ID.RM-3, will be broadened.

NIST further claims:

> This change is not intended to diminish the CSF's relevance to critical infrastructure organizations, including the importance of ensuring the security and resilience of our nation's critical infrastructure, but to embrace and enhance its broader use.

While M[3]AAWG is not concerned with a name change that reflects the evolving and expanding cybersecurity risk environment, we urge caution. We ask NIST to consider that this broadening of scope could have the opposite effect; it could weaken the very cybersecurity risk management programs for critical infrastructure that are the CSF's greatest strength. While there are various general frameworks, standards, and guidelines (e.g., NIST's own Special Publications, CIS controls, and the ISO 27000 family) available to assist organizations to address security risks, the NIST CSF's particular focus on critical infrastructure risks, needs, and concerns was unique. By trying to be everything to everyone, CSF 2.0 could become yet another general security framework that caters to a wide audience, rather than a tightly focused set of resources and guidance targeted and tailored to the specific cybersecurity risks to critical infrastructure, and to the particular environment in which critical infrastructure providers operate.

It is not clear why this extension is necessary at this point, when other general resources already exist and can be leveraged by organizations in any sector.

M[3]AAWG suggests that rather than simply renaming CSF 2.0, NIST could instead preserve CSF 1.1's focus on critical infrastructure by consolidating the relevant sections of the CSF applicable to critical infrastructure cybersecurity risks and maintaining them as a separate framework along the lines of the other NIST frameworks referenced in Section 2.2 of the CSF Concept Paper.

1.2. Scope the CSF to ensure it benefits organizations regardless of sector, type, or size

In Section 1.2, NIST notes:

> Since publication of CSF 1.1, Congress has explicitly directed NIST to consider small business concerns and the cybersecurity needs of institutions of higher education.

M[3]AAWG recognizes the importance and usefulness of improving support for the security of small businesses and the education sector, and the value of becoming more flexible in supporting different kinds of organizations that provide critical infrastructure. However, critical infrastructure, as defined by the Cybersecurity and Infrastructure Security Agency (CISA), traditionally includes services and facilities "so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." (See https://www.cisa.gov/critical-infrastructure-sectors.) Not all educational institutions and small businesses can or should be considered critical infrastructure.

Indeed, it might be useful to extend the 16 sectors that CISA considers critical infrastructure at this point. However, this extension should be based on a clear methodological approach that specifies what is and is not critical infrastructure. For example, while some educational institutions and small businesses are critical, at least in part, others are not. Clear methodology and definitions would help potentially affected organizations. With a clear framework, they could better determine if – and, if so, to what extent – they fall under critical infrastructure considerations and requirements.

To the extent that CSF 2.0 is expanded to incorporate these additional sectors, M³AAWG recommends that NIST evaluate, identify, and distinguish critical and non-critical aspects of the various sectors' infrastructure as it develops applicable guidance and works to align it with the broader CSF 2.0. Further, NIST should consider providing guidance to assess the risks associated with devices and addressing the significant security risks that unsecured devices pose to networks and other connected devices when introduced into a critical infrastructure environment.

NIST's desire to be "helpful to organizations – regardless of sector, type, or size […] in addressing cybersecurity challenges" is noble in theory but may be difficult to implement in practice. For example, small entities often lack the dedicated cybersecurity staff needed to implement cybersecurity risk management programs. Accommodating new sectors should not distract from fully supporting existing critical infrastructure sectors. NIST should consider the impacts that overextending the CSF 2.0 would have on the 16 critical infrastructure sectors' cybersecurity risk assessment and management programs.

1.3. Increase international collaboration and engagement

M³AAWG commends NIST's plans to facilitate increased international collaboration and engagement as outlined in Section 1.3. M³AAWG offers its support in the areas in which it is active internationally, especially with regard to issues related to messaging, mobile, and malware. While cooperation is useful, M³AAWG suggests that NIST also consider how and with whom to collaborate. Such engagement could delay CSF 2.0 updates and potentially allow foreign adversarial parties, including nation-state actors, to unduly influence the process.

Critical infrastructure presents a high-value cybersecurity attack target for foreign adversaries, including nation-state actors. M³AAWG recommends that NIST consider the threats and the challenges these pose even to the most-resourced organizations, and provide guidance on how these threats can be tackled by critical infrastructure cybersecurity risk management programs.

2.2. Relate the CSF clearly to other NIST frameworks

Linking the CSF to other key cybersecurity and privacy-related documents and frameworks is useful. However, NIST should consider that too many references can dilute the effectiveness of the Framework. Also, if the emphasis is meant to be on securing critical infrastructure, it is not immediately clear that mapping the CSF to other standards will necessary help impacted entities. Furthermore, the focus of these references should be specific to critical infrastructure concerns.

2.3. Leverage Cybersecurity and Privacy Reference Tool for online CSF 2.0 Core

M³AAWG agrees that the NIST Cybersecurity and Privacy Reference Tool is useful and should be leveraged as well as developed further.

2.6. Remain technology- and vendor-neutral, but reflect changes in cybersecurity practices

M³AAWG welcomes a technology and vendor-neutral approach in the CSF 2.0 that also reflects the changing cybersecurity landscape. M³AAWG supports such an approach in its own work.

3. CSF 2.0 (and companion resources) will include updated and expanded guidance on Framework implementation

M³AAWG concurs with the NIST proposal for expanded guidance but suggests that such guidance remain focused on (and usable in the context of) critical infrastructure. Guidance should stay closely scoped so as not to overwhelm critical infrastructure providers. It is important for organizations to be able to find NIST's excellent resources quickly and easily when they need them.

M³AAWG would be happy to leverage its community and its existing documentation to provide resources for implementing DNS, email and messaging security, and to improve abuse handling, malware, and DDoS mitigation.

3.2. Develop a CSF Profile template

M³AAWG supports NIST's creation of CSF profiles addressing email providers, messaging more generally, DNS, and IoT. M³AAWG also offers its expertise in DDoS mitigation, addressing malware, and online abuse handling, should these become relevant.

3.3. Improve the CSF website to highlight implementation resources

M³AAWG is happy to support the creation and mapping of relevant resources for the updated CSF website. Communication infrastructure is important in everyday life but crucial during emergency situations; email is a critical part of that infrastructure. M³AAWG has published relevant documents that provide guidance for securing email infrastructure, including, among others, documents regarding the security technologies SPF, DKIM, and DMARC. In light of email's significance as an attack vector, securing this infrastructure is paramount. M³AAWG's work also addresses DNS abuse, the illegitimate use of computing resources such as web hosting, and other areas of online abuse that enable attacks. M³AAWG also works on improving abuse response processes.

M³AAWG documents are available publicly on our website (see https://www.m3aawg.org/published-documents). Many have been translated into other languages.

Recognizing the importance of proper implementation, M³AAWG offers its support in this area and is ready to liaise with NIST regarding any forms of support that NIST deems beneficial.

4. CSF 2.0 will emphasize the importance of cybersecurity governance

M³AAWG supports the inclusion of governance in CSF 2.0 as outlined by NIST in Section 4. Functional governance includes critical executive sponsorship, assures funding, and can establish organizational baselines and provide necessary accountabilities and responsibilities. A proper risk view of threats, threat actors, and vulnerabilities is also fundamental, especially if NIST aims to provide tools and guidance for specific concerns and pertinent risks in the critical infrastructure space.

However, NIST should be careful not to overemphasize issues of compliance and documentation over actual, usable, real-world security. GRC is relevant and important, but it should support security. While governance is relevant, it is important to consider the extent to which this and other extensions or additions to CSF 2.0 may consume time and effort that could be spent more effectively on operational security concerns in critical infrastructures – namely, hands-on technical work and the governance and management tasks that enable such work.

5. CSF 2.0 will emphasize the importance of cybersecurity supply chain risk management (C-SCRM)

M³AAWG applauds NIST's proposal to include additional guidance to address supply chain and third-party risks in CSF 2.0 "given the increasing globalization, outsourcing, and expansion of the use of technology services (such as cloud computing)." M³AAWG suggests that NIST consider collaboration with and leveraging the work of, for example: the National Counterintelligence and Security Center (NCSC) Supply Chain and Cyber Directorate, see https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-supply-chain-threats; the IETF Supply Chain Integrity, Transparency and Trust Working Group, see https://datatracker.ietf.org/wg/scitt/about/; and the Open Source Security Foundation's Secure Supply Chain Consumption Framework, see https://openssf.org/blog/2022/11/16/openssf-expands-supply-chain-integrity-efforts-with-s2c2f.

6. CSF 2.0 will advance understanding of cybersecurity measurement and assessment

M³AAWG concurs that "[m]easurement and assessment of cybersecurity risk management programs and strategies continues to be an important area in the use of the CSF." Measurement and assessment are fundamental to understanding and mitigating security risks, both at the organizational as well as the national and international levels. To that end, M³AAWG recommends that more attention be paid to instrumentation and monitoring of associated systems and networks in CSF 2.0. For example, control systems are often assumed to be air-gapped from the global internet and completely unmonitored for anomalous traffic, leading to predictably poor results.

Conclusion

M³AAWG supports NIST's efforts to develop a flexible and effective cybersecurity framework that serves as a foundational tool and resource for addressing and managing cybersecurity risks within organizations, across sectors, globally, and in a technology-neutral manner. We applaud NIST's collaborative approach that encourages participation by government, industry, and other interested stakeholders in the development process. Thank you for the opportunity to submit these comments. We welcome the opportunity to engage with NIST to answer any questions during this process.

Please address any inquiries about our comments or work to M3AAWG's Executive Director, Amy Cadagin, at comments@m3aawg.org

Sincerely,

Amy Cadagin
Executive Director, Messaging Malware Mobile Anti-Abuse Working Group
amy@m3aawg.org

P.O. Box 9125
Brea, CA 92822