epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

Before the
CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY
DEPARTMENT OF HOMELAND SECURITY
Washington, DC 20032

In the Matter of	)	
	)	
Shifting the Balance of Cybersecurity Risk:	)	CISA-2023-0027
Principles and Approaches for Secure by Design	)	
Software	)	

COMMENTS ON REQUEST FOR INFORMATION

by

Electronic Privacy Information Center (EPIC)

Submitted February 20, 2024

Chris Frascella
Counsel
Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036

Summary

We applaud the important work that the Cybersecurity and Infrastructure Security Agency (CISA) is undertaking to help businesses implement and maintain more cybersecure practices, especially in the context of software development. The security and privacy of personal data is of the utmost concern to American consumers, and too often we have seen sensitive information breached. When systems are compromised, not only the breached business incurs financial losses, but trust in the marketplace diminishes as well. Preventing bad actors from harvesting personal data from software and systems containing this information is both a cybersecurity and a privacy priority, and federal policy must continue to incentivize businesses to act accordingly.

We support using incentives to enhance cybersecurity, for example by tasking manufacturers with taking ownership for the outcomes and not merely the inputs of their cybersecurity practices. We also support establishing a baseline for cybersecurity practices that is closer to reasonable (e.g., no extra charge for features that amount to foundational protections). We urge CISA to consider how its report might better: emphasize the role of data minimization in both cybersecurity and privacy contexts; recommend the use of consistent, independent, and thorough audits at software companies; reiterate other practices that constitute the current baseline for reasonable cybersecurity practices; and support enforcement by individuals and agencies charged with implementing and enforcing privacy and data security standards. We also offer additional security considerations related to artificial intelligence (AI).

Table of Contents

Summary **ii**

I. Introduction **1**

II. Externalizing Costs for Deficient Data Security and Data Privacy onto American Consumers is Unsustainable, as the Administration Has Recognized. **3**

III. CISA's Draft White Paper Makes Many Strong Recommendations. **7**
a. Using incentives to enhance security practices by tasking manufacturers with taking ownership for outcomes and not merely inputs 7
b. Establishing a baseline that aligns with actual reasonable practice 9

IV. CISA Should Incorporate Other Important Concepts into its White Paper. **9**
a. Data minimization is a fundamental cybersecurity practice. 11
b. Audits must be adequately independent, thorough, and frequent. 11
c. Other near-consensus practices the white paper should encourage include data mapping, segmentation of systems, and threat detection. 12
d. The white paper should be framed to support meaningful enforcement. 16

V. Additional Cybersecurity Considerations for Artificial Intelligence **18**

VI. Conclusion **19**

APPENDIX 1- New Baseline Expectations for Data Security: Consensus on Cybersecurity Hygiene for the Modern Threat Environment

Comments

I. Introduction

The Cybersecurity and Infrastructure Security Agency ("CISA" or "the Agency") requested comment on its draft white paper,[1] "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software," as well as on thirteen additional topics including the economics of software vulnerabilities, the economics of customer demand, and secure development of artificial intelligence (AI).[2] The **Electronic Privacy Information Center (EPIC)** files these comments to applaud the Agency for its prompt action in support of strengthening baseline cybersecurity requirements.[3]

EPIC is a public interest research center in Washington, D.C., established in 1994 to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation. EPIC has long defended the rights of consumers and has played a leading role in developing regulatory authority to address emerging privacy and cybersecurity issues.[4] EPIC

[1] Cybersecurity and Infrastructure Security Agency, Request for Information on "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software", 88 Fed. Reg. 88,104 (Dec. 20, 2023), https://www.federalregister.gov/documents/2023/12/20/2023-27948/request-for-information-on-shifting-the-balance-of-cybersecurity-risk-principles-and-approaches-for [hereinafter RFI].

[2] *See* RFI at 88,106, https://www.federalregister.gov/d/2023-27948/p-50 (software vulnerabilities); id. https://www.federalregister.gov/documents/2023/12/20/2023-27948/request-for-information-on-shifting-the-balance-of-cybersecurity-risk-principles-and-approaches-for#p-60 (customer demand); id. at 88,107 https://www.federalregister.gov/documents/2023/12/20/2023-27948/request-for-information-on-shifting-the-balance-of-cybersecurity-risk-principles-and-approaches-for#p-82 (AI).

[3] Electronic Privacy Information Center, https://epic.org/. EPIC Spring Intern Sophie Nyombi Nantanda contributed to the preparation of these comments.

[4] *See, e.g.*, EPIC, Generating Harms: Generative AI's Impact & Paths Forward (May 2023), https://epic.org/documents/generating-harms-generative-ais-impact-paths-forward/; Consumer Reps. & EPIC, How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking (2022), https://epic.org/documents/how-the-ftc-can-mandate-data-minimization-through-a-section-5-unfairness-rulemaking/; EPIC, What the FTC Could Be Doing (But Isn't) To Protect Privacy: The FTC's Unused Authorities (2021), https://epic.org/privacy/consumer/EPIC-FTC-Unused-Authorities-Report-June2021.pdf; *In re* Implementation of the Telecommunications Act of 1996, Petition of the Electronic Privacy Information Center for Rulemaking to Enhance Security and Authentication Standards For Access to Customer Proprietary Network

routinely advocates before regulatory agencies for rules that protect consumers from exploitative or negligent data practices.[5] This advocacy is aligned with pillars one and three of the National Cybersecurity Strategy,[6] which call for stronger minimum cybersecurity requirements to defend critical infrastructure and for privacy and data security practices that drive security and resilience.

In Section II of these comments, we emphasize the vulnerability of American consumers to unauthorized access to their sensitive information and the externalized costs of deficient cybersecurity practices borne by individuals and markets. We also discuss CISA's draft white paper and related questions in the context of the White House National Cybersecurity Strategy (NCS).

In Section III, we articulate our support for what is already included in the draft white paper, including alignment with the NCS and promotion of some consensus baseline cybersecurity practices.

Section IV addresses what we would have liked to see in the draft white paper but was not included. This includes data minimization, auditing, other consensus baseline cybersecurity practices, and framing that supports enforcement as a means of creating incentives for secure by design practices.

Section V briefly raises additional cybersecurity considerations for secure software development as it relates to AI.

Information, CC Docket. No. 96-115, RM-11277 (Aug. 30, 2005), https://www.fcc.gov/ecfs/search/search-filings/filing/5513325075.

[5] *See, e.g.*, EPIC, Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem (Nov. 2022), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf [hereinafter "Disrupting Data Abuse"]; *In re* Data Breach Reporting Requirements, Comments of EPIC, WC Docket. No. 22-21 (Feb. 22, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/10222069458527.

[6] *See* Fact Sheet: Biden-Harris Administration Announces National Cybersecurity Strategy (Mar. 2, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/.

II. Externalizing Costs for Deficient Data Security and Data Privacy Onto American Consumers is Unsustainable, as the Administration Has Recognized.

We applaud the Agency's attention to the externalized costs of deficient cybersecurity on consumers.[7] As many as half of U.S. consumers have been affected by data breaches because a company holding their personal information was hacked.[8] That is significantly higher than the global average of just 33 percent of consumers.[9] These data breaches can lead to far-reaching harms including account compromise, identity theft,[10] and public exposure of sensitive personal information. And yet in many cases the underlying breach is neither difficult nor expensive to prevent if best practices are followed by the company that holds or controls the data. The Department of Homeland Security has itself estimated that 85 percent of data breaches were preventable,[11] and more recently the Internet Society has estimated 95 percent of breaches could have been prevented with reasonable safeguards.[12] The Federal Trade Commission (FTC) has brought numerous enforcement actions against companies for failing to implement readily-available low-cost security measures.[13] Despite these realities, earlier this year an IBM study reported that

[7] See RFI at (5)(b)(i) https://www.federalregister.gov/documents/2023/12/20/2023-27948/request-for-information-on-shifting-the-balance-of-cybersecurity-risk-principles-and-approaches-for#p-57 ("Do software manufactures calculate costs for consumers?").
[8] *See* Prof. Carsten Maple, *2022 Consumer Digital Trust Index: Exploring Consumer Trust in a Digital World* 9 (2022), available at https://cpl.thalesgroup.com/resources/encryption/consumer-digital-trust-index-report.
[9] *See* id.
[10] In October 2023, DOJ BJS estimated that as of 2021 more than one in five (22%) of Americans aged 16 and older have experienced identity theft at some point in their lifetime. *See* Bureau of Justice Statistics, Victims of Identity Theft, 2021, at 14, Table 10 (Oct. 2023), https://bjs.ojp.gov/document/vit21.pdf.
[11] *See* 37 Dep't of Homeland Sec. Comput. Emergency Readiness Team, TA15-119, *Alert: Top 30 Targeted High Risk Vulnerabilities* (2016), https://www.cisa.gov/news-events/alerts/2015/04/29/top-30-targeted-high-risk-vulnerabilities.
[12] *See* Internet Society's Online Trust Alliance, *2018 Cyber Incident & Breach Trends Report* at 3 (July 9, 2019), https://www.internetsociety.org/wp-content/uploads/2019/07/OTA-Incident-Breach-Trends-Report_2019.pdf.
[13] *See, e.g.*, Complaint, *In re Residual Pumpkin Entity, LLC, d/b/a CafePress*, FTC File No. 1923209 at ¶ 11(a), 11(i)(i) (Jun. 23, 2022), https://www.ftc.gov/legal-library/browse/cases-proceedings/1923209-cafepress-matter [hereinafter CafePress]; Complaint, *In re SkyMed International, Inc.*, FTC File No. 1923140 at ¶ 23 (Jan. 26, 2021), https://www.ftc.gov/legal-library/browse/cases-proceedings/1923140-skymed-international-inc-matter; Complaint, *In re InfoTrax Systems, L.C.*, FTC File No. 1623130 at ¶ 11 (Dec. 30,

breached organizations were more likely to pass the cost of incidents on to consumers rather than invest in better cybersecurity practices.[14] This is not a sustainable model.

The consequences of failing to safeguard consumer data are not merely financial and do not fall solely on individual consumers victimized by breaches. The National Telecommunications and Information Administration (NTIA) has emphasized that Americans are increasingly concerned about online security and privacy, reporting that 45 percent of American households have abandoned conducting financial transactions, posting on social networks, or expressing opinions on the internet due to privacy and/or security concerns—and that 30 percent refrained from at least two of these activities.[15] 63 percent of surveyed online households voiced concerns about identity theft, with 22 percent concerned about loss of control over personal data and 23 percent concerned with data collection by online services.[16] These numbers were elevated if the household had suffered a security breach in the year prior to the survey: for example, 70 percent were concerned about identity theft and 30 percent were concerned about data collection or tracking by online services.[17] As NTIA has

2019), https://www.ftc.gov/legal-library/browse/cases-proceedings/162-3130-infotrax-systems-lc [hereinafter InfoTrax]; Complaint, *In re LightYear Dealer Technologies, LLC*, FTC File No. 1723051 at ¶ 22 (Sept. 6, 2019), https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3051-lightyear-dealer-technologies-llc-matter [hereinafter LightYear]; Complaint, *FTC v. Equifax, Inc.*, No. 1:2019-cv-03297 at ¶¶ 23(A)(iv), 24 (N.D. Ga. Jul. 22, 2019), https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3203-equifax-inc [hereinafter Equifax]; Complaint, *FTC v. Ruby Life Inc. d/b/a AshleyMadison.com*, No. 1:16-cv-02438 at ¶¶ 23(A)(iv), 24 (D.D.C. Dec. 14, 2016), https://www.ftc.gov/legal-library/browse/cases-proceedings/152-3284-ashley-madison [hereinafter AshleyMadison]; Complaint, *In re Lenovo, Inc.*, FTC File No. 1523134 at ¶ 25 (Jan. 2, 2018), https://www.ftc.gov/legal-library/browse/cases-proceedings/152-3134-lenovo-inc [hereinafter Lenovo].

[14] *See* IBM Report: Half of Breached Organizations Unwilling to Increase Security Spend Despite Soaring Breach Costs (July 24, 2023), https://newsroom.ibm.com/2023-07-24-IBM-Report-Half-of-Breached-Organizations-Unwilling-to-Increase-Security-Spend-Despite-Soaring-Breach-Costs.

[15] *See* Rafi Goldberg, Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities, National Telecommunications and Information Administration, https://www.ntia.gov/blog/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities (last visited Oct. 31, 2023).

[16] *See* id.

[17] *See* id.

reported, there is a clear connection between the strength of privacy and security safeguards on the one hand and healthy commerce and trust in American networks on the other hand.

PricewaterhouseCoopers and McKinsey have also found that consumers believe their privacy and data security are a high priority.[18] Pew Research Center has found that users consider privacy of their data to be of the utmost importance and found that users feel powerless and vulnerable when companies fail to safeguard their data.[19] In 2022, VentureBeat summarized a Thales report as indicating that "more than one-fifth of consumers stopped using a company that experienced a data breach."[20] The cybersecurity status quo is no longer acceptable. If greater protections are not

[18] *See, e.g.*, PwC, Consumer Intelligence Series; Protect.me (2017), available at https://www.fisglobal.com/-/media/fisglobal/worldpay/docs/insights/consumer-intelligence-series-protectme.pdf ("88% say that their willingness to share their personal data is determined by how much they trust a company, and 87% will go elsewhere if they are given reason not to trust a business."); PwC, Are we ready for the Fourth Industrial Revolution?, https://www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/fourth-industrial-revolution.html (last visited Oct. 31, 2023) (64% of consumers want assurance of immediate notification if personal data is compromised); Venky Anant et al., The consumer-data opportunity and the privacy imperative, McKinsey & Company (Apr. 27, 2020), https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative (noting that consumer trust levels are "low overall", with the highest being 44% in healthcare and in financial services).

[19] *See, e.g.*, Kenneth Olmstead and Aaron Smith, Americans' experiences with data security, Pew Research Center (Jan. 26, 2017), https://www.pewresearch.org/internet/2017/01/26/1-americans-experiences-with-data-security/ ("roughly half (49%) of all Americans feel their personal information is less secure than it was five years ago."); Brook Auxier, et al, Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information, Pew Research Center (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/ americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ ("81% of Americans think the potential risks of data collection by companies about them outweigh the benefits… Roughly seven-in-ten or more say they are not too or not at all confident that companies will admit mistakes and take responsibility when they misuse or compromise data"); Andrew Perrin, Half of Americans have decided not to use a product or service because of privacy concerns, Pew Research Center (Apr. 14, 2020), https://www.pewresearch.org/fact-tank/2020/04/14/half-of-americans-have-decided-not-to-use-a-product-or-service-because-of-privacy-concerns/ ("Overall, adults who experienced any of these three data breaches were more likely than those who did not to avoid products or services out of privacy concerns (57% vs. 50%).").

[20] *See* VB Staff, Report: 33% of global consumers are data breach victims via hacked company-held personal data, VentureBeat (Dec. 11, 2022), https://venturebeat.com/security/report-33-global-consumers-data-breach-victims-hacked-company-held-personal-data/.

implemented, multiple breaches each impacting tens or hundreds of millions of Americans will continue to occur every year, further diminishing public trust.[21]

Last year, the White House outlined a strategy and corresponding implementation plan that can help to guide the federal government's response to these issues.[22] Most relevant to this discussion, the strategy calls for establishing cybersecurity minimum requirements in critical sectors and for improving privacy and data security practices in all sectors (by shaping market forces to drive security and resilience).[23] CISA clearly has an important role to play in strengthening requirements in critical sectors, but through efforts like this white paper the Agency also clearly demonstrates what role it might play in helping to shape market forces.[24]

[21] *See, e.g.*, Press Release, Identity Theft Resource Center Sees Record-Setting Number of Data Compromises in Q2; On Pace to Set New Yearly Record, Identity Theft Resource Center (July 12, 2023), https://www.idtheftcenter.org/post/identity-theft-resource-center-sees-record-setting-number-of-data-compromises-q2-on-pace-new-yearly-record/ (also reporting T-Mobile as the largest breach in the first half of 2023); Bree Fowler, Data Breaches Break Record in 2021, CNET (Jan. 24, 2022), https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/. Statista provides a graph of the number of reported data breaches dating back to 2005 (at which time there were 157); Statista Rsch. Dep't, Annual Number of Data Compromises and Individuals Impacted in the United States from 2005 to 2022, Statista (Jan. 2023), https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.

[22] *See* Fact Sheet, The White House, Biden-Harris Administration Announces National Cybersecurity Strategy (Mar. 2, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/ [hereinafter NCS March Fact Sheet]; The White House, National Cybersecurity Implementation Plan (July 2023), https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf.

[23] The White House, National Cybersecurity Strategy 23 (March 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

[24] Most directly, CISA's white paper addresses secure-by-design software practices, mirroring the Strategy's emphasis on "[s]hifting liability for software products and services to promote secure development practices." NCS March Fact Sheet. However, as we outline Section IV, *infra*, there's more the Agency can and should be doing to advance the Administration's cybersecurity priorities.

III. CISA's Draft White Paper Makes Many Strong Recommendations.

EPIC supports much of what CISA has chosen to include in its draft white paper. Most notably: using incentives to enhance security practices by taking ownership for outcomes and not merely inputs, and beginning to establish a new baseline that aligns with actual reasonable practices.

a. Using incentives to enhance security practices by tasking manufacturers with taking ownership for outcomes and not merely inputs

Arguably the most important and impactful change to improving cybersecurity outcomes will be achieved by putting an emphasis on the effectiveness of actual practices and not merely a checklist of compliance inputs. As the draft white paper notes:

> Manufacturers should take ownership of their customers' security outcomes rather than measuring themselves solely on their efforts and investments. The responsibility should be placed upstream, with the manufacturers, where it has the greatest likelihood of reducing the chances of compromise.[25]

This is consistent with Pillar Three of the NCS, as it creates incentives to shift the burden on the entity best-equipped to internalize the costs of adequate cybersecurity.[26] We discuss how the white paper can further support market-level incentives in Section IV(d) *infra*.

b. Establishing a baseline that aligns with actual reasonable practice

We are encouraged to see the draft white paper address many baseline cybersecurity practices, such as access controls and authentication, governance, and vulnerability management. While effectiveness in results is more important than compliance in efforts, these consensus or near-consensus practices form a portion of the current foundation for reasonable cybersecurity practices (the other portion is not included in the draft, and is discussed in Section IV immediately *infra*).

---

[25] CISA, et al., Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software 12, https://www.cisa.gov/sites/default/files/2023-10/SecureByDesign_1025_508c.pdf (Oct. 25, 2023 draft) [hereinafter "White Paper Draft"].
[26] NCS March Fact Sheet.

Access controls include both role-based and attribute-based controls, multi-factor authentication,[27] and the elimination of default passwords.[28] These practices can stop some of the most straightforward attempts to compromise a system. The FTC has brought enforcement actions identifying inadequate access controls as a deficient cybersecurity practice since 2017 if not earlier[29] and has recommended the use of access controls since at least 2015.[30] CISA's own framework may be most helpful here, in particular Goals 2.A and 2.B which pertain to passwords, 2.C and 2.D which pertain to disabling accounts, and 2.G which pertains to credential-based attacks.[31] Goal 2.H addresses access- and authentication-based threats specifically as they relate to multi-factor authentication (MFA), noting that SMS-based MFA is a least-preferred safeguard.[32]

Governance includes corporate reports, reports to board of directors, and empowered secure by design executives.[33]

Vulnerability management includes red teaming, paying attention to patching statistics, deprecating unsafe features, and treating vulnerability management as a quality and safety issue, not merely a compliance issue.[34] The FTC has brought enforcement actions against companies with inadequate vulnerability management since 2015.[35]

---

[27] White Paper Draft at 12, 22, 23.
[28] *Id.* at 15.
[29] *See* AshleyMadison at ¶ 31b.
[30] *See, e.g.*, Fed. Trade Comm'n, Start With Security: A Guide for Business (June 2015), https://www.ftc.gov/business-guidance/resources/start-security-guide-business [hereinafter "Start with Security"].
[31] CISA, Cross-Sector Cybersecurity Performance Goals 11-12 (March 2023), https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf [hereinafter "CISA CPGs"].
[32] CISA CPGs at 13 (2.H); New York State Dep't Fin. Servs., Re: Guidance on Multi-Factor Authentication (Dec. 7, 2021), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20211207_mfa_guidance ("Text message-based MFA is vulnerable to SIM-swapping.").
[33] White Paper Draft at 27.
[34] Id. at 15, 16, 17, 22.
[35] *See, e.g.*, First Am. Complaint, FTC v. Wyndham Worldwide Corp., 799 F.3d 236 at ¶ 24d, 29 (3d Cir. 2015); CafePress at ¶ 11a,d,e; Equifax at ¶ 22a,23a; Complaint, FTC v. D-Link Corp., No. 3:17-CV-00039-JD at ¶ 15a (N.D. Cal. Mar. 20, 2017); *In re* Zoom Video Communications, Inc., FTC File No. 1923167 at ¶

While the current draft of the white paper is a good start, we encourage the Agency to consider incorporating additional foundational practices. See Section IV immediately below, as well as Appendix 1.

IV. CISA Should Incorporate Other Important Concepts into its White Paper.

While CISA has already included a number of important recommended practices in its white paper draft, see Section III(c), *infra*, the final publication will be even more impactful if it incorporates additional best practices such as data minimization. Cybersecurity threats not only directly jeopardize national security and the revenue of individual companies but also imperil the privacy and security of the personal data of individual consumers, as discussed in Section II, *infra*. As the white paper notes: "Security should not be a luxury option, but should be considered a right customers receive without negotiating or paying more."[36] Given the outsized influence cybersecurity practices can have on all of these priorities, we urge CISA to include additional guidance in the final version of its white paper to better support cybersecurity best practices, namely: data minimization, auditing, other consensus or near-consensus technical controls. The Agency should also seek to articulate cybersecurity best practices in ways that support enforcement action.

a. Data minimization is a fundamental cybersecurity practice.

A hacker can't gain access to data that a company does not have, and companies should have strong incentives to limit the scope and nature of their collection, especially regarding sensitive data. Software developers should prompt companies to distinguish between what data they actually need to collect vs. not; to establish with whom data may be shared (internally in terms of access controls

12(b) (Feb. 1, 2021), https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3167-zoom-video-communications-inc-matter [hereinafter Zoom].

[36] White Paper Draft at 9.

and externally in terms of partnerships or product integrations); and to determine how long data must be retained.[37] Additionally, we note that limiting sensitive data access to those circumstances when it is strictly necessary (i.e., purpose limitations) also reduces the likelihood of compromise.

Cybersecurity threats not only directly jeopardize national security and the revenue of individual companies but also imperil the privacy and security of the personal data of individual consumers. As Profs. Dan Solove and Woodrow Hartzog have argued:

> [V]iewing data security policy primarily as a collection of requirements for breach notifications and technical controls excludes many of the most important issues from security, and it silos privacy and security in ways that are unproductive…[38] There are several ways that bad privacy can lead to bad security: (1) Weak privacy controls can lead to improper access through the front door; (2) Collecting and storing unnecessary data can make data breaches much worse; (3) Poor privacy regulation can allow for more tools and practices that compromise security; and (4) A lack of accountability over data can increase the likelihood that the data will be lost, misplaced, or misused.[39]

Data minimization, for example, fulfills the reasonable expectations of consumers (including purpose limitations for use of their data) at the same time it addresses data security concerns (companies "don't have to protect what [they] don't collect").[40] The FTC has explicitly listed data minimization alongside risk mitigation and data management and retention as a data security best practice.[41] Additionally, NIST has noted that privacy and security programs have a shared responsibility for managing security risks for PII in a system; that controls for security risks will

[37] Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers at 23, 28-29 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.
[38] *See* Daniel J. Solove & Woodrow Hartzog, Breached! Why Data Security Law Fails and How to Improve It 132-33 (2022), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4173764.
[39] Id. at 143.
[40] John Davisson, Data Minimization: A Pillar of Data Security, But More Than That Too (June 22, 2023), https://epic.org/data-minimization-a-pillar-of-data-security-but-more-than-that-too/.
[41] *See* Fed. Trade Comm'n, Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51,273, 51,277 (advanced notice issued Aug. 22, 2022), https://www.federalregister.gov/d/2022-17752/p-88 [hereinafter FTC ANPR] ("The term 'data security' in this ANPR refers to breach risk mitigation, data management and retention, data minimization, and breach notification and disclosure practices").

likely be the same regardless of whether they are designated as privacy or security controls;[42] that there is need for close collaboration between privacy and security programs in selecting appropriate controls;[43] and that systems must not merely be resistant to attacks and designed to limit damage when attacks do occur but also be protective of individuals' privacy.[44]

b. Audits must be adequately independent, thorough, and frequent.

Audits of software companies must be both independent and thorough. As one example, an audit should not merely report the audit subject's response as to whether an organization has a strong password policy in place; rather, the auditor should actually attempt to set up access with a weak password to see if the policy has been implemented and works as intended.[45] There have been too many examples of audits acting as mere box checking exercises and failing to identify serious deficiencies. For example, whistleblower Peter "Mudge" Zatko explained in Congressional testimony last year that there were serious deficiencies in Twitter's auditing process:

> [H]ow was Twitter still operating like this? Since there was a 2011 consent decree that was aimed at addressing a fair amount of this? . . . One, there were a lot of evaluations and examinations, which were interview questions. So essentially, the organization was allowed to grade their own homework. Did you make things better? Yes, we did. Okay, check. There wasn't a lot of ground truth. There wasn't a lot of quantified measurements. And a fair amount of the interviews came from companies, auditors that Twitter themselves were able to hire. So I think that's a little bit of a maybe conflict of interest.[46]

---

[42] *See* Joint Task Force Transformation Initiative Interagency Working Group (2020) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5, Includes updates as of December 20, 2020, at 13, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf [hereinafter "NIST SP 800-53-r5"]. This publication is for federal government systems, however its observations are applicable globally.
[43] *See* NIST SP 800-53-r5 at 14.
[44] *See* NIST SP 800-53-r5 at ix.
[45] *See* Kevin G. Coleman, *Security Assessment or Security Audit?*, infoTECH Spotlight (Sept. 21, 2009), https://it.tmcnet.com/topics/it/articles/64874-security-assessment-security-audit.htm.
[46] Data Security at Risk: Testimony from a Twitter Whistleblower: Hearing Before the S. Comm. on the Judiciary, 117th Cong. (2022) (testimony of Peter Zatko), https://www.judiciary.senate.gov/meetings/data-security-at-risk-testimony-from-a-twitter-whistleblower.

Mudge suggested the solution include "accountability, and setting quantitative goals and standards that can be measured and audited independently" in order to "change management structures, and drive change in companies when it's needed such as this."[47] We urge CISA to incorporate this discussion of audits in the white paper, specifically requiring actual investigation and analysis and not merely interviews.[48] We also encourage CISA to promote processes that reduce the likelihood of a conflict of interest as described in Mudge's testimony. The California Privacy Protection Agency has proposed measures that may be helpful as relates to the independence of cybersecurity audits, for example ensuring an internal auditor is accountable to an organization's leadership rather than to the management responsible for overseeing the audited cybersecurity program.[49]

c. Other near-consensus practices the white paper should encourage include data mapping, segmentation of systems, and threat detection.

There is striking similarity across multiple state laws, federal sectoral laws, FTC enforcement actions, and both government and non-government frameworks regarding basic modern cybersecurity hygiene.[50] Notably, that includes CISA's Cross-Sector Cybersecurity Performance Goals. For example, as discussed above, data minimization is widely regarded as an essential

[47] Id.

[48] For example, the regulator should state explicitly that a certification is deficient if the company's audit was based solely on staff interviews and did not entail any actual testing of whether the safeguards are operating as intended. *See, e.g.*, The White House, What We Urge You To Do To Protect Against The Threat of Ransomware at 2 (June 2, 2021), https://www.whitehouse.gov/wp-content/uploads/2021/06/Memo-What-We-Urge-You-To-Do-To-Protect-Against-The-Threat-of-Ransomware.pdf ("what we urge you to do now") [hereainafter "2021 WH Memo"].

[49] *See* Draft Cybersecurity Audit Regulations for California Privacy Protection Agency (CPPA) Sept. 8, 2023 Board Meeting, at 7-9 Section 7122, available at https://cppa.ca.gov/meetings/materials/20230908item8.pdf (last visited Oct. 31, 2023).

[50] *See, e.g.*, Comments of EPIC to the FTC Proposed Trade Regulation Rule on Commercial Surveillance & Data Security 194-197 (Nov. 2022), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf; *see also* Comments of the Electronic Privacy Information Center, Center for Digital Democracy, and Consumer Federation of America, to the California Privacy Protection Agency, Proceeding No. 02-23 at Appendix 1 (Mar. 27, 2023), https://epic.org/documents/comments-of-the-electronic-privacy-information-center-center-for-digital-democracy-and-consumer-federation-of-america-to-the-california-privacy-protection-agency/. This is discussed further in Appendix 1.

cybersecurity safeguard across regimes.[51] We identify commonly-required cybersecurity practices holistically in Appendix 1.[52] Below we focus only on the consensus or near-consensus measures that were not included in the draft white paper, namely: data mapping, segmentation of systems, and threat detection. To be clear, we are not asking CISA to create new requirements, only to raise the visibility of prevalent longstanding best practices to the extent that the white paper doesn't already.[53]

i. Data Mapping

Similar to how a software bill of materials (SBOM) can help to quickly identify what components and systems may be impacted by a particular vulnerability,[54] data mapping helps an organization to identify at what points what data is accessible to what systems. Although this largely falls on the organization that is using the software rather than the developers themselves, as with data minimization, there are simple steps a software vendor can take that could nudge its customers to undertake this effort and that could facilitate the effort itself.

[51] *See, e.g.*, NIST, Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 at 34 (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf [hereinafter "NIST CSF 1.1"]; FTC ANPR *supra* note 41; 16 C.F.R. pts. 314.4(c)(6), 682; PCI-DSS Principal Requirement 3; N.Y. Comp. Codes R. & Regs. tit. 23, § 500.13 (2022).

[52] Although it is not included in Appendix 1, cybersecurity insurance can also be relevant. For example, an IAPP survey of three cybersecurity insurance providers revealed common expectations of best practices, including firewalls, patching, passwords, and authentication, and noted that they may deny coverage if policyholders "do not exercise the degree of caution they promised in the underwriting process." *See* William McGeveran, The Duty of Data Security, 103 Minn. L. Rev. 1135, 1171–72 (2018), https://www.minnesotalawreview.org/wp-content/uploads/2019/02/1McGeveran_FINAL.pdf ("Insurers can and do push their policyholders to adopt practices that reduce the insurer's risk of loss—and simultaneously promote better protection of personal data."); id. at 1173.

[53] In a 2016 report on data breaches, then-California Attorney General Kamala Harris stated as her first recommendation: "[t]he 20 controls in the Center for Internet Security's Critical Security Controls define a minimum level of information security that all organizations that collect or maintain personal information should meet." *See* Kamala D. Harris, Attorney General, California Data Breach Report 30 (2016), https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf. That statement applied to the largest economy in the country, and was made approximately seven years ago. *See also* The White House, Fact Sheet: Act Now to Protect Against Potential Cyberattacks (Mar. 21, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/fact-sheet-act-now-to-protect-against-potential-cyberattacks/ ("we urge companies to execute the following steps with urgency").

[54] White Paper Draft at 23-24.

Data mapping ensures that a company understands the scope of what it must protect and the way it should respond when its security measures have failed to prevent a breach. As Profs. Solove and Hartzog have explained:

> Privacy requirements such as data mapping provide awareness about potential security vulnerabilities. Data mapping shows what data is being collected and maintained, the purposes for having this data, the whereabouts of this data, and other key information.[55]

It is difficult to imagine a company could consider itself "prepared" to respond to a cyber incident if it does not map what data it collects and where it is stored.[56] And yet the reality is that even large companies do not have accurate or comprehensive maps of what data they collect, what limitations apply to that data, who has access to that data, and where and how it is stored.[57] The FTC has brought enforcement actions for deficient data mapping practices since 2019 or earlier.[58] CIS Critical Security Controls v.8 Mapping to NIST Special Publication 800-53 Rev. 5 organizes the various elements of effective data mapping well (see Controls 3.1, 3.2, 3.7, 3.8).[59]

ii. Segmentation of Systems

At first glance segmentation of systems may seem beyond the scope of a single vendor's responsibility, as it pertains to how the customer prevents one compromised system from resulting in a second compromised system (e.g. obtaining access to the system for the HVAC vendor and from

[55] *See* Solove & Hartzog, *supra* note 38 at 156–57.
[56] This is also consistent with NIST and FINRA frameworks. *See* McGeveran, *supra* note 52, at 1183–84 ("The NIST Framework and FINRA's small business self-assessment tool similarly begin with identification of personal data and associated vulnerabilities."); *see also* NIST CSF 1.1 at 24.
[57] *See, e.g.*, Lorenzo Franceschi-Bicchierai, Facebook Doesn't Know What It Does With Your Data, Or Where It Goes: Leaked Document, Vice (Apr. 26, 2022), https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes; Elizabeth Dwoskin, Silicon Valley can't keep track of your data, Washington Post (Sept. 15, 2022), https://www.washingtonpost.com/technology/2022/09/15/mudge-twitter-facebook-data-privacy/.
[58] *See, e.g.*, InfoTrax at ¶ 14; Complaint, Zoom at ¶ 12(g).
[59] *See* CIS v8:NIST SP 800-53-r5 Mapped.

there accessing a system containing consumer credit card information).[60] However, the software itself can function as a gatekeeper and prompt the customer to establish more effective controls between itself and other systems (or within its own sub-systems, as with access controls). We note that the FTC has recommended segmentation of systems as a cybersecurity best practice since at least as early as 2015[61] and that the White House urged companies to implement this practice "now" in June 2021.[62] CISA's Cross-Sector Cybersecurity Performance Goals explicitly require assessing segmentation of systems.[63]

iii. Threat Detection

Although the white paper discusses security logs for analysis after the fact,[64] it is important that software vendors are also able to provide administrators at their customers' organizations with alerts in real time when there is suspicious activity within their systems. Threat detection includes practices such as continuous traffic monitoring, which facilitates early detection of attempts at unauthorized access.[65] The FTC faulted at least eight companies for not persistently monitoring traffic logs between 2015 and 2022,[66] perhaps most notably Equifax.[67] CIS Control 13 addresses this in both detection and protection capacities.[68]

---

[60] *See, e.g.*, Target Hackers Broke in Via HVAC Company, Krebs on Security (Feb. 5, 2014), https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.
[61] *See* Start with Security.
[62] *See* 2021 WH Memo.
[63] CISA CPGs 12 (2.F).
[64] White Paper Draft at 19.
[65] *See, e.g.*, CISA CPGs at 12 (2.G); Cybersecurity Basics at 4 ("Monitor your computers for unauthorized personnel access, devices (like USB drives), and software."; "Check your network for unauthorized users or connections."; "Investigate any unusual activities on your network or by your staff."); 16 C.F.R. § 314.4(c)(8); N.Y. Comp. Codes R. & Regs. Tit. 23, § 500.06 (2022); NIST, Getting Started with the NIST Cybersecurity Framework: A Quickstart Guide (Updated Apr. 19, 2022), https://csrc.nist.gov/Projects/cybersecurity-framework/nist-cybersecurity-framework-a-quick-start-guide ("Maintain and monitor logs"); NIST CSF 1.1 at 36, 38–39. *See also* 2021 WH Memo (urging that companies hunt and block "now").
[66] *See, e.g.*, AshleyMadison at ¶ 35.
[67] *See, e.g.*, Equifax at ¶ 23(A)(iii) and ¶ 23(C)(iii).
[68] *See* CIS v8:NIST SP 800-53-r5 Mapped.

d. The white paper should be framed to support meaningful enforcement.

The white paper draft at numerous points makes it clear that CISA is offering guidance to companies. However, the white paper also makes statements that could support private or regulatory enforcement actions against companies that are overly complacent about cybersecurity. This latter impact is also valuable, especially in the context of shaping market forces and shifting burdens to those best equipped to prevent harm, as articulated in the National Cybersecurity Strategy.

We encourage CISA to consider how it might frame concepts in its white paper in ways that could be useful to litigants and regulators seeking to demonstrate, for example, that a company's cybersecurity practices were negligent. Discussing security as a sub-category of product quality is a step in this direction.[69] So is asking about externalized costs on consumers and not merely on software customers,[70] as it makes it clear that a tech company should be mindful of these points as it creates and maintains its products and services. Recommending using attention-grabbing alerts, including analogizing to vehicle safety alerts, helps to discourage customers from affirmatively diverting from best practice.[71] As another example, widespread availability of security configuration templates could create incentives to use them[72] due to the risks in litigation from failing to take advantage of them.

We encourage CISA to imagine that its recommendations will be implemented widely, to consider how that might impact litigation and other regulatory action, and to frame its recommendations accordingly. For example, it has been well documented by the FTC and by others

[69] White Paper Draft at 26.
[70] RFI at 5(b)(i) https://www.federalregister.gov/documents/2023/12/20/2023-27948/request-for-information-on-shifting-the-balance-of-cybersecurity-risk-principles-and-approaches-for#p-57.
[71] White Paper Draft at 13 (urging that software include indicators when MFA is not enabled or when protocols relying on weak encryption are still active within an application), 16.
[72] Id. at 12 (urging threat modeling to be used to determine which security controls should be on by default), 16 (discussing templates based on risk appetite).

that third party service providers are a popular attack vector for cyber threat actors,[73] including in numerous FTC enforcement actions brought against companies that failed to oversee the data security practices of third parties.[74] The white paper could address oversight of third-party vendors and product integrations in a way that acknowledges this reality. It could offer recommendations that, if adopted, would help courts to distinguish companies that did their best and were truly victims of sophisticated threat actors as opposed to companies whose conduct conveys that they simply did not care about how their deficient practices might impact others. This goal could be achieved by including a discussion in the white paper of what information a company should seek from potential software vendors and what information vendors should proactively provide to potential partners or business customers for assurance that safeguards are not merely implemented but are actively and consistently maintained.[75]

We applaud CISA's efforts to equip companies to improve their cybersecurity practices but encourage the Agency to also consider its recommendations on the broader scale of marketplace incentives and risk management.

---

[73] *See, e.g.*, ABA Cybersecurity Legal Task Force, Vendor Contracting Project: Cybersecurity Checklist Second Edition 1 (2021), https://www.potteranderson.com/media/publication/941_Vendor%20Contracting%20Project%20-%20Cybersecurity%20Checklist.pdf; See also 16 C.F.R. § 314.4(f); 201 Mass. Code Regs. 17.03(2)(f) (2010); McGeveran, *supra* note 52 at 1171 (noting private sector framework of Vendor Security Alliance proposes a standard questionnaire for evaluating the security practices of potential service providers, including questions about access controls and pen-testing); N.Y. Comp. Codes R. & Regs. tit. 23, § 500.11 (2022); CCPA § 1798.81.5(c); FINRA 2015 at 26–30; FINRA 2022 at 6–7; CISA CPGs at 9-10 (1.G, 1.H, 1.I); NIST CSF 1.1 at 28, 39. *See also* Start with Security ("make sure your service providers implement reasonable security measures").

[74] *See, e.g.*, Wyndham at ¶ 24(j); LightYear at ¶ 11(b); AshleyMadison at ¶ 31(d); Lenovo at ¶ 24; Complaint, In re Support King, LLC, FTC File No. 1923003 at ¶ 17(e) (Dec. 21, 2021), https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3003-support-king-llc-spyfonecom-matter; Zoom at ¶ 12(c).

[75] As one example, Verizon has reported in the payment security context that the majority of organizations fail to maintain compliance between annual compliance validations. *See* Verizon, 2022 Payment Security Report 82 (Sept. 2022), https://www.verizon.com/business/resources/T38f/reports/2022-payment-security-report.pdf (Verizon consistently reports that 44 percent or more of organizations fail to maintain PCI- DSS compliance in between annual compliance validations (most recently more than 56 percent failed to maintain compliance).

V. Additional Cybersecurity Considerations for Artificial Intelligence.

CISA asks about necessary security considerations for the development of secure artificial intelligence (AI).[76] Risks includes data leaks, inferences, and harmful secondary uses. Possible solutions include use of synthetic data and utilizing quasi-open models rather than wholly open-source models.

There are numerous examples of data leaks from AI-powered products, including both leaks of PII to users and leaks of user conversations to third parties.[77] Data inferences and combined datasets can produce information that is just as sensitive as PII used in training—or even input data itself—especially where government datasets are combined with commercial datasets. Synthetic data may be a viable method for guarding against adversarial attacks designed to obtain this information.[78]

In terms of harmful secondary uses, especially in the context of open-source models, AI-powered tools can be repurposed for malicious ends.[79] One possible solution here may be to opt instead for quasi-open models—for example, allowing users to adjust model weights without giving users access to the full model.

---

[76] RFI at 12, https://www.federalregister.gov/documents/2023/12/20/2023-27948/request-for-information-on-shifting-the-balance-of-cybersecurity-risk-principles-and-approaches-for#p-82.
[77] Bill Touulas, OpenAI rolls out imperfect fix for ChatGPT data leak flaw, Bleeping Computer (Dec. 21, 2023), https://www.bleepingcomputer.com/news/security/openai-rolls-out-imperfect-fix-for-chatgpt-data-leak-flaw/; Ram Shankar Siva Kumar, A Few Useful Lessons about AI Red Teaming, HAI Seminar (Oct. 18, 2023), https://hai.stanford.edu/events/ram-shankar-siva-kumar-few-useful-lessons-about-ai-red-teaming.
[78] Christian Reimsbach-Kounatze et al., *Emerging Privacy Enhancing Technologies: Current Regulatory & Policy Approaches*, 351 OECD Digit. Econ. Papers 4 (Mar. 2023), https://www.oecd.org/publications/emerging-privacy-enhancing-technologies-bf121be4-en.htm.
[79] Rhiannon Williams, Text-to-image AI models can be tricked into generating disturbing images, MIT Technology Review (Nov. 17, 2023), https://www.technologyreview.com/2023/11/17/1083593/text-to-image-ai-models-can-be-tricked-into-generating-disturbing-images/.

VI. Conclusion

We again applaud CISA for helping to improve the cybersecurity practices of the private sector by offering guidance on reasonable cybersecurity practices and by facilitating incentives to drive better market behavior. We urge CISA to include data minimization, auditing, and other consensus measures in this white paper to strengthen that baseline.

Respectfully submitted, this the 20th of February 2024, by:

Chris Frascella
Counsel
Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036
frascella@epic.org

Sophie Nyombi Nantanda
EPIC Spring Intern

APPENDIX 1- New Baseline Expectations for Data Security: Consensus on Cybersecurity Hygiene for the Modern Threat Environment (Non-Exhaustive List)**

Recommended Data Security Protocol	**Uniform Baseline**
Data Minimization (including retention policies)	• Complaint, In re Drizly, LLC, FTC File No. 2023185 at ¶ 13(f) (Oct. 24, 2022) • Complaint, In re Chegg, Inc., FTC File No. 2023151 at ¶ 9(a) (Oct. 31, 2022) • NIST, Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 34 (Apr. 16, 2018) • CIS Critical Security Controls 3.1, 3.4, 3.5 (Feb. 2023) • Cal. Code Regs. Tit. 11, § 7002 (2023) • N.Y. Gen. Bus. Law, § 899-bb(2)(b)(ii)(C)(4) (2020) • Or. Rev. Stat. tit. 50, § 646A.622(2)(d)(C)(i), (iv) (2021)
Governance (including training and security reviews)	• Complaint, In re Zoom Video Communications, Inc., FTC File No. 1923167 at ¶ 12(a) (Feb. 1, 2021) • Complaint, FTC v. Equifax, Inc., No. 1:2019-cv-03297 at ¶ 23(E) (N.D. Ga. Jul. 22, 2019) • Complaint, In re LightYear Dealer Technologies, LLC, FTC File No. 1723051 at ¶ 11(b) (Sept. 6, 2019) • Complaint, FTC v. Ruby Life Inc. d/b/a AshleyMadison.com, No. 1:16-cv-02438 at ¶ 31(c) (D.D.C. Dec. 14, 2016) • Complaint, In re SkyMed International, Inc., FTC File No. 1923140 at ¶ 12(b) (Jan. 26, 2021) • Complaint, In re Chegg, Inc., FTC File No. 2023151 at ¶ 9(e) (Oct. 31, 2022) • Complaint, In re Uber Technologies, Inc., FTC File No. 1523054 at ¶ 18(b) (Oct. 26, 2018) • NIST Framework v. 1.1 31 (2018) • CISA, Cross-Sector Cybersecurity Performance Goals 1.B, 1.C, 2.I, 2.J (March 2023) • FINRA, Core Cybersecurity Threats and Effective Controls for Small Firms 10 (May 2022) (*included in first tier because it's largely not finance-specific and is designed for small firms*) • CIS CSC 14 (Feb. 2023) • 201 Mass. Code Regs. 17.03(2)(b)(1), 17.04(8) (2010) • N.Y. Gen. Bus. Law, § 899-bb(2)(b)(ii)(A)(4) (2020) • Or. Rev. Stat. tit. 50, § 646A.622(2)(d)(A)(iv) (2021)
Data mapping	• Complaint, In re InfoTrax Systems, L.C., FTC File No. 1623130 at ¶ 14 (Dec. 30, 2019) • Complaint, FTC v. Equifax, Inc., No. 1:2019-cv-03297 at ¶ 22(B) (N.D. Ga. Jul. 22, 2019) • Complaint, In re Zoom Video Communications, Inc., FTC File No. 1923167 at ¶ 12(g) (Feb. 1, 2021) • NIST Framework v. 1.1 24 (2018) • CIS CSC 3.1, 3.2, 3.7, 3.8 (Feb. 2023) • N.Y. Comp. Codes R. & Regs. tit. 23, § 500.3 (2022)

Access Controls	• First Am. Complaint, FTC v. Wyndham Worldwide Corp., 799 F.3d 236 at ¶ 24(e),(f),(j) (3d Cir. 2015) • Complaint, In re Chegg, Inc., FTC File No. 2023151 at ¶ 9(a),(b),(c) (Oct. 31, 2022) • Complaint, In re InfoTrax Systems, L.C., FTC File No. 1623130 at ¶ 10(d) (Dec. 30, 2019) • Complaint, FTC v. Equifax, Inc., No. 1:2019-cv-03297 at ¶ 22(D), 23(C) (N.D. Ga. Jul. 22, 2019) • Complaint, FTC v. Ruby Life Inc. d/b/a AshleyMadison.com, No. 1:16-cv-02438 at ¶ 31(b) (D.D.C. Dec. 14, 2016) • Complaint, In re LightYear Dealer Technologies, LLC, FTC File No. 1723051 at ¶ 11(e) (Sept. 6, 2019) • Complaint, In re SkyMed International, Inc., FTC File No. 1923140 at ¶ 12(c) (Jan. 26, 2021) • Complaint, In re Drizly, LLC, FTC File No. 2023185 at ¶ 13(c) (Oct. 24, 2022) • Complaint, In re Support King, LLC, FTC File No. 1923003 at ¶ 17(b) (Dec. 21, 2021) • Complaint, In re Uber Technologies, Inc., FTC File No. 1523054 at ¶ 18(a)(iii), 24 (Oct. 26, 2018) • Complaint, In re Residual Pumpkin Entity, LLC, d/b/a CafePress, FTC File No. 1923209 at ¶ 11(c), (f), 25 (Jun. 23, 2022) • Complaint, FTC v. D-Link Corp., No. 3:17-CV-00039-JD at ¶ 15(b),(c) (N.D. Cal. Mar. 20, 2017) • Complaint, In re Zoom Video Communications, Inc., FTC File No. 1923167 at ¶ 12(d) (Feb. 1, 2021) • Complaint, In re Paypal, Inc., FTC File No. 1623102 at ¶ 40(c)(1) (May. 24, 2018) • NIST Framework v. 1.1 29, 30 (2018) • CISA, CPGs 2.A, 2.B, 2.C, 2.D, 2.E, 2.H, 2.L, 2.U (March 2023) • FINRA, Core Cybersecurity Threats and Effective Controls for Small Firms 7 (May 2022) • CIS CSC 3.3, 4.7, 5, 6, 12.7, 13.5 (Feb. 2023) • 201 Mass. Code Regs. 17.04(1)(b),(c),(d,3), 17.04(2) (2010) • Or. Rev. Stat. tit. 50, § 646A.622(2)(d)(A)(vii) (2021) • N.Y. Comp. Codes R. & Regs. tit. 23, § 500.07, 500.12 (2022)
Segmentation of Systems	• First Am. Complaint, FTC v. Wyndham Worldwide Corp., 799 F.3d 236 at ¶ 24(a), 28 (3d Cir. 2015) • Complaint, In re Zoom Video Communications, Inc., FTC File No. 1923167 at ¶ 12(e) (Feb. 1, 2021) • Complaint, FTC v. Equifax, Inc., No. 1:2019-cv-03297 at ¶ 22(C)-(D), 23(B) (N.D. Ga. Jul. 22, 2019) • Complaint, In re InfoTrax Systems, L.C., FTC File No. 1623130 at ¶ 10(e) (Dec. 30, 2019) • NIST Framework v. 1.1 30 (2018) • CISA, CPGs 2.F, 2.W, 2.X (March 2023) • CIS CSC 3.12, 4.4, 12, 13 (Feb. 2023)
Vulnerability Management	• First Am. Complaint, FTC v. Wyndham Worldwide Corp., 799 F.3d 236 at ¶ 24(d), 29 (3d Cir. 2015)

(including data retention, end of life protocols, patch management, and pen-testing)	• Complaint, In re Zoom Video Communications, Inc., FTC File No. 1923167 at ¶ 12(b) (Feb. 1, 2021) • Complaint, FTC v. Equifax, Inc., No. 1:2019-cv-03297 at ¶ 22(A), 23(A) (N.D. Ga. Jul. 22, 2019) • Complaint, In re InfoTrax Systems, L.C., FTC File No. 1623130 at ¶ 10(b) (Dec. 30, 2019) • Complaint, In re LightYear Dealer Technologies, LLC, FTC File No. 1723051 at ¶ 10,11(c)-(d) (Sept. 6, 2019) • Complaint, FTC v. Ruby Life Inc. d/b/a AshleyMadison.com, No. 1:16-cv-02438 at ¶ 31(e) (D.D.C. Dec. 14, 2016) • Complaint, In re SkyMed International, Inc., FTC File No. 1923140 at ¶ 12(d) (Jan. 26, 2021) • Complaint, In re Residual Pumpkin Entity, LLC, d/b/a CafePress, FTC File No. 1923209 at ¶ 1(a), (d)-(e), (h) (Jun. 23, 2022) • Complaint, In re Paypal, Inc., FTC File No. 1623102 at ¶ 40(b) (May. 24, 2018) • Complaint, In re Drizly, LLC, FTC File No. 2023185 at ¶ 13(d)-(e) (Oct. 24, 2022) • Complaint, In re Support King, LLC, FTC File No. 1923003 at ¶ 17(c) (Dec. 21, 2021) • Complaint, FTC v. D-Link Corp., No. 3:17-CV-00039-JD at ¶ 15(a) (N.D. Cal. Mar. 20, 2017) • NIST Framework v. 1.1 26, 33, 36, 39, 40, 43 (2018) • CISA, CPGs 1.E (March 2023) • CIS CSC 7, 10, 16, 18 (Feb. 2023) • 201 Mass. Code Regs. 17.03(2)(h),(i), 17.04(6),(7) (2010) • N.Y. Gen. Bus. Law, § 899-bb(2)(b)(ii)(B)(4) (2020) • Or. Rev. Stat. tit. 50, § 646A.622(2)(d)(B) (2021)
Threat Detection	• First Am. Complaint, FTC v. Wyndham Worldwide Corp., 799 F.3d 236 at ¶ 24(h)-(i) (3d Cir. 2015) • Complaint, In re Zoom Video Communications, Inc., FTC File No. 1923167 at ¶ 12(e) (Feb. 1, 2021) • Complaint, FTC v. Equifax, Inc., No. 1:2019-cv-03297 at ¶ 22(F), 23(A)(iii)-(iv), 23(C)(iii) (N.D. Ga. Jul. 22, 2019) • Complaint, In re InfoTrax Systems, L.C., FTC File No. 1623130 at ¶ 10(f), 17 (Dec. 30, 2019) • Complaint, In re LightYear Dealer Technologies, LLC, FTC File No. 1723051 at ¶ 11(d) (Sept. 6, 2019) • Complaint, FTC v. Ruby Life Inc. d/b/a AshleyMadison.com, No. 1:16-cv-02438 at ¶ 35 (D.D.C. Dec. 14, 2016) • Complaint, In re Chegg, Inc., FTC File No. 2023151 at ¶ 9(g) (Oct. 31, 2022) • Complaint, In re SkyMed International, Inc., FTC File No. 1923140 at ¶ 12(f) (Jan. 26, 2021) • NIST Framework v. 1.1 36, 38-39 (2018) • CISA, CPGs 2.G, 2.T, 2.U, 3.A (March 2023) • CIS CSC 8, 9, 10.4, 10.6, 10.7, 13 (Feb. 2023) • 201 Mass. Code Regs. 17.04(4) (2010)

Incident Response	• NIST Framework v. 1.1 35, 41-44 (2018) • CISA, CPGs 2.S, 4.A, 4.B, 4.C, 5.A (March 2023) • CIS CSC 11, 17 (Feb. 2023)
Business Continuity (includes disaster recovery)	• NIST Framework v. 1.1 25, 35, 43-44 (2018) • CISA, CPGs 2.O, 2.P, 2.R, 5.A (March 2023) • CIS CSC 11 (Feb. 2023)

**As we noted in our comments to the Office of the National Cyber Director last year, there are a wealth of existing resources that map parallel requirements across cybersecurity regimes, which should facilitate organizations implementing these consensus measures.[80]

[80] See Comment from EPIC and Consumer Reports, In re: Opportunities for and Obstacles to Harmonizing Cybersecurity Regulations, ONCD-2023-0001-0028 (Oct. 31, 2023), https://www.regulations.gov/comment/ONCD-2023-0001-0028; also available at https://epic.org/documents/in-re-opportunities-for-and-obstacles-to-harmonizing-cybersecurity-regulations-rfi/.