Sec. 5274 of the National Defense Authorization Act of 2023 (Sec. 5274) requires OIGs to notify all non-governmental organizations or business entities that are specifically mentioned in an OIG report. Sec. 5274 further requires the OIG to attach any response received from a non-governmental organizations or business entity to the report where they are mentioned. Therefore, in accordance with Sec. 5274, attached is a response provided to CPSC OIG regarding the *Evaluation of the CPSC's FISMA Implementation for FY 2023,* Document No: 23-A-05, Issued July 28, 2023. This response represents the views of the Center for Internet Security and not CPSC OIG and was not reviewed by this office.

Written Comments

Submitted by the

Center for Internet Security

August 27, 2023

regarding the

Evaluation of the CPSC's FISMA Implementation for FY 2023

Document No: 23-A-05

Issued July 28, 2023

Office of the Inspector General

U.S. Consumer Product Safety Commission

I. EXECUTIVE SUMMARY

On July 28, 2023, the Office of Inspector General ("OIG") of the U.S. Consumer Product Safety Commission (the "Commission" or "CPSC") produced a report called "Evaluation of the CPSC's FISMA Implementation for FY 2023" ("Evaluation" or "Report"). The Report relies in part on the guidance of the Critical Security Controls ("CIS Controls") produced by the independent nonprofit Center for Internet Security ("CIS") (www.cisecurity.org). While the Report does not describe specifically how the CIS Controls were used in the analysis, we appreciate the confidence in the CIS Controls and offer the following observations about how they support OMB guidance, as well as the goals of the FISMA process, and can be broadly applied. In short, and as more specifically described below:

A. The CIS Controls are effective, measurable, and inherently provide a risk-management basis to an enterprise security program.

B. The CIS Controls are much more than a list of recommendations – they are the centerpiece of an ecosystem of products, services, and information that can be used to build and manage an enterprise security program.

C. The CIS Controls are designed for "pro-active co-existence" with a worldwide ecosystem of security frameworks, recommendations, and other guidance.

D. Use of the CIS Critical Security Controls is internationally compatible.

II. BACKGROUND

To provide the annual independent evaluation of compliance of the information security program of the Commission as required by the Federal Information Security Modernization Act ("FISMA"), the Commission's OIG retained the independent public accounting firm of Williams, Adley, & Co.-DC LLP ("Williams Adley"). Williams Alley produced a report to document its evaluation. The Report noted that *"Evaluation, testing, and analysis were performed in consideration with guidance from the following:,"* including the "Center for Internet Security

Top 18 Security Controls,"[1] more formally known as the Critical Security Controls (or the CIS Controls).

Established in 2000 as an independent nonprofit organization, the Center for Internet Security's mission is to make the connected world a safer place by using open, collaborative deliberation processes to define, share, and sustain security best practices against cyber threats. These best practices represent the consensus opinion of experts from across the global security community and are freely available to all enterprises. CIS has over 20 years of success in developing, sharing, and sustaining security best practices, powered by a successful nonprofit business model. For example, CIS was instrumental in establishing the first public guidelines for security hardening of commercial IT systems (now known as CIS Benchmarks) when there was little online security leadership – and CIS is now the world's largest independent source of security configuration hardening.

CIS also operates both the Multi-State Information Sharing and Analysis Center ("MS-ISAC") and the Elections Infrastructure ISAC ("EI-ISAC"). Currently, these two ISACs provide cyber threat sharing information and some cybersecurity defensive tools to all 56 states and territories and over 15,000 tribal and local government organizations.

Most notably, CIS is also the home of the CIS Critical Security Controls, the set of internationally-recognized, prescriptive, prioritized operational security practices that form the foundation of essential cyber hygiene--network defense that is demonstrated to prevent 80-90% of all known pervasive and dangerous cyberattacks. The CIS Controls had their origins at the National Security Agency and are now compiled and used by cybersecurity experts around the world. By design, the CIS Controls help implement the goals of the NIST framework by providing a roadmap for network operators to improve cybersecurity by identifying specific actions to be done in priority order based on the current state of the global cyber threat. What results is the clearest, most definitive blueprint of how to protect an organization from cyber-attacks. While the NIST Cybersecurity Framework ("NIST CSF") is the *what*--NIST defines the categories of cybersecurity and an organizational view of security risk management—the Controls are the *how*--the prioritized technical pathway to achieve the NIST goals. Moreover, the CIS Controls

[1] *Evaluation of the CPSC's FISMA Implementation for FY 2023*, Document No: 23-A-05, Issued July 28, 2023, Office of the Inspector General, U.S. Consumer Product Safety Commission. https://www.oversight.gov/sites/default/files/oig-reports/CPSC/Evaluation-CPSCs-FISMA-Implementation-FY2023.pdf See the CIS Controls on page 34.

are specifically referenced in the NIST CSF as one of the tools to implement an effective cyber-security program.[2]

CIS's ability to develop useful, real-world security practices like the CIS Benchmarks and CIS Controls is driven by: our large-scale activity to gather feedback from worldwide users of our guidance; and our nationwide, 24x7 mission operating the two ISACs (supporting all 56 states and territories and over 15,000 local and tribal government organizations).

III. THE CIS CRITICAL SECURITY CONTROLS ARE THE RIGHT STANDARD AS THE NATION MIGRATES FROM A CHECK-THE-BOX TO A RISK-MANAGEMENT APPROACH TO CYBERSECURITY BECAUSE OF THEIR EFFECTIVENESS, MEASURABILITY, ADAPTABILITY, AND SCALABILITY, AS WELL AS THEIR GROWING ADOPTION AROUND THE WORLD.

While the Report does not describe specifically how the CIS Controls were used in the analysis, we appreciate the confidence in the CIS Controls and offer the following observations about how they support OMB guidance, as well as the goals of the FISMA process, and can be broadly applied:

A. The CIS Controls are effective, measurable, and inherently provide a risk-management basis to an enterprise security program.

From the report (Page 10): *"Reflecting OMB's shift in emphasis away from compliance in favor of risk management, IGs are encouraged to evaluate the IG metrics based on the risk tolerance and threat model of their agency and to focus on the practical security impact of weak control implementations, rather than strictly evaluating from a view of compliance or the mere presence or absence of controls."* The CIS Controls support these goals as follows:

CIS uses an open, documented, data-driven process to establish the security effectiveness of every recommendation in the Controls. The CIS Community Defense Model starts from the threat intelligence industry's leading analyses of real-life attacks (e.g., the Verizon Data Breach Investigations Report) to identify the most important and pervasive classes of cyber attack; formalizes the description of these attack classes using the industry-leading MITRE ATT&CK Framework; then establishes the specific effectiveness of every recommendation in terms of its

[2] NIST Cybersecurity Framework, Appendix A, page 20, and throughout the Framework Core (referred to as "CCS CSC" - Council on Cyber Security (the predecessor organization to CIS for managing the Critical Security Controls): https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

value against each attack class. This enables our recommendations to focus on the most important problems, prioritize action against them, and also avoid "good things to do." It also allows us to make strong and defensible statements about the effectiveness of the CIS Controls as a whole or for any subset of them. ***Overall, CIS Controls mitigate approximately 83% of all attack techniques found in the MITRE ATT&CK Framework***.[3]

The CIS Controls can be tailored by size and maturity of the implementing organization. The CIS Controls Implementation Groups[4] provide both an onramp 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. ***Even at the simplest level, IG1, the CIS Controls remain very effective, protecting against 74% of all attack vectors identified in the MITRE ATT&CK model.***[5]

B. The CIS Controls are much more than a list of recommendations – they are centerpiece of an ecosystem of products, services, and information that can be used to build and manage an enterprise security program.

From the Report (Page 15): *"The CPSC information security program was not effective because the CPSC still has not developed a* ***holistic formal approach*** *to manage information security risks or to effectively utilize information security resources to address previously identified information security deficiencies. Explicit guidance and processes to address information security risks and integrate those risks into the broader agency-wide ERM program have not been developed. Therefore, the CPSC's ERM program remains insufficient ....."*

CIS provides numerous tools and services, most freely available, to support an enterprise security program, including tools to: implement and measure against CIS security hardening guidance; assess and manage a security improvement program; apply sector-specific guidance (e.g., "cloud," Small Enterprises); learn from communities of similar enterprises.

The marketplace also supports CIS best practices across a wide variety of categories, including vulnerability management, configuration checking and management, and GRC.

---

[3] https://www.cisecurity.org/insights/white-papers/cis-community-defense-model-2-0
[4] https://www.cisecurity.org/controls/implementation-groups
[5] *Id* at n.8.

C. The CIS Controls are designed for "pro-active co-existence" with a worldwide ecosystem of security frameworks, recommendations, and other guidance.

Many enterprises must report progress against multiple security frameworks or sets of requirements, depending on their industry sector, regulatory environment, geographic reach, types of data handled, supply chain concerns, etc. Reporting to multiple systems creates confusion, reformatting, and repeat-work.

Recognizing this challenge, CIS develops freely available, industry-vetted mappings to and from CIS products to numerous major security frameworks (like the NIST CSF, NIST 800-53, PCI, HIPAA, CMCC, ISO/IEC 27001-27002, etc.).[6] Wherever possible, we reach out the target framework and offer to cooperate and develop a joint cross-map between frameworks. For example, in the most recent version of the CIS Controls, we worked jointly with the Cloud Security Alliance to up-front map between the CIS Controls and their Cloud Control Matrix. This provides a clear and authoritative way to use both in their enterprise security program.

Currently, we have mapped to over 25 cybersecurity frameworks around the world.

D. Use of the CIS Critical Security Controls is internationally compatible

Selected global adoptions and endorsements of the CIS Controls signify its growing status as an emerging global, de facto minimum standard of information security. (See Annex 1.)

For example, the Federal Communication Commission ("FCC") is currently undertaking a cybersecurity rulemaking in emergency communications sector that names the CIS Critical Security Controls as one of two acceptable standards. CIS is assisting the implementation of these best practices globally through new technical specification work items at the European Telecommunications Standards Institute ("ETSI") – in coordination with all relevant industry and standards bodies.[7] Key cybersecurity threats and mitigations have been known and identified in multiple organizations and nations worldwide, including ETSI's Emergency Telecommunications Technical Committee ("EMTEL"), 3GPP, and GSMA. Indeed, the European Union's new NIS2

---

[6] https://www.cisecurity.org/controls/cis-controls-navigator/

[7] *Notice of Proposed Rulemaking in the Matter of Communications Assistance for Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System, PS Docket No. 15-94 Wireless Emergency Alerts, PS Docket No. 15-91 Protecting the Nation's Communications Systems from Cybersecurity Threats, PS Docket No. 22-329*, Document 22-82, released 27 October 2022, (hereafter referred to as *NPRM*). See Federal Register, Vol 87, No. 225, Wednesday, November 23, 2022, at pages 71539 - 71557 *See* ETSI, Doc. CYBER(22)032007, Protecting the European Public Warning Service from cyber security threats, 29 Nov 2022.

Directive mandates measures that similar to and in some instances exceeding the FCC's proposed requirements.[8] The EU 2018 Electronic Communication Code also requires safety requirements that are equivalent to those proposed by the FCC.[9] The significant level of interest at recent ETSI standards plenary meetings, combined with the new EU cyber security mandates coming into force, suggests that this new work can be undertaken expeditiously.

Not just global standards bodies have been relying on the CIS Controls. Overall, since 2016, over 416,000 organizations around the world have downloaded the CIS Controls globally. Of the 30,220 downloads of the CIS Controls so far in 2023, appoximately 61% are from outside the U.S.

IV. CONCLUSION

The CPSC OIG Report on the Commission's FISMA Implementation for FY 2023 relies in part on the guidance of the CIS Critical Security Controls, which support OMB guidance and the of the FISMA process and can be broadly applied. In short:

A. The CIS Controls are effective, measurable, and inherently provide a risk-management basis to an enterprise security program.

B. The CIS Controls are much more than a list of recommendations – they are centerpiece of an ecosystem of products, services, and information that can be used to build and manage an enterprise security program.

C. The CIS Controls are designed for "pro-active co-existence" with a worldwide ecosystem of security frameworks, recommendations, and other guidance.

D. Use of the CIS Critical Security Controls is internationally compatible.

We would be happy to answer any questions that you might have.

---

[8] *See Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*.

[9] *See* Title V, Security*, Consolidated text: Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code*

ANNEX 1:

SELECTED ADOPTION AND ENDORSEMENT OF THE CIS CRITICAL SECURITY CONTROLS

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

- **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
- **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
- **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

- **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