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
OFFICE OF THE NATIONAL CYBER DIRECTOR
Washington, DC 20500

In the Matter of	)	
	)	
Opportunities for and Obstacles to	)	ONCD-2023-0001
Harmonizing Cybersecurity Regulations	)	RIN 0301-AA00

COMMENTS ON REQUEST FOR INFORMATION

by

Electronic Privacy Information Center (EPIC), and Consumer Reports

Submitted October 31, 2023

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

Maria Villegas Bravo
Law Fellow
Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036

Summary

We applaud the important work that the Office of the National Cyber Director (ONCD) is undertaking to ensure that strong and consistent cybersecurity rules apply across all critical infrastructure sectors and to create a harmonized regulatory environment that ensures baseline cybersecurity protections can be implemented and be effective. The security and privacy of personal data is of the utmost concern to American consumers, and too often we have seen sensitive information breached. Companies that hold sensitive data, including biometrics, credentials, financial records, health data, communications data, and location data, face acute cybersecurity risks and should have a clear understanding of their baseline compliance obligations regardless of their industry. Preventing bad actors from harvesting personal data from repositories containing this information is both a cybersecurity and privacy priority, and federal policy must reflect this reality through a set of harmonized, baseline cybersecurity requirements.

We urge ONCD to identify in its report the cybersecurity measures around which there is already consensus or near-consensus across different frameworks. We believe there is already consensus or near-consensus on standards for: data minimization, heightened measures for high-risk activities, governance, data mapping, access controls, segmentation of systems, vulnerability management, threat detection, incident response, and business continuity. We have provided a non-exhaustive list of underlying frameworks supporting these measures in Appendices 1 and 2.

We also urge ONCD to establish a common set of proposed rules that could apply across federal regulatory regimes requiring that:

- Companies should meet the highest standard that applies to them not the least common denominator;
- Third party service providers not directly subject to regulation should be evaluated as a significant attack vector for companies that are directly regulated;
- There must be consequences for false or deficient certifications of compliance; and
- Compliance auditing must be independent and thorough.

Additionally, we encourage ONCD to raise awareness about existing resources that can help companies understand how the cybersecurity requirements they must satisfy under one regime may map onto parallel requirements under another regime.

We also recommend that ONCD consider—in engaging regulatory cybersecurity requirements for critical infrastructure sectors—the impacts of cyber incidents on individual privacy and safety, and to incorporate those considerations into its work carrying out the 2023 National Cybersecurity Strategy.

Table of Contents

Comments

I. Introduction

The Office of the National Cyber Director ("ONCD" or "Director's Office") requested comment on opportunities for and obstacles to harmonizing cybersecurity regulations,[1] per Strategic Objective 1.1 of the National Cybersecurity Strategy.[2] The **Electronic Privacy Information Center (EPIC)** and **Consumer Reports** file these comments to applaud the Director's Office for its prompt action in support of strengthening baseline cybersecurity requirements across critical infrastructure sectors. We support regulations that help businesses operating in critical infrastructure sectors to move away from box-checking compliance exercises and move towards meaningful investments in actual improvements that safeguard consumer data.

EPIC[3] 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 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.

---

[1] Off. of the Nat'l Cyber Dir., Request for Information on Cyber Regulatory Harmonization; Request for Information: Opportunities for and Obstacles To Harmonizing Cybersecurity Regulations, 88 Fed. Reg. 55,694 (Aug. 16, 2023), https://www.federalregister.gov/documents/2023/08/16/2023-17424/request-for-information-on-cyber-regulatory-harmonization-request-for-information-opportunities-for [hereinafter RFI].

[2] The White House, National Cybersecurity Implementation Plan 12 (July 2023), https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf [hereinafter NCIP].

[3] Electronic Privacy Information Center, https://epic.org/.

[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 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/.

Consumer Reports is an independent, nonprofit member association that works side by side with consumers for truth, transparency, and fairness in the marketplace.[7] This includes efforts to raise the bar on cybersecurity practices to safeguard consumer data.[8]

In Section II of these comments, we emphasize the vulnerability of American consumers to unauthorized access to their sensitive information, which they largely have no choice but to entrust to entities working in critical infrastructure sectors. We urge ONCD to strategically reframe its harmonization mandate to consider not merely system integrity and the impact of cyber incidents on businesses, but also data privacy and the impact of incidents on American consumers.

In Section III, we urge the Director's Office to identify broadly-accepted cybersecurity controls and to publish this information promptly, allowing for more discussion where there is greater contention about "best practice," but not delaying in amplifying immediately actionable information wherever possible. We offer suggestions for what ONCD might use as a starting place for such a publication.

Section IV addresses universal non-technical considerations the Director's Office should require regardless of which frameworks are imposed by regulatory agencies, namely: elevating standards rather than undermining them, recognizing third parties as possible attack vectors to reach entities subject to cybersecurity regulation, encouraging enforcement in certification-based regimes, and requiring independent and thorough audits.

Section V identifies specific international regulations, largely as further support for the strategic shift to incorporate consumer privacy harms into ONCD's analysis discussed in Section II and for the publication of consensus measures listed in Section III.

We conclude in Section VI by urging ONCD to raise awareness about existing resources that can help companies understand how the same cybersecurity efforts already seem to be able to satisfy the requirements of multiple different frameworks.

II. ONCD Should Incorporate Consumer Privacy into Its Harmonization Effort as a Strategic Shift That Unlocks Opportunities and Aligns Interests.

ONCD noted in its RFI that it welcomes comments that propose a strategic shift or offer a change in perspective that may unlock hidden opportunities and align stakeholder interests.[9] By incorporating consumer privacy into its strategy for harmonization of cybersecurity regulations in critical infrastructure sectors, the Director's Office can properly contextualize cybersecurity best practices such as data minimization, more effectively mitigate the downstream harms of deficient cybersecurity practices on American consumers, and simultaneously advance the Administration's priorities under pillar three of the National Cybersecurity Strategy.

[7] Consumer Reports, *About Us*, https://www.consumerreports.org/cro/about-us/what-we-do/index.htm.
[8] *See, e.g.*, Comments of Consumer Reports, *In re* Cybersecurity Labeling for Internet of Things, PSHSB Dkt. No. 23-239 (Oct. 6, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/100623134834.
[9] *See* RFI at 55,697, https://www.federalregister.gov/d/2023-17424/p-109.

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:

> viewing 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…[10] 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.[11]

Data minimization, for example, addresses reasonable expectations of consumers (including purpose limitations for use of their data[12]), at the same time it addresses the data security concerns because companies "don't have to protect what [they] don't collect."[13] The FTC has explicitly listed data minimization alongside risk mitigation and data management and retention as a data security best practice.[14] 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 likely be the same regardless of whether they are designated as privacy or security controls,[15] that there is need for close collaboration between privacy and security programs in selecting appropriate controls,[16] 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.[17]

As many as half of U.S. consumers have been affected by data breaches because a company holding their personal information was hacked.[18] That is significantly higher than the global average

---

[10] *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.
[11] Id. at 143.
[12] *See* Section V, *infra*.
[13] 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/.
[14] *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").
[15] *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.
[16] *See* NIST SP 800-53-r5 at 14.
[17] *See* NIST SP 800-53-r5 at ix.
[18] *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.

of just 33 percent of consumers.[19] These data breaches can lead to far reaching harms including account compromise, identity theft,[20] 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 estimated that 85 percent of data breaches were preventable,[21] and more recently the Internet Society has estimated 95 percent of breaches could have been prevented with reasonable safeguards.[22] The Federal Trade Commission (FTC) has brought multiple enforcement actions against companies for failing to implement readily-available low-cost security measures.[23] Despite these realities, earlier this year an IBM study reported that breached organizations were more likely to pass the cost of incidents on to consumers rather than invest in better cybersecurity practices.[24] 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

[19] *See* id.
[20] 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.
[21] *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.
[22] *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.
[23] *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 [hereinafter SkyMed]; Complaint, *In re InfoTrax Systems, L.C.*, FTC File No. 1623130 at ¶ 11 (Dec. 30, 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].
[24] *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.

activities.[25] 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.[26] 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.[27] As NTIA has 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.[28] 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.[29] 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."[30] The cybersecurity status quo is no longer acceptable. If greater protections are not

[25] *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).
[26] *See* id.
[27] *See* id.
[28] *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).
[29] *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%).").
[30] *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, with implications for further-diminished trust.[31]

In its National Cybersecurity Strategy, the Administration identified as its third pillar: "Shape Market Forces to Drive Security and Resilience"[32] including promoting privacy and the security of personal data in order to "make our digital ecosystem more trustworthy."[33] By incorporating privacy considerations into its harmonization effort, the Director's Office will not only address cybersecurity risks and practices more effectively, but also do so in a way that strengthens trust by promoting the privacy and security of consumer data, not merely the integrity of systems.

III. ONCD Should Identify Areas of Near-Consensus While Developing a Two-Tiered Set of Risk-Based Baseline Standards.

Responsive to Questions 4, 8.

The Director's Office asks what government and non-government frameworks map cybersecurity standards and controls to cybersecurity outcomes, and asks how well they work in practice to address disparate requirements.[34] We urge ONCD to first recognize existing consistencies in standards rather than the disparate requirements and to publish this information promptly.[35] There are surely areas in which more harmonization work will be required than others, but such a publication could give businesses a sense for what future regulatory requirements are likely to include at a minimum, so they can begin adopting these practices sooner rather than later. It is critical however that ONCD not end its work at identifying the least common denominator across all

[31] *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/.

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

[33] *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/.

[34] *See* RFI at 55,695, https://www.federalregister.gov/documents/2023/08/16/2023-17424/request-for-information-on-cyber-regulatory-harmonization-request-for-information-opportunities-for#p-53.

[35] Alternatively or additionally, ONCD could publish a list of per se unreasonable practices, as proposed by Melanie Teplinsky at the most recent NIST Information Security and Privacy Advisory Board (ISPAB) meeting, https://csrc.nist.gov/Events/2023/ispab-october-meeting (minutes not yet available as of the time of this writing, but Melanie Teplinsky stated that there is fairly broad industry agreement as to what provisions are so far afield that they should be per se unacceptable and that ISPAB should be able to start a list of these, as a sort of inverse safe harbor), and as proposed by Derek E. Bambauer in *Cybersecurity for Idiots*, 106 Minn. L. Rev. Headnotes 172 (2021), available at https://minnesotalawreview.org/article/cybersecurity-for-idiots/.

regulations and frameworks—some industries require more robust safeguards than others and it would be inappropriate to disregard those particular requirements merely because they do not appear in requirements across all sectors. We address this specific point further in Section IV(a) below.

There is striking similarity across multiple state laws, federal sectoral laws, FTC enforcement actions, and both government and non-government frameworks regarding essential cybersecurity hygiene.[36] Despite these similarities, industry commenters have already begun to advocate for cybersecurity regulations to be paused pending the conclusion of the ONCD's harmonization efforts,[37] regardless of the uncertain duration of fulfilling ONCD's mandate.[38] Consumers should not have to wait for basic cybersecurity protections, and the Director's Office can encourage businesses to act now by publishing what efforts seem to be required under any regime. We believe this will advance the Administration's goals under pillar three of the National Cybersecurity Strategy as well because it will put companies on notice as to the new normal in basic cybersecurity hygiene.[39] In Appendices 1 and 2 we provide a more exhaustive annotation of the underlying frameworks for what commonly-required practices we expect ONCD might include, but offer an overview immediately below.

The ONCD should now take advantage of its harmonization and normalization roles to (re)set expectations with industry as relates to the responsibility to safeguard consumer information

[36] *See, e.g.*, Disrupting Data Abuse *supra* note 5 at 194-197; *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 Section V *infra*, and Appendices 1 and 2. The cyber insurance industry may also present opportunities to inform federal regulatory harmonization. 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.

[37] *See, e.g.*, Comments of T-Mobile, *In re* Review of International Section 214 Authorizations to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks, IB Dkt. No. 23-119 at 23 (Aug. 31, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/10831234137677; Comments of Verizon at 22 (Aug. 31, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/108312266504640; Comments of CTIA at 49 (Aug. 31, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/108311863500689; Reply Comments of CTIA at 6 (Oct. 2, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/10022428126256.

[38] *See* Christian Vasquez, White House grapples with harmonizing thicket of cybersecurity rules, CyberScoop (Sept. 18, 2023), https://cyberscoop.com/cybersecurity-strategy-harmonization-critical-infrastructure/ ("That monumental task is likely to span years — perhaps even administrations.").

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

from unauthorized access, with greater regulatory gravitas than California's Department of Justice did in 2016[40], the FTC did in 2015,[41] and the White House did in 2021.[42]

We begin with data minimization and heightened measures for heightened risk, then discuss programmatic components common across cybersecurity regimes, and finally address technical controls about which there is near-consensus.

a. Data Minimization

Although it is not explicitly addressed in most cybersecurity regulations, data minimization is an accepted fundamental risk-reduction concept in cyber hygiene and information management.[43] 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. Although data minimization principles include data retention considerations,[44] some regimes might

[40] 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.

[41] The FTC has been offering explicit guidance on specific cybersecurity practices since at least as early as 2015. *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"].

[42] The White House, What We Urge You To Do To Protect Against The Threat of Ransomware (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"]. *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") [hereinafter "2022 WH FS"].

[43] *See, e.g.*, FTC ANPR, https://www.federalregister.gov/d/2022-17752/p-88 (The term "data security" in this ANPR refers to breach risk mitigation, data management and retention, data minimization, and breach notification and disclosure practices); NIST SP 800-53-r5 at 72, 270; NIST, Using Risk Management to Improve Privacy in Information Systems (Sept. 11, 2015), https://csrc.nist.gov/CSRC/media/Presentations/Using-Risk-Management-to-Improve-Privacy-in-In-(2)/images-media/day3_research_1035-1125.pdf; Federal Privacy Counsel, Fair Information Practice Principles (FIPPs), https://www.fpc.gov/resources/fipps/; 16 C.F.R. pts. 314.4(c)(6), 682; Payment Card Industry Data Security Standard: Requirements and Testing Procedures, Version 4.0 at 73-101 (Requirement 3) (March 2022), https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf [hereinafter PCI-DSS]. No completion of a webform is required to view PCI-DSS requirements as they relate to CIS requirements, see https://www.cisecurity.org/insights/white-papers/cis-controls-mapping-to-payment-card-industry-pci. *See also* N.Y. Comp. Codes R. & Regs. tit. 23, § 500.13 (2022); NIST, Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (Apr. 16, 2018), at 34 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf [hereinafter "NIST CSF 1.1"].

[44] 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.

address data retention separately as a technical control under vulnerability management, focusing on the secure and timely disposal of data. Additionally, we note that limiting sensitive data access to those circumstances when it is strictly necessary (i.e. purpose limitations[45]) also reduces the likelihood of compromise.

b. Heightened Measures for High-Risk Activities

Companies must be required to exercise additional measures to ensure they implement stronger protections in higher-risk situations.[46] While there will likely be significant variety in the appropriate safeguards to implement here, it seems commonsense that for certain situations, such as remote access or sensitive data processing, greater precautions must be taken, and ONCD should emphasize this. Indeed, we urge ONCD to propose a risk-based, two-tiered framework in its harmonization effort. The first tier would set the baseline that would apply to all critical infrastructure organizations; it would set the floor no lower than what CIS has developed or the FTC has established for all commercial entities. The second tier would impose different requirements dependent upon the types of data and processing contexts in which the risks are greater (thereby implicating the second tier rather than the first tier), but would still constitute a uniform baseline within each respective data and processing situation. ONCD should not be reluctant about flagging any perceived "disharmony" that actually reflects an appropriate risk-based differentiation.

c. Common Programmatic Components

1. Governance

Governance issues includes identifying leadership accountable for implementing the program, conducting security reviews, and providing current employee training (including threat intelligence education). Since 2017 if not earlier, the FTC has repeatedly established the need for a

[45] Purpose limitations on data collection and processing are addressed more robustly by international models, see Section V *infra*, and we strongly urge ONCD to follow their lead.

[46] *See, e.g.*, Karen Scarfone, Security Concerns with Remote Access, https://csrc.nist.gov/CSRC/media/Events/HIPAA-Security-Rule-Implementation-and-Assurance/documents/NIST_Remote_Access.pdf (last visited Oct. 31, 2023); NIST CSF 1.1 at 29; N.Y. Comp. Codes R. & Regs. tit. 23, § 500.12(b) (2022); Kristin Cohen, Location, Health, and Other Sensitive Information: FTC Committed to Fully Enforcing the Law against Illegal Use and Sharing of Highly Sensitive Data FTC Bus. Blog (July 11, 2022), https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal; 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 ("Protect sensitive data") [hereinafter "NIST Quickstart"]; CISA, Cross-Sector Cybersecurity Performance Goals 14 (Goal 2.L) (March 2023), https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf [hereinafter "CISA CPGs"].

written information security plan;[47] this should include a designated leadership role.[48] Security reviews entail assessing the extent to which the organization's program includes all necessary components to improve its security posture (necessary components could be determined by legal or best practice standard, or by expert conducting the review).[49] Employee training strengthens an organization against social engineering attacks such as phishing attempts.[50] While specific training needs are likely to vary greatly, the Director's Office must expect that any regulation would entail some basic employee education in identifying and resisting attempts at cyber intrusion or compromise. The White House urged companies to implement employee education to this effect "with urgency" in 2021.[51] CISA CPG Control 2.I notes that training should be within 10 days of onboarding.[52] CIS Critical Security Controls v.8 Mapping to NIST Special Publication 800-53 Rev. 5 in Control 14 has a clear and thorough articulation of what this might look like, including annual updates (in many circumstances more frequent updates may be prudent).[53] FINRA has also published

[47] *See, e.g.*, SkyMed at ¶ 12a; LightYear at ¶ 11a; AshleyMadison at ¶ 31a; Complaint, *In re* TaxSlayer, LLC, FTC File No. 1623063 at ¶ 15(a) (2017), https://www.ftc.gov/legal-library/browse/cases-proceedings/162-3063-taxslayer-matter [hereinafter TaxSlayer]; Complaint, *In re* Uber Technologies, Inc., FTC File No. 1523054 at ¶ 18(c) (Oct. 26, 2018), https://www.ftc.gov/news-events/news/press-releases/2018/10/federal-trade-commission-gives-final-approval-settlement-uber [hereinafter Uber]; Complaint, *In re* Paypal, Inc., FTC File No. 1623102 at ¶ 40a (May. 24, 2018), https://www.ftc.gov/legal-library/browse/cases-proceedings/162-3102-paypal-inc-matter [hereinafter Venmo].

[48] *See, e.g.*, NIST.SP.800-53r5 at 231 (PM-2). This also appears in cybersecurity insurance applications. *See, e.g.*, IAPP, Sample cyberinsurance applications, https://iapp.org/resources/article/sample-cyberinsurance-applications/ (last visited Oct. 31, 2023) [hereainafter "IAPP Cyberinsurance Samples"].

[49] *See, e.g.*, NIST CSF 1.1 at 26 (ID.GV-3, ID.GV-4); Center for Internet Security (CIS) Critical Security Controls (CSC) Control 14.

[50] *See, e.g.*, Security Tip (ST04-014): Avoiding Social Engineering and Phishing Attacks, CISA (Aug. 25, 2020), https://www.cisa.gov/uscert/ncas/tips/ST04-014; FTC et al., Cybersecurity for Small Business: Cybersecurity Basics 10, https://www.ftc.gov/system/files/attachments/cybersecurity-small-business/cybersecuirty_sb_factsheets_all.pdf [sic] ("Keep in mind that phishing scammers change their tactics often, so make sure you include tips for spotting the latest phishing schemes in your regular training") [hereinafter Cybersecurity Basics]; id. at 11 ("Teach [staff] how to avoid phishing scams and show them some of the common ways attackers can infect computers and devices with malware. Include tips for spotting and protecting against cyber threats in your regular employee trainings and communications."); see also 16 C.F.R. § 314.4(e); 201 Mass. Code Regs. 17.03(2)(b)(1), 17.04(8) (2010), available at https://www.mass.gov/doc/201-cmr-17-standards-for-the-protection-of-personal-information-of-residents-of-the/download; N.Y. Comp. Codes R. & Regs. tit. 23, § 500.10, 500.14 (2022); FINRA, Report on Cybersecurity Practices at 31-32 (Feb 2015), https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf [hereinafter FINRA 2015]; FINRA, Core Cybersecurity Threats and Effective Controls for Small Firms at 10 (May 2022), https://www.finra.org/sites/default/files/2022-05/Core_Cybersecurity_Threats_and_Effective_Controls-Small_Firms.pdf [hereinafter FINRA 2022]; NIST Quickstart ("Train users"); CISA CPGs at 13 (2.I, 2.J); NIST CSF 1.1 at 31.

[51] *See* 2022 WH FS.

[52] *See* CISA CPGs at 13.

[53] Throughout these comments, we refer to CIS CSC v8 requirements through the document that maps them to NIST's SP-800-53-r5 rather than through the primary CIS CSC publication, to avoid citing to a resource that requires the completion of a webform to access. *See* CIS Critical Security Controls v8 Mapping to NIST 800-53 Rev. 5 (Moderate and Low Baselines), https://www.cisecurity.org/insights/white-papers/cis-controls-v8-mapping-to-nist-800-53-rev-5 (last visited Oct. 31, 2023) [hereinafter "CIS v8:NIST SP 800-53-r5 Mapped"].

a brief series of questions to self-assess the effectiveness of an employee training program.[54] Some frameworks require that employee training extend to third parties as well.[55]

2. Data Mapping

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.[56]

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.[57] 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.[58] The FTC has brought enforcement actions for deficient data mapping practices since 2019 or earlier.[59] 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).[60]

d. Near-Consensus Technical Controls

1. Access Controls

Access controls include strong password and user authentication practices. There is general consensus that the principle of least privilege and separation of duties should be utilized.[61] The FTC has brought enforcement actions identifying inadequate access controls as a deficient cybersecurity practice since 2017 if not earlier,[62] and has recommended them since at least as early as 2015.[63]

---

[54] *See* FINRA 2022 at 10.
[55] *See* Section V *infra*.
[56] *See* Solove & Hartzog, *supra* note 10 at 156–57.
[57] This is also consistent with NIST and FINRA frameworks. *See* McGeveran, *supra* note 36, 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.
[58] *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/.
[59] *See, e.g.*, InfoTrax at ¶ 14; Complaint, *In re* Zoom Video Communications, Inc., FTC File No. 1923167 at ¶ 12(g) (Feb. 1, 2021), https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3167-zoom-video-communications-inc-matter [hereinafter Zoom].
[60] *See* CIS v8:NIST SP 800-53-r5 Mapped.
[61] *See, e.g.*, NIST CSF 1.1 at 30 (PR.AC-4, also citing to comparable requirements across other frameworks); FINRA 2022 at 7.
[62] *See* AshleyMadison at ¶ 31b.
[63] *See, e.g.*, Start with Security.

Deficient password practices can include failing to change passwords from manufacturer defaults or using easy-to-guess passwords, failing to adequately protect password databases from attacks by hackers, failing to revoke passwords for ex-employees of service providers, allowing employees to reuse passwords to access multiple services, and failing to monitor unsuccessful login attempts.[64] CISA's framework may be most helpful here, in particular Goals 2.A, 2.B, 2.C, 2.D, and 2.G.[65]

NIST advises that user authentication safeguards should be commensurate with risks not only to the organization but also to the privacy and security of individuals.[66] Deficient authentication practices can include failing to provide security notifications to users when login credentials were changed, failing to require multi-factor authentication, failing to require authentication to access backup databases, and failing to prevent bad actors from using breached authentication data to verify a user.[67] CISA Goal 2.H addresses these threats specifically as they relate to multi-factor authentication (MFA), noting that SMS-based MFA is a least-preferred safeguard.[68] CIS Control 6.6 also requires establishing and maintaining an inventory of authentication and authorization systems.[69] The White House identified MFA as one of the most impactful cybersecurity practices in 2021.[70]

As a second tier requirement: PCI-DSS v. 4 in Requirement 8 requires de-activating accounts within 90 days of inactivity,[71] requiring re-authentication after a user session has been idle for more than 15 minutes,[72] and locking out accounts for a minimum of 30 minutes after not more than 10 login attempts.[73]

---

[64] *See, e.g.*, CafePress at ¶ 11(f); CafePress at ¶ 11(c); Equifax at ¶ 22(D); AshleyMadison at ¶ 31(b)(iii), (b)(i), (b)(vi); First Am. Complaint, FTC v. Wyndham Worldwide Corp., 799 F.3d 236 at ¶¶ 24(e)–(f) (3d Cir. 2015), https://www.ftc.gov/legal-library/browse/cases-proceedings/1023142-x120032-wyndham-worldwide-corporation [hereinafter Wyndham]; Complaint, FTC v. D-Link Corp., No. 3:17-CV-00039-JD at ¶ 15(b),(c) (N.D. Cal. Mar. 20, 2017), https://www.ftc.gov/legal-library/browse/cases-proceedings/132-3157-x170030-d-link [hereinafter D-Link]; Complaint, *In re* Chegg, Inc., FTC File No. 2023151 at ¶¶ 9(b)–(c) (Oct. 31, 2022), https://www.ftc.gov/legal-library/browse/cases-proceedings/chegg.

[65] CSA CPGs at 11-12.

[66] NIST CSF 1.1 at 30 (PR.AC-7, "Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)").

[67] *See, e.g.*, Venmo at ¶ 40(c)(1); Uber at ¶ 18(a)(iii), 24; Zoom at ¶ 12(d); LightYear at ¶ 11(e); CafePress at ¶ 25. *See also* 2022 WH FS ("change passwords across your networks so that previously stolen credentials are useless to malicious actors").

[68] 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.").

[69] *See* CIS v8:NIST SP 800-53-r5 Mapped.

[70] *See* 2021 WH Memo. Other top practices were: endpoint detection and response (which we call threat detection), encryption (which we agree should be required but acknowledge may require additional discussion), and a skilled, empowered security team (which applies to multiple controls).

[71] *See* PCI-DSS at 169.

[72] *See* id. at 170.

[73] *See* id. at 173.

2. Segmentation of Systems

Segmentation of systems (e.g., internal firewalls) can help to limit how much consumer harm results from a single breach by making it difficult for a threat actor infiltrating one part of the company's network to access other parts of the network.[74] The FTC has recommended this since at least as early as 2015;[75] and the White House urged companies to implement this practice "now" in June 2021.[76] As a second tier requirement: PCI-DSS v. 4 in Requirement 1 requires assessing network security controls at least once every six months.[77]

3. Vulnerability Management

Vulnerability management includes end of life protocols for unsupported software, devices, etc.,[78] patch management (including assessing whether a patch was effective),[79] and penetration testing to check their security team's work.[80] Taking precautions against known vulnerabilities, such as prompt installation of security patches and software updates, can reduce the likelihood of breach, preventing unauthorized access in the first place.[81] The FTC has brought enforcement actions against companies failing to do this since 2015.[82]

4. Threat Detection

Threat detection includes practices such as continuous traffic monitoring, which facilitates early detection of attempts at unauthorized access.[83] The FTC faulted at least eight companies for not persistently monitoring traffic logs in 2015-2022,[84] perhaps most notably Equifax.[85] CIS Control 13

[74] *See, e.g.*, Cybersecurity Advisory, NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations (Oct. 5, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a.
[75] *See* Start with Security.
[76] *See* 2021 WH Memo.
[77] *See* PCI-DSS at 49.
[78] *See, e.g.*, Cybersecurity & Infrastructure Security Agency, Understanding Patches and Software Updates (Feb. 23, 2023), https://www.cisa.gov/news-events/news/understanding-patches-and-software-updates.
[79] *See* 2022 WH FS (urging companies to do this "with urgency"); *see also* string cite of FTC cases in note 82 *infra*.
[80] *See* 2021 WH Memo.
[81] *See* McGeveran, *supra* note 36 at 1172–73 (citing to IAPP, sample cyber insurance applications, and noting that all three companies inquire about patching in their risk assessment questionnaires); *see also* Known Exploited Vulnerabilities Catalog, Cybersecurity & Infrastructure Sec. Agency, https://www.cisa.gov/known-exploited-vulnerabilities-catalog (last visited Oct. 31, 2023); NIST Quickstart ("Manage device vulnerabilities"); CISA CPGs at 9 (1.E); NIST CSF 1.1 at 26, 36, 39, 43.
[82] *See, e.g.*, Wyndham at ¶ 24d, 29; CafePress at ¶ 11a,d,e; Equifax at ¶ 22a,23a; D-Link at ¶ 15a; Zoom at ¶ 12b.
[83] *See, e.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 Quickstart ("Maintain and monitor logs"); CISA CPGs at 12 (2.G); NIST CSF 1.1 at 36, 38–39. *See also* 2021 WH Memo (urging that companies hunt and block "now").
[84] *See, e.g.*, AshleyMadison at ¶ 35.
[85] *See, e.g.*, Equifax at ¶ 23(A)(iii) and ¶ 23(C)(iii).

addresses this in both detection and protection capacities.[86] As a second-tier requirement: PCI-DSS v. 4 in Requirement 10 recommends checking logs daily, including holidays.[87]

5. Incident Response

We will keep our comments in this subsection very brief. The White House has recommended doing incident response drills since 2021 if not earlier.[88] Questions about incident response also frequently appear in cybersecurity insurance applications.[89] CISA[90] and NIST[91] have both offered guidance here.

6. Disaster Recovery/Business Continuity

Disaster recovery or business continuity planning prepares an organization to maintain functionality despite an emerging cyber incident (e.g. ransomware attack locking users out). Cybersecurity insurance applications often ask about business continuity planning, for obvious reasons (e.g. the ability to continue to generate revenue, to mitigate legal risk by continuing to fulfill contractual obligations, etc.).[92] The White House has recommended keeping offline backups since at least as early as 2021.[93]

e. More Nuanced Measures

We have not discussed in the above sections device mapping,[94] encryption,[95] or several other common elements of cybersecurity regulations or frameworks. This is not because these are not important controls but rather because they may merit closer inspection to identify "best practices." Indeed, it may be easier to first establish a list of "unacceptably bad" practices in these areas more immediately.[96] We believe the practices outlined above appear with such regularity that they merit

---

[86] *See* CIS v8:NIST SP 800-53-r5 Mapped.
[87] *See* PCI-DSS at 221.
[88] *See* 2021 WH Memo; 2022 WH FS.
[89] *See, e.g.*, IAPP Cyberinsurance Samples *supra* note 48.
[90] *See, e.g.*, Cybersecurity & Infrastructure Security Agency, Incident Response Plan (IRP) Basics, https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf (last visited Oct. 31, 2023).
[91] *See, e.g.*, Paul Chiconski, et al., Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology, NIST Special Publication (SP) 800-61, Rev. 2 (Aug. 2012), https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.
[92] *See, e.g.*, IAPP Cyberinsurance Samples.
[93] *See* 2022 WH FS.
[94] *See, e.g.*, Wyndham at ¶ 24g, 27; LightYear at ¶ 11g.
[95] Lack of adequate encryption and related safeguards is probably the most-frequently occurring deficiency in FTC data security-related enforcement actions. *See, e.g.*, Fed. Trade Comm'n, Closing Letter to Dana Rosenfeld, Counsel for Verizon Communications, Inc. at 1 (Nov. 12, 2014), https://www.ftc.gov/legal-library/browse/cases-proceedings/closing-letters/verizon-communications-inc ("our investigation examined the fact that Verizon regularly shipped routers to consumers with the default security set to an outdated encryption standard"); Complaint, *In re* Support King, LLC, FTC File No. 1923003 at ¶ 17a, 17d (Dec. 21, 2021), https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3003-support-king-llc-spyfonecom-matter [hereinafter SpyFone]; Uber at ¶ 18d; Lenovo at ¶ 21; AshleyMadison at ¶ 31(b)(v), 33; D-Link at ¶ 15b, 15c; Equifax at ¶ 22D, 22E, 23(C)(i), 23D; LightYear at ¶ 8, 11f; InfoTrax at ¶ 10g; SkyMed at ¶ 12c, 13; CafePress at ¶ 11b; Wyndham at ¶ 24b, 31. In June 2021, the White House included encryption among its most impactful cybersecurity practices all companies should be implementing "now." 2021 WH Memo.
[96] *See, e.g.*, Bambauer *supra* note 35.

immediate action by the Director's Office. We address what we believe are commonsense non-regulation-specific measures in Section IV immediately below.

IV. ONCD Should Ensure That Harmonization of Regulations Incorporates Key Non-Technical Considerations Meriting Special Attention.

Regardless of which set(s) of cybersecurity requirements a regulated entity may be subject to, the Director's Office should take the opportunity presented through its harmonization role to establish guidance and guardrails on issues that will be relevant in any regulatory regime or combination of regimes, such as elevation rather than elimination of standards, risks presented by third party service providers, certifications of compliance, and auditing.

a. Regulatory Reciprocity Should Elevate Standards Not Undermine Them.

Responsive to Question 10.

Although we encourage ONCD to expediently identify those areas of regulatory consensus or near-consensus on best practices in basic cybersecurity for critical infrastructure sectors, it is important that the Director's Office not convey directly or indirectly that its harmonization effort is tantamount to attempting to reduce a company's compliance with cybersecurity requirements to only those which appear across all applicable regulatory regimes (i.e. the entirety of the Venn diagram should not be replaced by the overlap in the center of the diagram). Thus far, ONCD has been clear that sector regulators can go beyond the baseline to address cybersecurity risks specific to their sectors[97]—we encourage the Director's Office to maintain this position. Where a less demanding standard in one regulation is entirely subsumed within a more demanding standard in another regulation, it makes sense that a business should be able to demonstrate compliance with the lesser standard through its compliance with the greater standard; however, unless the lesser standard is updated to match the more stringent requirements of the greater standard, it would be inappropriate and counterproductive for a company to assert its compliance with the lesser standard as satisfying compliance with the greater standard. As the Director's Office has implied, inadequate and inconsistent outcomes will not advance the goals of the National Cybersecurity Strategy.[98]

The stated purpose of this RFI is to "understand existing challenges with regulatory overlap, and explore a framework for reciprocity."[99] This harmonization effort should make it easier for companies to demonstrate their compliance with requirements across regulatory regimes, but not eliminate practices essential to effective data security and data privacy. As one hypothetical example, the Safeguards Rule[100] under the Gramm-Leach-Bliley Act (GLBA) doesn't explicitly require segmentation of systems,[101] but CISA's Cross-Sector Cybersecurity Performance Goals (CGPs)[102] does. An entity subject to both regimes should still be required to certify appropriate use of measures such as internal firewalls.

---

[97] *See* RFI at 55,694, https://www.federalregister.gov/d/2023-17424/p-11.
[98] *See* id., https://www.federalregister.gov/d/2023-17424/p-7.
[99] Id., https://www.federalregister.gov/d/2023-17424/p-3; per Implementation Plan initiative 1.1.1. *See* NCIP.
[100] *See* 16 C.F.R. § 314.
[101] *See* FTC Safeguards Rule: What Your Business Needs to Know, FTC, https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know (last visited Oct. 31, 2023).
[102] CISA CPGs 12 (2.F).

b. Regulated Entities Must Guard Against Incidents Originating from Access by Third Parties, Even if the Third Party is Not Directly Regulated**.**

Responsive to Questions 7, 10.

The Director's Office should facilitate normalization of oversight of third parties, even where a given cybersecurity regulation may not explicitly require it. This is significant because it pertains to entities not subject to a given regulation. It has been well-documented by the Federal Trade Commission (FTC) and by others that third party service providers are a popular attack vector for cyber threat actors,[103] including numerous enforcement actions under its Section 5 authority against companies failing to oversee the data security practices of third parties.[104] Additionally, under both COPPA[105] and GLBA,[106] the FTC imposed an expectation that companies will use reasonable means to confirm that service providers or third parties with access to data not merely implement but actively maintain adequate safeguards to ensure the confidentiality and security of consumer information. "The Commission views the regular assessment of the security risk of service providers as an important part of maintaining the strength of a financial institution's safeguards."[107]

We trust that regulators will implement sensible cybersecurity requirements that will include regulations regarding third parties and other service providers with access to a regulated entity's systems and data. However, we expect that entities in critical infrastructure sectors should be as or more attentive to the third parties that they work with than the commercial entities regulated by the

---

[103] *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; 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/. See also 16 C.F.R. § 314.4(f); 201 Mass. Code Regs. 17.03(2)(f) (2010); McGeveran, *supra* note 36 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").

[104] *See, e.g.*, Wyndham at ¶ 24(j); LightYear at ¶ 11(b); AshleyMadison at ¶ 31(d); Lenovo at ¶ 24; SpyFone at ¶ 17(e); Zoom at ¶ 12(c).

[105] *See* Complying with COPPA: Frequently Asked Questions, FTC L(1), https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions (last visited Oct. 31, 2023) (referring to § 312.8).

[106] *See* Standards for Safeguarding Customer Information, 16 C.F.R. § 314 (2021), https://www.federalregister.gov/documents/2021/12/09/2021-25736/standards-for-safeguarding-customer-information (citing to 16 CFR 314.4(d)). In terms of enforcement actions, *see, e.g.*, Complaint, *In re* Ascension Data & Analytics, LLC, FTC File No. 1923126 at ¶¶ 13, 14–17, 20 (2021), https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3126-ascension-data-analytics-llc-matter; TaxSlayer at ¶ 14(d).

[107] Standards for Safeguarding Customer Information, 16 C.F.R. § 314 (2021), (citing Kevin McCoy, Target to Pay $18.5M for 2013 Data Breach that Affected 41 Million Consumers, USA Today (May 23, 2017), https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/) ("For example, in 2013, attackers were reportedly able to use stolen credentials obtained from a third-party service provider to access a customer service database maintained by national retailer Target Corporation, resulting in the theft of information relating to 41 million customer payment card accounts.").

FTC. We explore additional precautions regarding third parties in our discussion of international frameworks below.[108]

c. Certification-Based Cybersecurity Regimes Require Enforcement**.**
Responsive to Questions 2(h), 6(k).

We urge ONCD to direct regulators to put a robust enforcement process in place, especially if the regulator is going to accept self-certification of compliance with cybersecurity requirements from regulated entities. At least one agency has already proposed accepting self-certifications as sufficient evidence of compliance with its regulatory regime.[109] Unfortunately, false or deficient certifications about privacy and cybersecurity compliance are a known issue. The Department of Justice has set up an entire initiative to address this issue with regard to federal contractors.[110] Verizon has reported in the payment security context that the majority of organizations fail to maintain compliance between annual compliance validations.[111] Again, independently of whatever practices a regulator may require of a company, ONCD should direct regulatory agencies to dedicate resources to investigating false or deficient assertions of compliance and bringing enforcement actions where appropriate.

d. Audits Must Be Adequately Independent and Thorough**.**
Responsive to Question 6(l).

For the same reason that it is important to ensure that self-certifications of compliance are adequate and accurate, audits measuring compliance must be both independent and thorough. As one example, an audit should not merely report the audit subject's response as to whether the 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.[112] 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

[108] *See* Section V *infra*.
[109] *See, e.g.*, *In re* Review of International Section 214 Authorizations to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks, Order and Notice of Proposed Rulemaking, IB Docket No. 23-119 at ¶ 4, 122 (Rel. Apr. 25, 2023), *available at* https://www.fcc.gov/ecfs/search/search-filings/filing/104251437004710.
[110] *See, e.g.*, Press Release, Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative (Oct. 6, 2021), https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative; Madison Alder, Verizon agrees to settle False Claims allegations over cyber standards for federal contractors, FedScoop, (Sept. 5, 2023), https://fedscoop.com/verizon-to-settle-cyber-false-claims-allegations/.
[111] *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).
[112] *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.

> 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."[113]

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."[114] We urge the Director's Office to encourage regulators to establish quantitative goals and standards for audits, requiring actual investigation and analysis and not merely interviews.[115] We also encourage ONCD 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 to the Director's Office as relates to the independence of cybersecurity audits.[116]

V. International Frameworks Underscore that ONCD's Strategy Should Incorporate Consumer Privacy as well as Points of Near-Consensus.

Responsive to Question 9.

ONCD also asks about international regulatory regimes.[117] Most international digital laws focus on data privacy and data protection, which further underscores our exhortation that ONCD incorporate consumer privacy concerns in its harmonization and normalization efforts.[118] Most notably, these include strict purpose limitations on data collection under GDPR, the European Commission's proposed Cyber Resilience Act, and ISO/IEC 27001:2022.[119] Governments and international organizations are also beginning to issue guidance on cybersecurity practices. These are outlined in greater detail in Appendix 2, but briefly we will note here that they include the GDPR[120] and the proposed Cyber Resilience Act[121] in Europe, China's Personal Information Security Specification,[122] the Monetary Authority of Singapore's Technology Risk and Management

---

[113] 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.

[114] Id.

[115] 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.*, 2021 WH Memo at 2.

[116] *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).

[117] *See* RFI at 55,697, https://www.federalregister.gov/d/2023-17424/p-93.

[118] *See* Section II *supra*.

[119] *See* Appendix 2 for full citations and additional information.

[120] General Data Protection Regulation No. 2016/679, 2016 O.J. (L 119).

[121] Cyber Resilience Act, Eur. Parl. Doc. (COM(2022) 454 final). *See also* Amy Chang, *Cybersecurity Score – European Union (EU) Cyber Resilience Act*, Explainers, Cybersecurity Policy RStreet (Oct. 27 2023), https://www.rstreet.org/research/cybersecurity-score-european-union-eu-cyber-resilience-act/.

[122] Info. Sec. Tech. – Pers. Info. Sec. Specification (promulgated by State Admin. for Mkt. Supervision of the People's Republic of China & Standardization Admin. of the People's Republic of China, Mar. 06, 2020,

Guidelines,[123] and ISO/IEC 27001.[124] We further note that these include training for third parties like vendors,[125] assessing third parties' security practices,[126] and monitoring third party access to information commensurate with the risk of the transaction.[127]

VI. ONCD Should Raise Awareness of Existing Resources That Map Requirements.

Responsive to Question 4.

There are numerous resources already available that identify parallel requirements across cybersecurity regimes. These include but are not limited to:[128]

- NIST SP-800-53-r5, Security and Privacy Controls for Information Systems and Organizations, catalogs security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, outlining parallel requirements between itself and the 2002 edition of ISO/IEC 27001;[129]
- NIST CSF v. 1.1, Framework for Improving Critical Infrastructure Cybersecurity, enables organizations in critical infrastructure and in other sectors to apply principles and best practices of risk management to improving security and resilience, outlining parallel requirements between NIST CSF v.1.1 with CIS CSC, COBIT 5, ISA 62443-2-1:2009, ISO/IEC 27001:2013, and NIST SP 800-53 Rev. 4;[130]
- CISA, Cross-Sector Cybersecurity Performance Goals (CPGs), providing clearly-defined IT and OT protections to organizations seeking to drive down cybersecurity risk and written to be easy to communicate with senior business leadership, outlining parallel requirements between CPGs and NIST CSF;[131]
- CIS, Critical Security Controls v8 Mapping to NIST CSF, a mapping document for organizations defending assets in cyberspace, outlining parallel requirements between CIS Controls version 8 and NIST CSF,[132] there are maps to other regimes as well;[133]

---

effective Oct. 01, 2020) Nat'l Info. Sec. Standardization Tech. Comm. Sept. 20, 2020 https://www.tc260.org.cn/front/postDetail.html (Hereafter GB/T 35273—2020).

[123] Tech. Risk Mgmt. Guidelines (promulgated by the Monetary Authority of Singapore, Jan. 2021, effective Jan. 2021) Monetary Authority of Singapore, Jan 18. 2021 https://www.mas.gov.sg/regulation/guidelines/technology-risk-management-guidelines (Hereinafter TRMG) .

[124] ISO/IEC 27001:2022 https://www.iso.org/standard/27001.

[125] *See, e.g.*, ISO/IEC 27001:2022 A.6.3; TRMG 3.6.2.

[126] *See, e.g.*, TRMG 3.4.2, 5.3, 6.4, 14.1-14.2; GB/T 35273—2020 9.2.

[127] *See, e.g.*, GB/T 35273—2020 9.7; TRMG 3.4, 6.4.3.

[128] While some of these resources refer to older versions of frameworks, this can be a matter of reorganizing practices into a more logical or consistent structure (e.g. CISA restructuring its CPGs to align more closely with NIST's framework), rather than changes in underlying practices required or recommended by the framework. *See, e.g.*, CISA CGPs *supra* note 46 at 7.

[129] *See* NIST SP 800-53-r5 *supra* note 15.

[130] *See* NIST CSF 1.1 *supra* note 43 (comparing NIST's CIS CSC, CSF v.1.1 with COBIT 5, ISA 62443-2-1:2009, ISO/IEC 27001:2013, NIST SP 800-53 Rev. 4.).

[131] *See* CISA CPGs.

[132] *See* CIS v8:NIST SP 800-53-r5 Mapped *supra* note 53.

[133] *See* CIS Critical Security Controls Version 8, https://www.cisecurity.org/controls/v8 (last visited Oct. 31, 2023), and a tool provided here: https://www.cisecurity.org/controls/cis-controls-navigator.

- the California Department of Justice, California Data Breach Report, Appendix B: The Critical Security Controls Master Mapping (Excerpt), a call to action for organizations, individuals, and regulators, to work toward a safer and more secure online future, outlining parallel requirements between CIS v. 6, NIST 800-53 Rev. 4, NIST CSF, ISO 27002: 2013, HIPAA, FFIEC Examiners Handbook, PCI-DSS 3.0.[134]

Source	NIST	ISO 27001	CIS	PCI-DSS	Other
NIST SP 800-53 rev. 5 (mapping updated July 2023)		2022			COBIT 5; ISA 62443-2-1:2009
NIST CSF v1.1 (v2.0 forthcoming)	SP 800-53-r4	2013	v6		
CISA CPGs (updated March 2023)	CSF v.1.1				
CIS v8 mapping	CSF v1.1; SP 800-53-r5 (Moderate and Low Baselines); SP 800-171-r2	2022 (also ISO 27002: 2022)	n/a	4.0	ISACA COBIT 19; CISA CPGs (2022); more[135]
Cal. Data Breach Report (CIS v6 mapping)	CSF v1.1; SP 800-53-r4	2013	n/a	3.0	HIPAA; FFIEC

The Director's Office should take advantage of its harmonization and normalization roles to raise awareness of already-existing resources by which regulated entities may streamline their cybersecurity practices and compliance reporting.

VII. Conclusion

We again applaud the Director's Office for its prompt action in advancing consumer protections, public safety, and national security by facilitating improved cybersecurity practices through this process.

[134] *See* Kamala D. Harris, Attorney General, California Data Breach Report at App'x B (2016), https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf.
[135] *See* resources cited in note 133, *supra*.

Respectfully submitted, this the 31st of October 2023, by:

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

Maria Villegas Bravo
Law Fellow
Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036
villegasbravo@epic.org

Justin Brookman
Dir., Technology Policy
Consumer Reports
101 Truman Ave
Yonkers, NY 10703

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

Recommended Data Security Protocol	**First Tier/Uniform Baseline** *(applies to all organizations)*	**Second Tier/Differentiated by Data, Processing Risks** *(e.g. specific to financial, health, etc.)*
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)	• 16 C.F.R. §§ 312.10, 314.4(c)(6), 682 • 45 C.F.R. § 164.502(b) • FFIEC Cybersecurity Assessment Tool ver. 1.1 App'x A p. 22 (May 2017) • Payment Card Industry Data Security Standard: Requirements and Testing Procedures v4, Principal Requirement 3 (March 2022) • N.Y. Comp. Codes R. & Regs. tit. 23, § 500.13 (2022)
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)	• 16 C.F.R. § 314.4(e) • 45 C.F.R. § 164.308 • FFIEC App'x A p. 1-6, 10-12 (2017) • PCI-DSS Principal Requirement 5, 6, 9, 12 (March 2022) • FINRA, Report on Cybersecurity Practices 31-32 (Feb 2015) • N.Y. Comp. Codes R. & Regs. tit. 23, §§ 500.3, 500.4, 500.8, 500.10, 500.14 (2022)

	• 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)	• FFIEC App'x A p. 5-6, 28-29 (2017) • PCI-DSS Principal Requirement 1 (March 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)	• FTC Safeguards Rule: What Your Business Needs to Know, FTC, https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know (last visited Oct. 31, 2023) (citing to 314.4(c)(1), (c)(5) of Safeguards Rule) • Final Rule, FTC, Standards for Safeguarding Customer Information, 86 Fed. Reg. 70286 (Dec. 9, 2021) (noting that "[s]uch overbroad access could create additional harm in the event of an intruder gaining access to a system by impersonating an employee or service

	• 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)	provider") • 45 C.F.R. § 164.308, 164.312 • FFIEC App'x A p. 9, 16-22, 26 (2017) • PCI-DSS Principal Requirement 2, 7, 8 (March 2022) • FINRA, Report on Cybersecurity Practices 17-20 (2015) • N.Y. Comp. Codes R. & Regs. tit. 23, §§ 500.7, 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)	• 45 C.F.R. § 164.308(a)(4)(ii)(A) • FFIEC App'x A 8, 16, 17, 20 (2017)

	• 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)	• PCI-DSS v4 Principal Requirement 1, 10 (March 2022)
Vulnerability Management (including data retention, end of life protocols, patch management, and pen-testing)	• First Am. Complaint, FTC v. Wyndham Worldwide Corp., 799 F.3d 236 at ¶ 24(d), 29 (3d Cir. 2015) • 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)	• 16 C.F.R. pts. 314.4(b)(2), 314.4(d), 314.4(g) • 45 C.F.R. § 164.308(a)(5) • FFIEC App'x A p. 6, 8-10, 13, 23-28 (2017) • PCI-DSS Principal Requirement 5,6,10,11 (March 2022) • FINRA, Report on Cybersecurity Practices 21-22 (2015) • N.Y. Comp. Codes R. & Regs. tit. 23, § 500.5 (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)	• 16 C.F.R. § 314.4(c)(8) • 45 C.F.R. § 164.308(a)(1)(ii)(D) • FFIEC App'x A p. 9, 13, 16, 25-26 (2017) • PCI-DSS Principal Requirement 10 (March 2022) • N.Y. Comp. Codes R. & Regs. tit. 23, § 500.6 (2022)

	• 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)	• 45 C.F.R. § 164.308(a)(6),(a)(7) • FFIEC App'x A p. 4, 14-15, 32-37 (2017) • PCI-DSS Principal Requirement 12.10 (March 2022) • N.Y. Comp. Codes R. & Regs. Tit. 23, § 500.16 (2022)
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)	• 45 C.F.R. § 164.308(a)(7) • FFIEC App'x A 7, 16, 25-26, 33-34 (2017) • PCI-DSS Principal Requirement 12.10 (March 2022)

APPENDIX 2- Baseline Requirements Mirrored in International Regulations (Non-Exhaustive List)

Recommended Data Security Protocol	**First Tier/Uniform Baseline**	**Second Tier/Differentiated by Data, Processing Risks**
Data Minimization (including retention policies)	• Articles 5(1)(c), 25, 89(1), Recital 156 General Data Protection Regulation No. 2016/679, 2016 O.J. (L 119) (Hereinafter GDPR) • Info. Sec. Tech. – Pers. Info. Sec. Specification (promulgated by State Admin. for Mkt. Supervision of the People's Republic of China & Standardization Admin. of the People's Republic of China, Mar. 06, 2020, effective Oct. 01, 2020) Nat'l Info. Sec. Standardization Tech. Comm. Sept. 20, 2020 at 4.D, 5.2 https://www.tc260.org.cn/front/postDetail.html (Hereafter GB/T 35273—2020) • Cyber Resilience Act, Eur. Parl. Doc. (COM(2022) 454 final) A.1.1.3e	
Governance (including training and security reviews)	• ISO/IEC 27001:2022 6.1.2(b-c), 6.1.4, 7.2.b, 9.2.1-9.2.3SSDF PW.1.2, PW.7.2, PW.8.2, PW.1.1, RV.3.1, • Cyber Resilience Act, Eur. Parl. Doc. (COM(2022) 454 final) 10.1-10.15, Annex 1 2.3 • GB/T 35273—2020 11.4, 11.6, 11.7 • NIST, *Secure Software development Framework (SSDF) Version 1.1* Natl. Inst. Stand. Tech. Spec. Publ. 800-218, PO.2.2 (2022) (Hereinafter SSDF) • Article 32, Recital 83 GDPR	• Tech. Risk Mngmt. Guidelines (promulgated by the Monetary Authority of Singapore, Jan. 2021, effective Jan. 2021) Monetary Authority of Singapore, Jan 18. 2021 at 3.1.2, 3.5.1, 3.6, 4.1-4.5.3, 5.7, 12.1-12.2, 13.1-13.3, 15.1 https://www.mas.gov.sg/regulation/guidelines/technology-risk-management-guidelines (Hereinafter TRMG)
Data mapping	• ISO/IEC 27001:2022 A.5.9, A.5.10, A.5.13, A.8.9	• TRMG 7.2

	• Article 30 GDPR	
Access Controls	• ISO/IEC 27001:2022 A.7.1-A.7.14 • ISO/IEC 27001:2022 A.8.1-A.8.34 • ISO/IEC 27001: A.5.18, A.6.1-A.6.8, A.8.1-A.8.5 • SSDF PS.1.1	• TRMG 9.1-9.3
Segmentation of Systems	• ISO/IEC 27001:2022 A.5.3, A.8.22, A.8.27 • SSDF PO.5.1	• TRMG 5.7.3, 7.6
Vulnerability Management (including data retention, end of life protocols, patch management, and pen-testing)	• ISO/IEC 27001:2022 7.5.3(f), A.8.10 • GB/T 35273—2020 4.D, 5.2, 6.1 • ISO/IEC 27001:2022 A.8.5, A8.20, A.8.24 • GB/T 35273—2020 6.3 • Article 32(1) GDPR	• TRMG 10.1-10.2
Threat Detection	• ISO/IEC 27001:2022 9.1.a, A.5.22, A.7.1-7.14, A.8.16 • SSDF PO.4.1 • GB/T 35273—2020 11.3 • Cyber Resilience Act, Eur. Parl. Doc. (COM(2022) 454 final) A.1.1.3.j	
Incident Response	• GB/T 35273—2020 10.1 • ISO/IEC 27001:2022 10.2, A.5.24- A.5.29, A.6.8 • Cyber Resilience Act, Eur. Parl. Doc. (COM(2022) 454 final) 10.2 • SSDF RV.1.1-RV3.4 • Articles 33, 34, Recitals 85-88 GDPR	• TRMG 7.7-7.8
Business Continuity (includes disaster recovery)	• ISO/IEC 27001:2022 10.2, A.5.26- A.5.34	• TRMG 8.1-8.5
Heightened measures for high-risk activity (e.g. third party	• GB/T 35273—2020 9.2, 9.7, 9.8 • GB/T 35273—2020 6.3, 9.2	• TRMG 3.4.2, 5.3, 6.4, 7.5, 11.4, 14.1-14.2

integrations and processing sensitive data like biometric data)	• Cyber Resilience Act, Eur. Parl. Doc. (COM(2022) 454 final) 8 • Article 9, Recitals 51-56 GDPR	• Artificial Intelligence Act, Eur. Parl. Doc. (COM/2021/206 final) 15.4