Center for Internet Security

CIS Response to NIST RFI for the Cybersecurity Framework

Introduction

The Center for Internet Security (CIS) hereby submits this response to the National Institute of Standards and Technology (NIST) Request for Information (RFI) pursuant to the notice published in the Federal Register on December 11, 2015. The RFI seeks comments on the variety of ways that its "Framework for Improving Critical Infrastructure Cybersecurity" (the Framework) is being used to improve cybersecurity risk management and possible ways to improve it.

CIS is a not-for-profit organization dedicated to enhancing the cybersecurity readiness and response among public and private sector entities. The mission of CIS is to identify, develop, validate, promote, and sustain best practices in cybersecurity; deliver world-class security solutions to prevent and rapidly respond to cyber incidents; and build and lead communities to enable an environment of trust in cyberspace. Utilizing its strong industry and government partnerships, CIS is home to the Multi-State Information Sharing and Analysis Center (MS-ISAC), the CIS Security Benchmarks, and the CIS Critical Security Controls.

CIS serves a broad-based national and international constituency across the public and private sectors. Th MS-ISAC is a voluntary and collaborative effort based on a strong partnership with the Office of Cybersecurity and Communications within the U.S. Department of Homeland Security (DHS). The MS-ISAC has been designated by DHS as the key resource for cyber threat prevention, protection, response and recovery for the nation's state, local, tribal and territorial (SLTT) governments and currently includes over 900 members, including all 50 states, over 300 cities, and nearly 300 counties. Through the Nationwide Cyber Security Review (NCSR), the MS-ISAC charts nationwide progress in cybersecurity and identifies emerging areas of concern across hundreds of SLTT governments. The National Campaign for Cyber Hygiene is a collaborative effort by CIS and the National Governors Association, which serves as a foundational cybersecurity program across hundreds of SLTT governments. The CIS Security Benchmarks organizes communities of technical expert volunteers to develop secure configurations serving over 700 private and public sector organizations across the globe, and supported by essentially the entire security industry. The Center for Internet Security Critical Security Controls for Effective Cyber Defense Version 6.0™ draws upon the expertise of hundreds of worldwide cybersecurity practitioners and subject matter experts. The current version of the CIS Controls, which are aligned to NIST guidance, have been downloaded over 19,000 times since October 2015 and are used by thousands of organizations around the world as a means to operationalize accepted cybersecurity best practice.

These activities create countless CIS relationships, formal and informal, across the entire security industry, major IT companies, and many others (e.g., critical infrastructure sectors, insurance, auditing, security training). In addition, CIS

personnel are active in both thought leadership and action across the industry, with dozens of major speaking events, interviews, and other media events just in the last year; and leadership or participation in numerous international and national standards activities and working groups.

How CIS Uses & Supports the NIST Cybersecurity Framework

As a long-standing supporter of NIST, CIS participated in the development of the Framework by attending the workshops and participating in the public comment process. The Framework calls out the CIS Controls as one of the "Informative References" - a way to help users implement the Framework using an existing, supported methodology. Since its publication, CIS has made the Framework an important element of its programs, mission evolution, and messaging. This close alignment is evident in the following ways:

> The most recent version of the CIS Controls (Version 6.0) includes a new appendix showing how to map from the CIS Controls to/from the Framework, making it easy for enterprises to use the Framework, but define their specific actions and priorities in terms of the CIS Controls (and take advantage of the large CIS Controls community of vendors, adopters, and training).
>
> CIS also recently published the CIS Community Attack Model - an open community framework for gathering and analyzing summaries of attacks seen across the industry. Within the Model, we use the Framework as the basic categorization scheme for defensive controls, providing a natural wa to keep the CIS Controls current based on the latest attack information and also provide a foundational community-level "threat model" to underpin defensive action within the Framework.
>
> Promoting cyber hygiene through policy recommendations, the National Campaign for Cyber Hygiene is also designed to align with the first five of the CIS Controls and the DHS Continuous Diagnostic and Mitigation (CDM) Program thereby promoting the adoption and implementation of the Framework. The CIS Controls are demonstrably a subset of the comprehensive catalog defined by NIST SP 800-53 and are referenced within the Framework.
>
> The CIS Cyber Risk Assessment and Fundamental Training (CRAFT) program utilizes both the Framework and the CIS Controls and consists of prioritized questions to help managers develop a cyber security plan of action, better focus on security priorities, and improve their cybersecurity posture.

The CIS Security Benchmarks are contained in the NIST National Checklist Program Repository as official configuration guidance for use by federal agencies and other entities subject to Federal Information Security Management Act (FISMA) compliance requirements. Additionally, the CIS Configuration Assessment Tool (CIS-CAT) is a validated product for the NIST Security Content Automation Protocol (SCAP) in the categories of FDCC Scanner and Authenticated Configuration Scanner.

The Framework recommends that organizations consider leveraging external guidance obtained from Information Sharing and Analysis Centers such as the MS-ISAC. In an effort to promote proper cybersecurity, the MS-ISAC's Business Continuity, Recovery and Cyber Exercise Workgroup monthly "15 Minute Table Top Exercises" now cross-references components of the Framework.

The Nationwide Cyber Security Review (NCSR) is a voluntary self-assessment survey designed to evaluate cybersecurity management conducted by MS-ISAC in partnership with the U.S. Department of Homeland Security (DHS), the National Association of State Chief Information Officers (NASCIO) and the National Association of Counties (NACo). The NCSR is now based on the Framework and is a tool for organizations to assess their progress against other organizations. The NCSR results are provided to Congress to highligh cybersecurity gaps and capabilities among our SLTT governments.

CIS leadership has been vocal in their support of the Framework in numerous speeches, panels, and other speaking engagements. We also agreed to co-sponsor (with G2, Inc.) the non-profit Cforum (www.cforum.org), addressing the need for a neutral open and public discussion forum on the Framework.

CIS directly supports the DHS Critical Infrastructure Cyber Community C^3 (pronounced "C Cubed") Voluntary Program, which assists owners and operators of critical infrastructure, academia, Federal government, SLTT governments, and business in their use of the Framework. The MS-ISAC serves as a conduit for the C^3 Voluntary Program to engage with SLTT to develop guidance on how to implement the Framework. Additionally, CIS leadership has presented at several C^3 conferences in support of the Framework.

Recommendations for Improvement

Prioritized Action

A common request of CIS community users is to establish prioritized actions to address the most common and pervasive threats. The CIS Controls assist in this

regard by establishing specific recommended actions in a prioritized order. We are also developing a Community Attack Profile Model that will provide guidance on what threats and attacks patterns are most relevant to particular industries and prioritize selection of controls. The NCSR provides MS-ISAC partners with a means to prioritize the Framework by defining a universal target maturity level and by allowing users to compare how their peers have performed in the different categories of the framework. The Framework could provide additional guidance on prioritizing a plan of action.

Support for a "Community-First" Approach

We believe that the most effective approach to use the Framework is to take a community-first approach. That is, natural groupings like sectors of the economy should band together to develop a common approach to prioritize action under the Framework. Identifying commonalities of threat, risk, and action could provide major improvement in understanding and negotiating cybersecurity among business partners and similarly positioned enterprises. Thi is the approach that CIS has taken as a default, and we think that the Framework should address this approach explicitly.

Privacy Concerns

Any framework recommending implementation of cybersecurity controls invariably has privacy implications. CIS expounded upon the nexus of cybersecurity and privacy by publishing a Privacy Companion to the CIS Controls. Since privacy is an area of much interest for the SLTT community, the MS-ISAC added a separate area to examine privacy, based on NIST 800-53 Revision 4. The Framework could provide additional guidance on addressing privacy issues.

Operationalize the Framework

Additionally, CIS received comments requesting guidance on how to operationalize the Framework. Many use the CIS Controls as a roadmap and guide to implement the Framework. The Framework could provide additional guidance on operationalization.

The Framework Tiers

The use of Tiers in the Framework should be considered for revision. As part of the NCSR, the MS-ISAC created a maturity scale that would allow for the measuring of organization's maturity for each of the sub-categories of the Framework Core. The MS-ISAC risk maturity scale is based on how the Framework Core sub-categories are formalized and managed. The tiered approach, while useful for tracking the organization-wide cyber risk management, was difficult to directly integrate into NCSR and was omitted from the NCSR self-assessment.

Conclusion

CIS remains strongly committed to support the Framework among its constituent communities and promote its broader adoption and implementation. There is a strong a need for a cybersecurity framework to serve as a common and shared reference to inform the discussion regarding the necessary actions to secure cyberspace. No undertaking to tackle such a grand challenge as improving security in the cyber domain is without difficulty but that does not make it an unworthy endeavor. MS-ISAC, CIS Security Benchmarks, and CIS Controls provide complementary tools to help implement the Framework, and CIS will continue to work towards further adoption and implementation of the Framework. To that end, CIS looks forward to participating in the NIST workshop on the Framework in April 2016. CIS is dedicated to improving cybersecurity readiness and response among the public and private sector and will continue to work with the Framework to help make cybersecurity best practice, common practice.

For further information please contact:
Frank Guido
Center for Internet Security
703-600-1935
frank.guido@cisecurity.org