Written Comments

Submitted by the

Center for Internet Security

November 6, 2023

Regarding the

NIST Cybersecurity Framework (CSF) 2.0

November 6, 2023

Comments on the Discussion Draft of the

NIST Cyber Security Framework Core 2.0

Thank you for the opportunity to comment on the discussion draft. Some of us at the Center for Internet Security (CIS)[1] have been involved with the NIST Cyber Security Framework since the public announcement, the workshops to define it, and its use since Version 1.0.

As one of the original Information References in the NIST CSF 1.0, we have extensive experience in supporting adopters of the Center for Internet Security Critical Security Controls[2], many of whom also choose to use the NIST CSF. We believe this has worked out roughly as you intended from Version 1 – the NIST CSF providing a comprehensive, enterprise-level "language" to describe and manage a cyber risk program; and the Informative References providing a more technology and implementation focus as the basis for technical planning and implementation. The CIS Controls are the set of internationally-recognized, prescribed, prioritized operational security practices based on the current state of the global cyber threat that form the foundation of essential cyber hygiene. From our perspective the CIS Controls become the roadmap to implement the goals of the CSF. This has allowed us to bring a more prescriptive action-oriented complement and focus to the CSF, while also improving the CIS Controls to better align with and support the broader enterprise goals of the CSF.

Also, through our work in the Multi-State Information Sharing and Analysis Center (MS-ISAC)[3] (supporting all 56 states and territories and over 16,000 local and tribal government organizations), we are seeing and supporting a new trend: States that have crafted legislative language specifically listing both the NIST CSF and the CIS Controls. Some detailed examples are included below at Appendix 1. We think this helps bring an economic focus to a cyber risk program by bringing it closer to top-level business risk decisions.

We support the addition of Governance as a 6th function. In our experience, this is a necessary concern for users, and the addition will provide some clarity, structure, and comparability across implementations. In fact, to support our SLTT community, The Center for Internet Security (CIS), the Center for Technology in Government at the University at Albany, State University of New York (CTG UAlbany), the National Governors Association (NGA), and the National Conference of State Legislatures (NCSL) collaborated to study and document the effectiveness of different governance models for state governors and legislatures.[4]

We strongly support the move of Informative References to an on-line repository, rather than keeping references embedded in the core document. This will allow better and more current

[1] For more information about the Center for Internet Security (CIS), see: https://www.cisecurity.org/

[2] For more information about the CIS Critical Security Controls, see: https://www.cisecurity.org/controls

[3] For more information about the MS-ISAC, see: https://www.cisecurity.org/ms-isac

[4] https://www.cisecurity.org/insights/white-papers/managing-cyber-threats-through-effective-governance

mapping between versions of the CSF and the Informative References. We also suggest some published criteria by which implementation guidance may be included in the on-line references. For example, it would seem appropriate to require a commitment to clear and published configuration management for any references, provision of a single link to details of the guidance, up-front identification of specific costs or paywalls to access the guidance, and a commitment to support NIST work in machine-readable formats.

For example, we have always maintained authoritative, on-line and freely-available cross-mappings to the NIST CSF (and numerous other frameworks) to the current versions of the CIS Critical Security Controls, consistent with our intention of simplifying security planning and implementation for our adopters.

In addition to the items mentioned above that support the use of the CIS Controls in combination with them NIST CSF, we have developed an ecosystem of complementary products and services that support the CSF focus on data-driven, risk-based security improvement making, effectiveness for all size and type of enterprises, and adoption that is consistent with international counterparts.

- The CIS Community Defense Model (CDM) use standard data sources (e.g., the Verizon Data Breach Investigations Report[5]) and the industry-accepted MITRE ATT&CK Framework[6] to establish specific security value for each of our recommendations.

- We developed CIS Controls Implementation Groups[7] to provide both an on-ramp for organizations just starting out as well as a roadmap to greater cyber defense maturity by offering three tiers, which tailor the Controls to the size and maturity of the implementing organization

- We support cost-effectiveness of security programs by helping enterprises focus on the most important baseline things to do to defend against the most common attack types, while also providing a clear path for greater security and maturity. CIS has also developed tools, models, and working aids to help enterprises measure and manage the cost of their cybersecurity program. All CIS primary content and almost all of the CIS materials are available at no cost, and there is also a robust commercial marketplace of tools to help enterprises with implementation and management.

- CIS products are known and adopted all around the world, providing opportunities for common baselines and framework harmonization. Significantly, over 400,000 organizations around the world (over half from outside the United States), including national and state governments and private sector organizations, have downloaded the CIS Critical Security Controls. For a select listing of those global organizations that have

[5] https://www.verizon.com/business/resources/reports/dbir/

[6] https://www.cisecurity.org/insights/white-papers/cis-community-defense-model-2-0

[7] https://www.cisecurity.org/controls/implementation-groups

endorsed the CIS Controls, see Appendix 2. We are also the world's largest source for independent, security configuration guidance (the CIS Benchmarks and Hardened Images in the Cloud).

In summary, the CIS Critical Security Controls have served as an effective, measurable, scalable, and cost-effective method of implementing the goals of the NIST CSF that are supported by CIS's mapping to other cybersecurity frameworks and their global adoption.

We look forward to working with the NIST team to continue our long-standing support for the Cyber Security Framework.

Appendix 1: State Statutes That Specifically Refer to NIST CSF and the CIS Critical Security Controls

State of Nevada: An existing statute requires state data collectors to implement and maintain "reasonable security measures" to protect such records. A new Nevada statute, which became effective on January 1, 2021, requires that the state data collectors comply with the CIS Critical Security Controls or the NIST Cybersecurity Framework, thus defining what constitutes reasonable security for the state as a collector of personally identifiable information. https://www.leg.state.nv.us/App/NELIS/REL/80th2019/Bill/6534/Overview

Safe Harbor Statutes:
The following four states have enacted statutes that incentivize the voluntary adoption of cyber best practices by creating a safe harbor for organizations that adopt one of several industry standards, like the CIS Critical Security Controls. In three of these cases, the incentive is an affirmative defense, in one it is a cap on punitive damages.

Here is the Ohio statute language that they all use almost verbatim:

> A covered entity's cybersecurity program, as described in section 1354.02 of the Revised Code, reasonably conforms to an industry recognized cybersecurity framework for purposes of that section if division (A), (B), or (C) of this section is satisfied.
> (A)(1) The cybersecurity program reasonably conforms to the current version of any of the following or any combination of the following, subject to divisions (A)(2) and (D) of this section:
>
> > (a) The "framework for improving critical infrastructure cybersecurity" developed by the "national institute of standards and technology" (NIST);
> > (b) "NIST special publication 800-171";
> > (c) "NIST special publications 800-53 and 800-53a";
> > (d) The "federal risk and authorization management program (FedRAMP) security assessment framework";
> > (e) The "center for internet security critical security controls for effective cyber defense";
> > (f) The "international organization for standardization/international electrotechnical commission 27000 family - information security management systems."

These four states include:

State of Iowa: Affirmative Defenses for Entities Using Cybersecurity Programs
Overview: Incentivizes voluntary adoption of cybersecurity best practices, including the CIS Critical Security Controls, by creating affirmative defenses in a lawsuit resulting from a data breach.

Status: Effective date: July 1, 2023.
Link: https://www.legis.iowa.gov/docs/publications/LGE/90/HF553.pdf

State of Connecticut: An Act Incentivizing the Adoption of Cybersecurity Standards for Businesses

Overview: Incentivizes voluntary adoption of cybersecurity best practices, including the CIS Critical Security Controls, by creating a cap against punitive damages in a lawsuit resulting from a data breach.
Status: Effective date: October 1, 2021.
Link: Text of Public Act No. 21-118 (CIS Controls at page 4): Substitute House Bill No. 6607 - Public Act No. 21-119

State of Utah: The Cybersecurity Affirmative Defense Act

Overview: Incentivizes voluntary adoption of cybersecurity best practices, including the CIS Critical Controls, by creating an affirmative defense against lawsuits resulting from a data breach.
Status: Effective date: May 5, 2021.
Link: Text of enrolled bill (CIS Controls at page 5): Enrolled Copy HB 80 1 DATA SECURITY AMENDMENTS

State of Ohio: The Data Protection Act

Overview: Incentivizes voluntary adoption of cybersecurity best practices, including the CIS Critical Controls, by creating an affirmative defense against lawsuits resulting from a data breach.
Status: Effective date: November 1, 2018.
Link: Senate Bill 220, codified at O.R.C. §§ 1354.01-1354.05: http://codes.ohio.gov/orc/1354

Appendix 2: Select Global Endorsements That Support Implementing the Goals of the NIST CSF

This list represents some of the government and private sector entities that have recommended or otherwise adopted the CIS Critical Security Controls.

- **NIST, "Framework for Improving Critical Infrastructure Cybersecurity Framework," Version 1.1, Apr 16, 2018**. Cites and maps to "CIS CSC" throughout Appendix A, Framework Core at 22-44. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

- **Verizon, "DBIR Data Breach Investigations Report," 2022.** Recommends the CIS Controls. "In addition, we provide a description of what Center for Internet Security (CIS) Critical Security Controls to prioritize in each industry section for ease of reading if you want to get straight to strategizing your security moves." Report at 50. The CIS Controls Implementation Group 1 (IG1) is recommended at the industry sections at 53, 55, 57, 59, 61, 63, 65, 67, 71, 73. https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf

- **American Aerospace and Defense Industry, NAS9933, Critical Security Controls for Effective Capability in Cyber Defense, Nov. 29, 2018.** Based on the CIS Controls. https://global.ihs.com/images/SUPPLEMENTAL_DOCUMENTS/21/AIA-NAS9933_overview.pdf

- **Federal Financial Institutions Examination Council, "FFIEC Encourages Standardized Approach to Assessing Cybersecurity Preparedness," Aug. 28, 2019.** Recommends the Critical Security Controls as one of four specific tools. The FFIEC prescribes uniform principles, standards, and report forms and to promote uniformity in the supervision of financial institutions. https://www.ffiec.gov/press/pr082819.htm

- **Conference of State Bank Supervisors, "Cybersecurity 101, A Resource Guide for Bank Executives," 2017.** Recommends use of the Critical Security Controls at 8, 12, 24. https://www.csbs.org/sites/default/files/2017-11/CSBS%20Cybersecurity%20101%20Resource%20Guide%20FINAL.pdf

- **FCC, Communications Security, Reliability and Interoperability Council, CISRIC III, Working Group 11, "Consensus Cyber Security Controls Final Report," March 2013**. Finds that the "user community within Working Group 11 would prefer for the FCC to encourage industry to use the 20 Controls because they believe that the 20 Controls will protect the network infrastructure directly. The user group also believes that the 20 Controls have been demonstrated to be effective in protecting critical infrastructure from attacks that are likely to come through the enterprise systems and therefore the 20 Controls should be used by the communications industry." Report at 8. https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG11_Report_March_%202013Final.pdf

- **FCC, Communications Security, Reliability and Interoperability Council, CSRIC IV, Working Group 3, "Emergency Alert System (EAS) Initial Security Subcommittee Report," May 2014.** Recommending the CIS Controls (then known as the "SANS 20 Critical Security Controls") as part of its recommended Network and Operational Controls. https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG-3_Initial-Report_061814.pdf

- **NIST, U.S. Resilience Project, "Best Practices in Cyber Supply Chain Risk Management."** Boeing's IS team stated that its "primary standard is the Critical Security Controls." See at 4. https://www.nist.gov/system/files/documents/itl/csd/NIST_USRP-Boeing-Exostar-Case-Study.pdf

- **U.S. Department of Transportation, Federal Highway Administration, Transportation Management Center Information Technology Security, Final Report, Sep. 2019**. Critical Security Controls cited throughout as insight into basic practices that serve as a starting point or baseline for organizations with limited resources and cybersecurity expertise, as well as guidelines for Traffic Management Centers looking to increase their system maturity. https://ops.fhwa.dot.gov/publications/fhwahop19059/fhwahop19059.pdf

- **State of Nevada, SB302, Chap. 412, An Act relating to privacy; requiring a governmental agency to comply, to the extent practicable, with certain standards with respect to the collection, dissemination and maintenance of records containing personal information of a resident of this State.** Requires state data collectors to implement and maintain "reasonable security measures" to protect such records. (NRS 603A.210.) A new Nevada statute, which became effective on January 1, 2021, requires that the state data collectors comply with the CIS Critical Security Controls or the NIST Cybersecurity Framework, thus defining what constitutes reasonable security for the state as a PII collector. https://www.leg.state.nv.us/App/NELIS/REL/80th2019/Bill/6534/Overview

- **State of Ohio, Chapter 1354, Businesses Maintaining Recognized Cybersecurity Programs.** The Ohio Data Protection Act became the first American statute to incentivize organizations to develop a strong data protection and cybersecurity program. The statute establishes legal protections for organizations that voluntarily adopt certain recognized cybersecurity best practices and implement a written information security program. See Senate Bill 220, codified at O.R.C. §§ 1354.01-1354.05, CIS Controls at 4. http://codes.ohio.gov/orc/1354

- **State of Utah, Data Security Amendments.** The Utah Cybersecurity Affirmative Defense Act incentivizes the voluntary adoption of cyber best practices by creating affirmative defenses to certain lawsuits stemming from a security breach. Specifically, the Act provides that a person or organization that "creates, maintains, and reasonably complies with a written cybersecurity program meeting certain requirements, and which is in place at the time of a breach of system security, has an affirmative defense to a claim brought under the laws of Utah alleging that the person failed to implement reasonable information security controls that resulted in the breach of system security." See House Bill 80 signed into law on March 11, 2021. https://le.utah.gov/~2021/bills/static/HB0080.html

- **State of Connecticut, "An Act Incentivizing the Adoption of Cybersecurity Standards for Businesses."** Connecticut adopted provisions that incentivizes the voluntary adoption of cyber best practices, including the CIS Controls. Instead of creating an affirmative defense, like Ohio and Utah, Connecticut's incentive is to bar punitive damages against any organization that is sued for a breach that uses one of the named best practices. See House Bill 6607 signed into law at Public Act No. 21-119 on July 6, 2021, https://cga.ct.gov/2021/ACT/PA/PDF/2021PA-00119-R00HB-06607-PA.PDF

- **State of California, "California Data Breach Report," Feb. 2016.** Attorney General Kamala Harris' report warns that failing to implement all relevant Controls in California "constitutes a lack of reasonable security." The Report effectively constituted a ground-breaking minimum level of information security. See https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf . Subsequent analysis cites the endorsement of the Controls as reasonable security: https://www.littler.com/publication-press/publication/employers-receive-last-minute-reprieve-most-onerous-ccpa-compliance?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original

- **State of Colorado, Data Security Best Practices.** The Colorado Attorney General Data Security Best Practices guide states that: "While each entity's data security needs and practices may differ, there are some common best practices that most, if not all covered entities can implement." The guide recommends the CIS Critical Security Controls as part of Step 2, the written information security policy at 3. https://coag.gov/app/uploads/2022/01/Data-Security-Best-Practices.pdf

- **World Economic Forum (WEF), White Paper, Global Agenda Council on Cybersecurity, World Economic Forum, Apr. 2016.** Listed CIS Controls as the first best practice at 19, CIS cyber hygiene at Appendix A at page 26. https://www3.weforum.org/docs/GAC16_Cybersecurity_WhitePaper_.pdf

- **ENISA (European Union Agency for Network and Information Security), "Technical Guidelines for the implementation of minimum security measures for Digital Service Providers," Dec. 2016**. Cited the CIS Controls as a means for meeting EU Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS). See page 10 and mapping throughout. https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers/at_download/fullReport

- **ETSI (European Telecommunications Standards Institute).** Transposed all of the Critical Security Controls and Safeguards and associated facilitation mechanisms into formal international specifications for global citation and normative use within the European Union. The Controls were also designated as the means of implementing most of the provisions of the of the original and recently adopted European Union (EU) Revised Network and Information Security (NIS2).

- ETSI TR 103 305-1: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls," https://www.etsi.org/deliver/etsi_tr/103300_103399/10330501/04.01.02_60/tr_10330501v040102p.pdf
- ETSI TR 103 305-3: "CYBER; Critical Security Controls for Effective Cyber Defence; Part 3: Service Sector Implementations," https://www.etsi.org/deliver/etsi_tr/103300_103399/10330503/02.01.01_60/tr_10330503v020101p.pdf
- ETSI TR 103 305-4: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 4: Facilitation Mechanisms," https://www.etsi.org/deliver/etsi_tr/103300_103399/10330504/02.01.01_60/tr_10330504v020101p.pdf
- ETSI TR 103 305-5: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 5: Privacy enhancement," https://www.etsi.org/deliver/etsi_tr/103300_103399/10330505/01.01.01_60/tr_10330505v010101p.pdf
- ETSI TR 103 456: "CYBER; Implementation of the Network and Information Security (NIS) Directive," https://www.etsi.org/deliver/etsi_tr/103400_103499/103456/01.01.01_60/tr_103456v010101p.pdf
- ETSI TR 103 866: "Cyber Security (CYBER); Implementation of the Revised Network and Information Security (NIS2) Directive applying Critical Security Controls," https://docbox.etsi.org/CYBER/CYBER/05-CONTRIBUTIONS/2022//CYBER(22)032048_Implementation_of_the_NIS2_Directive.zip