A Zero Cost Path to American Cybersecurity

INTERNET SECURITY ALLIANCE RECOMMENDATIONS

TO WHITE HOUSE OFFICE OF THE NATIONAL CYBER DIRECTOR

AUGUST 2025

TABLE OF CONTENTS

Executive Summary

The Internet Security Alliance's Board of Directors (see attached list), comprised of the nation's leading cybersecurity professionals representing nearly every critical industry sector, believes the new Director of ONCD comes to office at a critical time in our nation's history. Estimates are that we are experiencing up to 600 million cyber-attacks a day[1]. The economic damage of these attacks is in the trillions of dollars annually[2], and adversarial nation states have already successfully compromised elements of our telecommunications and energy critical infrastructures[3].

President Trump has made it clear that "foreign nations and criminals continue to conduct cyber campaigns targeting the United States... disrupting the delivery of critical services… cost billions of dollars, and undermine Americans' security and privacy" — and that "more must be done to improve the Nation's cybersecurity against these threats."[4]

This paper outlines five priority initiatives that operationalize the President's philosophy of government, which create a zero-cost pathway for /American cybersecurity. These are pragmatic programs that can be implemented quickly. They will generate significant material improvements in our nation's cybersecurity almost immediately. These steps will also put our nation's intermediate and long-term security on a measurably effective and economically sustainable path that will enable us to address newly growing threats of systemic failure.

Most importantly, implementing these priorities will cost the federal government virtually nothing*. Indeed, the modest start-up costs associated with some of these priorities will be more than offset by the savings they will quickly create. On balance, implementing the proposed projects will not only materially improve our nation's security, both immediately and in the long term, but will save the federal government billions of dollars in the process.*

As a bonus, the private sector will also save billions of dollars currently being wasted on unproven requirements. This money can be channeled into greater investment and innovation, which will generate increased economic growth and enhanced cybersecurity.

The Administration's leadership, combined with the National Cyber Director's coordinating authority, can integrate executive action, legislative priorities, and analytical tools into a single, coherent strategy. The Director's experience at the Millennium Challenge Corporation — where cost-benefit analysis guided every investment — reflects exactly the disciplined approach needed now.

The first step in this effort is eliminating the enormous wasteful duplication in current federal cybersecurity regulations, flagged by GAO[5] and others as a problem. President Trump's Executive Orders[6], as well as statute[7], clearly give OMB power to act quickly to rectify this situation. An April 2025 letter from Chairman Comer and Green, as well as other prominent Members, to Director Vought[8] urged OMB to *"act now"* because "eliminating the duplicative landscape of cyber regulations is the fastest, most cost-effective way to improve the nation's cybersecurity materially."

ISA's AI-driven analysis has pinpointed duplication in 76% of cyber regulations[9], and eliminating just the redundancies would cut the number of core regulations by about 75%, generating tens of billions of dollars in savings for the government and industry.

Building on that momentum, the Administration can advance complementary measures that lock in long-term gains by:

- Establishing a cost-benefit analysis requirement for future cyber rules
- Reauthorizing and modernizing the 2015 CISA Act before its September 30, 2025, expiration to address systemic risks from concentrated market dependencies and ensure the framework keeps pace with today's threat environment
- Passing the PIVOTT Act (already out of the House Homeland Security Committee), which would provide an adequately trained government cybersecurity workforce while closing the larger gap on a cost-neutral basis
- Creating the first macroeconomic model of cyber risk, allowing the government to measure risk generated by emerging technologies such as AI and Quantum, and empirically evaluate reforms for maximum security impact and economic return

By acting now, the Administration can fulfill the President's call to strengthen America's cyber defenses and set a lasting legacy of a leaner, stronger, and more resilient cybersecurity posture.

This program will position the National Cyber Director as the nation's offensive coordinator, integrating the intelligence, industry alignment, and operational support needed to execute President Trump's vision — uniting executive action, legislative reform, and industry partnership through a data-driven strategy to reshape the nation's cybersecurity for the next decade.

Introduction: Using Deregulation to Strengthen National Security

President Trump has made deregulation a central pillar of his national security and economic growth strategy[10], emphasizing the removal of outdated and duplicative regulations that slow innovation and weaken U.S. competitiveness. The Administration's approach focuses on eliminating rules that create unnecessary burden without corresponding benefit to security or economic growth.

This same approach can be the breakthrough the nation needs in cybersecurity. Today, America's critical infrastructure operates under a maze of overlapping and conflicting cyber mandates that divert billions from real defenses, consume scarce expert talent, and, ironically, have never been documented as enhancing our nation’s security..

PRIORITY ONE: OMB Should Use Existing Authority to Remove Duplicative Cybersecurity Regulations

Why This Must Be Done Now

Perhaps no issue in the cybersecurity field enjoys greater consensus than the problem of massive regulatory duplication.

Multiple government, industry, academic, and international studies have all documented the massive degree of wasted resources (between 40-78% depending on sector) generated by the senseless duplication of regulatory compliance regimes[11].

Even the pro-regulatory Biden Administration identified the elimination of cybersecurity regulatory redundancy as priority 1.1 in its own national cybersecurity implementation plan[12], with Ann Neuberger asserting that the regulatory duplication was a government-created problem, and it was up to the government to resolve it[13].

Unfortunately, the Biden Administration failed to take substantive action, leaving it to the Trump Administration and the current Congress to address this "government-created problem." Fortunately, initial directives from the White House and the Cybersecurity leadership in Congress have indicated an awareness of the need to address this issue. ONCD should make following through on these initial steps and actually eliminating cyber regulatory duplication a top priority.

In April 2025, House Oversight Chair James Comer, House Homeland Security Chair Mark Green and other prominent Members articulated how, under current authority and bolstered by President Trump's Executive Orders, OMB has the authority to "act now" to remove duplicative and conflicting cyber regulations, warning that compliance burdens are undermining the agility of U.S. companies to respond to threats. Their letter concludes that "eliminating the duplicative landscape of cyber regulations is the fastest, most cost-effective way to improve the nation's cybersecurity materially."[14]

ISA analysis shows up to 40% of cyber budgets — roughly $80 billion annually — are consumed by redundant mandates, with some large firms reporting 70% of cyber staff time spent on compliance rather than active defense[15]. Every hour spent on overlapping requirements is an hour lost to stopping attacks.

Leveraging Presidential Direction on AI

There are now multiple methodologies and technologies that can identify duplication in regulatory regimes, even across sectors, and using slightly different language[16]. The President's Executive Order on AI now explicitly directs agencies to use advanced analytics to improve efficiency and national security[17]. This directive provides both the political authority and operational mandate to apply AI at scale to identify and remove duplicative cyber requirements.

In June, a coalition of major cybersecurity trade groups — the Internet Security Alliance, the Information Technology Industry Council, The Business Software Alliance, The ACT, and the Global Resilience Federation Business Council — wrote to OMB Director Vought endorsing a plan for using advanced technology specifically to identify instances of duplicative cyber regulation[18]. Once the technology has identified the areas of duplication, sector risk management agencies would be required to work with industry to resolve the redundancy by a date specific to them. OMB's role would be to enforce the streamlined regulation by restricting funding for enforcement unless a consensus solution has been achieved.

Path Forward

The National Cyber Director, working with OMB, should require all agencies with cyber oversight to produce complete inventories of their mandates. AI-driven analysis can then rapidly map overlaps and contradictions, creating a prioritized list of the most costly and counterproductive requirements. At this point, duplications can be removed, compliance obligations consolidated, and sector-specific "single points of compliance" established — freeing billions for real defense.

Strategic Impact

Removing duplicative regulations would:

- Redirect tens of billions annually to active cybersecurity measures
- Free 40-70% of cyber talent for operational defense
- Dramatically cut compliance timelines, which often exist amid significant attacks
- Save the federal government billions of dollars from reduced agency costs with virtually no implementation cost[19]

PRIORITY TWO: Require Cost-Benefit Analysis for Cybersecurity Regulations

Why This Is Essential

The federal government has imposed cybersecurity regulations on industry for decades[20] — during which our nation's cybersecurity resilience has grown increasingly dire.

Despite spending trillions of dollars on cybersecurity regulatory compliance, no study has ever documented that the cybersecurity regulations actually enhance security. Indeed, the best research on this topic, reported in Douglas Hubbard's book *How to Measure Anything in Cybersecurity*, concluded that none of the regulatory methods used by the government has ever been shown to improve security[21].

The most fundamental criterion for the government imposing a mandate on private industry is that the requirement will effectively fulfill a public policy goal — in this case, security. In order for any such program of government mandates to be sustainable in a free-market economy, they must also be cost-justified.

Even after OMB installs a process to eliminate duplicative cyber regulations, there will still be a remaining regulatory structure. ISA's AI-driven analysis suggests eliminating duplication would reduce the number of cybersecurity regulations from the current several hundred down to about 75 core regulations[22].

However, just because a regulation is not duplicative, it does not necessarily follow that it is effective in achieving its purpose, let alone doing so in an economically sustainable fashion. ONCD, in its coordinating capacity, should work with OMB to ensure appropriate cost-benefit analysis is done on every cyber regulatory requirement. If an agency cannot demonstrate appropriate cost-benefit to ONCD, it should be forced to reform or remove the regulation. OMB can again assist in an enforcement action.

Across most federal regulatory domains, cost-benefit analysis (CBA) is standard practice[23] — ensuring that the benefits of a rule justify its costs. In cybersecurity, however, agencies often impose requirements costing billions without calculating whether those rules actually improve security. This leads to what ISA research identifies as an "anti-security" regulatory regime, where compliance diverts resources from real threats[24].

The Millennium Challenge Corporation (MCC) offers a proven model. MCC only approves projects with rigorous cost-benefit analysis, requiring demonstrable returns on investment and measurable outcomes[25]. Applying that discipline to cybersecurity would ensure that federal mandates produce measurable security gains.

Path Forward

The National Cyber Director should support legislation requiring a formal CBA for all cybersecurity regulations, using an MCC-style threshold for return on investment. Executive action can apply the same standard to all new executive branch cyber initiatives immediately, with results published in a transparent, publicly accessible format. Agencies should also conduct retrospective reviews of existing rules and sunset those that fail the test.

Strategic Impact

Rigorous CBA would:

- Prevent costly, low-impact rules from taking effect
- Build private-sector trust through transparent justification
- Save billions in unjustified compliance costs

PRIORITY THREE: Reauthorize and Modernize the 2015 Cybersecurity Information Sharing Act

The Looming Deadline

The Cybersecurity Information Sharing Act (CISA 2015) — the legal foundation for public-private cyber collaboration — will expire on September 30, 2025, unless reauthorized. Allowing it to lapse would severely limit the government's ability to share threat intelligence with industry, undermining national security.

Why Modernization Matters

The cyber threat picture is not the same in 2025 as it was in 2015. While the core of the 2015 CISA needs to be maintained, the incentives to report threats need to be updated beyond the traditional threat indicator model.

We now can, and have, suffered significant cyber incidents that have nothing to do with cyber-attacks (e.g., CrowdStrike)[26]. The ecosystem has grown incredibly complex, resulting in certain elements (products) having such dominant market penetration that they become single points of failure[27], subject to mistake (CrowdStrike) or attack (SolarWinds).

When passed in 2015, the law did not anticipate the degree of market concentration in cloud services, software supply chains, and other critical technologies (with some products having 70% or more of the market), creating a massive single point of failure[28] wherein an event can cascade across sectors. Unfortunately, only the company producing the element is knowledgeable about its degree of market penetration, and the company has no incentive to report this dangerous condition to the government. Ironically, in many cases, once the issue is recognized, it can be mitigated through collaborative government-industry action.

Addressing these vulnerabilities requires updating the law by modernizing the definition of "threat" to identify and mitigate such "single points of failure." The same incentives for reporting traditional threat indicators can be expanded to recognize these market-driven threats and thus enhance protection from potential systemic failures while costing virtually nothing to the federal government or the industry provider.

Path Forward

The National Cyber Director should work with Congress to secure reauthorization while incorporating targeted updates:

- Authority to assess and address systemic cyber risks
- Expanded liability protections for broader threat sharing
- Cost recovery for private sector configuration changes to meet national security standards

PRIORITY FOUR: Creating a Cost-Effective Cybersecurity Workforce for Government

Why Workforce Is the Foundation

The U.S. faces a shortage of over 500,000 cybersecurity professionals[29], with 35,000 vacancies in the federal government alone, forcing the government, even after recent redeployments, to rely on expensive outside contractors to fulfill needed national cybersecurity functions[30].

Having an adequately trained cybersecurity workforce is essential to national cyber defense. In the face of ever-increasing and sophisticated cyber threats, nothing can work — not the technology, not the standards, not the frameworks — nothing works without an adequately trained workforce.

The PIVOTT Act, already passed out of the House Homeland Security Committee and co-sponsored by Senator Rounds and Senator Peters in the Senate, is an adaptation of the service academy model — adapted for cybersecurity[31].

Under PIVOTT, students could enlist in existing cybersecurity programs (college/community college/certificate programs) and the federal government would pay for their tuition. In return, the students would have to do a specified amount of government service. PIVOTT's target is to eventually enroll up to 10,000 students a year. At that rate, PIVOTT would solve the federal government's cybersecurity workforce gap (35,000) in less than 4 years.

PIVOTT graduates would be paid at a rate similar to that of traditional service academy graduates, which is far less than the government pays current outside contractors. The amount saved by paying PIVOTT graduates instead of the current contractors more than offsets the cost of the PIVOTT students' tuition[32].

PIVOTT solves the federal government's cyber workforce shortage in less than 4 years at no net cost to the government.

After PIVOTT graduates complete their government service, they can go into the private sector, where they will continue to protect our nation from cyber-attacks[33].

Path Forward

The National Cyber Director should champion PIVOTT's passage while piloting its core concepts in federal agencies — such as agency-run apprenticeship programs, cyber training incentives for the private sector, and dedicated veteran transition pipelines. In parallel, launch long-term initiatives including a virtual national cyber academy, K-12 curriculum integration, and community college certification programs.

PRIORITY FIVE: Create a National Macroeconomic Cybersecurity Dashboard

Virtually every aspect of policy risk — economic risk, geopolitical risk, environmental risk, weather — is calibrated through the use of macroeconomic models that enable the measurement of costs and benefits and allow for multiple variant analysis.

Ironically, there is no such model for analyzing cyber risk[34].

The federal government is spending tens of billions of dollars every year on an extensive range of cybersecurity projects. Yet without a sophisticated model, policymakers are blind to the full economic cost of cyber threats, the ROI of defenses, the usefulness of alternative methods such as incentive programs rather than regulation, the systemic impacts of major incidents, and the most cost-effective ways to eliminate, mitigate, or transfer risk.

Leading private sector enterprises have now switched to doing their own cyber risk management by using sophisticated models that put cyber risk in empirical and economic terms, enabling them to make sound cyber risk strategic decisions[35].

Path Forward

The National Cyber Director should work with the expanse of the federal government to promote this more sophisticated cyber risk assessment methodology based on the proven NACD-ISA framework.

Contract for the development of a national macroeconomic model that the government can use to assess cost-benefit, including:

- Real-time economic exposure from active threats
- Sector-by-sector compliance costs
- Market concentration and systemic risk metrics

- ROI for public and private cybersecurity investments and regulations

This tool would enable data-driven prioritization, early warning of systemic risks, and evidence-based policy decisions.

Conclusion: A Window for Action

The President's deregulation order, the looming CISA 2015 deadline, bipartisan frustration with regulatory duplication, and the new AI directive create a rare moment to act decisively.

By removing duplicative cybersecurity regulations, applying cost-benefit discipline, modernizing CISA 2015, passing the PIVOTT Act, and building a national cyber economics dashboard, the U.S. can significantly strengthen its cyber defenses while freeing billions for productive investment.

With White House backing, these initiatives can transform cybersecurity from a compliance burden into a competitive advantage — and secure both the nation's digital future and the President's legacy as the leader who turned deregulation into a national security triumph.

ENDNOTES

1. Microsoft Digital Defense Report 2024, "Cyber Threats and Nation-State Activity," Microsoft Corporation, October 2024.

2. McAfee and Center for Strategic and International Studies, "The Hidden Costs of Cybercrime Report 2024," December 2024.

3. Cybersecurity and Infrastructure Security Agency (CISA), "Enhanced Visibility and Hardening Guidance for Communications Infrastructure," December 2024; CISA, “Unsophisticated Cyber Actor(s) Targeting Operational Technology,” May 2025.

4. *See* Exec. Order, "Sustaining Select Efforts to Strengthen the Nation’s Cybersecurity and Amending Executive Order 13694 and Executive Order 14144”, The White House, June 6, 2025

5. Government Accountability Office, "Cybersecurity Regulations: Industry Perspectives on the Impact, Progress, Challenges, and Opportunities of Harmonization," GAO-25-108436, July 2025.

6. *See* Exec. Order No. 13771, Reducing Regulation and Controlling Regulatory Costs (2017) and Exec. Order No. 14192, Unleashing Prosperity Through Deregulation (2025).

7. *See* Paperwork Reduction Act of 1980, 44 U.S.C. §§ 3501-3520, and Paperwork Reduction Act of 1995, Pub. L. No. 104-13.

8. Letter from Chairman James Comer and Chairman Mark Green to OMB Director Russell Vought, April 15, 2025. https://homeland.house.gov/wp-content/uploads/2025/04/04.07.25-Letter-to-OMB-on-cyber-regulations-CHS-OGR.pdf

9. Internet Security Alliance, "AI Analysis: Duplication in Federal Cybersecurity Regulations," ISA Research Report, July 2025. https://isalliance.org/ai-analysis-duplication-in-federal-cybersecurity-regulations/

10. *See* Exec. Order 13771, "Reducing Regulation and Controlling Regulatory Costs," January 30, 2017; Executive Order on Regulatory Reform, January 2025.

11. Office of the National Cyber Director, “Summary of the 2023 Cybersecurity Regulatory Harmonization Request for Information,” June 2024. https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/06/Cybersecurity-Regulatory-Harmonization-RFI-Summary-ONCD.pdf

12. Office of the National Cyber Director, "National Cybersecurity Strategy Implementation Plan," Priority 1.1, March 2023.

13. Anne Neuberger, Deputy National Security Advisor for Cyber and Emerging Technology, remarks at the Center for Strategic & International Studies (CSIS) Panel, March 2023.

14. Letter from House Oversight and Homeland Security Committee Leadership to OMB, April 7, 2025. https://homeland.house.gov/wp-content/uploads/2025/04/04.07.25-Letter-to-OMB-on-cyber-regulations-CHS-OGR.pdf

15. Internet Security Alliance, "We Spend 70 Billion on Cybersecurity with No Way to Assess its Effectiveness," March 2025. https://isalliance.org/we-spend-70-billion-on-cybersecurity-with-no-way-to-assess-its-effectiveness/

16. Frontier, "Semantic and ontology-based analysis of regulatory documents for construction industry digitalization," April 2025.

17. *See* Exec. Order (E.O.) 14179, Removing Barriers to American Leadership in Artificial Intelligence, January 2025, Office of Management and Budget, M-25-21, "Accelerating Federal Use of AI through Innovation, Governance, and Public Trust," April 2025.

18. Coalition Letter from ISA, ITI, BSA, ARA, ACT App Association, and NCTA to OMB Director Vought, April 2025. https://isalliance.org/industry-letter-to-omb-on-redundant-regulations/

19. Congressional Budget Office, "Cost Estimate of Streamlining Federal Cybersecurity Regulations," September 2024.

20. Richard A. Clarke & Robert K. Knake, *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats* (2019).

21. Douglas W. Hubbard and Richard Seiersen, "How to Measure Anything in Cybersecurity Risk," 2nd Edition, Wiley, 2023.

22. Internet Security Alliance, "AI Analysis: Duplication in Federal Cybersecurity Regulations," ISA Research Report, July 2025. https://isalliance.org/ai-analysis-duplication-in-federal-cybersecurity-regulations/

23. Office of Management and Budget, Circular A-4, "Regulatory Analysis," September 17, 2003, updated January 2024.

24. U.S. House Committee on Oversight and Accountability, Subcommittee on Cybersecurity, Information Technology, and Government Innovation. *Hearing: Enhancing Cybersecurity by Eliminating Inconsistent Regulations*, July 2024.

25. Millennium Challenge Corporation, "Guidelines for Peer Review of Cost-Benefit Analysis," MCC Policy Paper, February 2022.

26. U.S. Cybersecurity and Infrastructure Security Agency. "Widespread IT Outage Due to CrowdStrike Update." *CISA Alert*, July 19, 2024. https://www.cisa.gov/news-events/alerts/2024/07/19/widespread-it-outage-due-crowdstrike-update

27. Aon Global. "A Highlight Year For Systemic Risk – And Single Point Of Failure Events." *Aon Global 2025 Cyber Risk Report*, April 2025. https://www.aon.com/cyber-risk-report/a-highlight-year-for-systemic-risk-and-single-point-of-failure-events

28. Carnegie Endowment for International Peace. "Effects of Cloud Market Concentration." *Carnegie Cloud Governance Toolkit*. https://cloud.carnegieendowment.org/cloud-governance-issues/effects-of-cloud-market-concentration/

29. U.S. House Committee on Homeland Security. "Chairman Green Announces Hearing on America's Cyber Workforce Shortage Amid Rising Threats." *Media Advisory*, June 21, 2024. https://homeland.house.gov/2024/06/21/media-advisory-chairman-green-announces-hearing-on-americas-cyber-workforce-shortage-amid-rising-threats/

30. *Id.*

31. H.R. 4515, "PIVOTT Act of 2024," 118th Congress; S. 2874, companion bill introduced by Senators Rounds and Peters.

32. Congressional Budget Office, "Score of H.R. 4515, the PIVOTT Act," CBO Cost Estimate, December 2024.

33. U.S. House Committee on Homeland Security. "Preparing the Pipeline: Examining the State of America's Cyber Workforce." *Hearing before the Committee on Homeland Security*, 119th Cong., 1st sess., February 5, 2025.

34. PwC Cyber Risk Services: PricewaterhouseCoopers. "Cyber risk quantified. Cyber risk managed."

35. National Association of Corporate Directors and Internet Security Alliance, "Director’s Handbook on Cyber Risk Oversight 2023," 4th Edition, NACD-ISA, 2023.

APPENDIX

Outdated and Ineffective: Why Our Current Cybersecurity Programs Fail to Keep Us Safe

Based on Chapter 4 of Fixing American Cybersecurity: Creating a Strategic Public-Private Partnership, authored by Larry Clinton and Alexander T. Green.

Traditional Regulation: Ineffective in Cyberspace

Perhaps the most common response for those becoming aware of the cybersecurity issue, and the ultimate tactic suggested by Clarke and Knake, is to suggest that what is needed is a standard regulatory model. Presumably, in such a system, the federal government would prescribe a set of effective standards that industry would have to comply with, subject to independent audit and enforcement for lack of compliance, including stiff penalties.

Unfortunately, this suggestion demonstrates a fundamental lack of understanding of the nature of the cybersecurity problem. It also highlights the lack of awareness of the extent to which regulation has already been attempted, where it has found little success. More importantly, it demonstrates the failure to realize that the traditional regulatory frameworks are fundamentally ill-suited to the digital age—a conclusion that has been reached even by those who have been put in charge of implementing such frameworks.[2]

Much of our traditional regulatory processes and judicial enforcement is designed to address malfeasance. However, the core problem with cybersecurity is not that the technology or the users are incompetent, uncaring, or evil. The core problem is technology is under attack. The attacks are not *because* the system is inherently vulnerable, although it is. As discussed in Chapter 1, most of our infrastructure is extremely vulnerable but rarely attacked. The primary cause of cyberattacks is overwhelming economic incentives. Certainly, technical modifications and operational enhancements, which are the focus of most cyber regulations, may improve security on the margins, but the evidence is now clear that these regulatory models are not up to the task and only pile on more requirements to overtasked security teams without demonstrating corresponding security gains.

Cybersecurity is a unique twenty-first-century problem. Traditional regulation is based on the independent agency model, which was initiated with the Interstate Commerce Commission (ICC) to deal with the hot technology of the 1800s: railroads. This model essentially calls for elected officials, such as Congress, to set broad policy parameters. An expert agency would then implement these policies by adopting specific standards or compliance requirements. This model has been copied for the past two centuries to deal with issues as divergent as consumer products (Consumer Product Safety Commission [CPSC]), telecommunications (Federal Communications Commission [FCC]), and financial management (Securities and Exchange Commission [SEC]). It assumes that the independent agents have adequate expertise to set the standards or compliance requirements and that, when followed, the requirements achieve the goal, whether safety, transparency, or fairness. It also usually assumes that there is a stable set of standards or requirements that the agency can determine have been followed, consistent with the broad policy parameters. Typically, regulated entities are audited to assess compliance with these standards.

The reasons these industrial age methods are proving ineffective is largely because they were designed to address fundamentally different types of problems from those we face today in cybersecurity. The model essentially attempts to locate a static standard that, for example, assures consumer safety wherever producers are in compliance. The key factor is that the subject being regulated is fairly stable. However, cybersecurity is not like consumer-product safety. If a regulator were to set standards for automobile brake pads, scientific analysis would be done to determine the appropriate amount of friction required to stop a vehicle of *x* size and *y* weight traveling at *z* speed. Over time, the size of the vehicles and the speeds at which they travel may vary, but the math doesn't change. So a standard in this sense can be developed and reliably applied with penalties for noncompliance.

However, in cyber, the technology is constantly changing, as are the attack methods, and new vulnerabilities are continuously being introduced or resurfacing. In other words, the target state for security is always moving. Clear standards, such as those needed for auto safety, become outdated quickly. The typical notice and comment rule-making process used for regulation by most agencies and government institutions is not equipped to handle the ever-changing cyber landscape. Transforming a proposal into an enforceable final rule can take several years, and by the time it is finalized, the initial risk or vulnerability of concern has evolved into something completely different. While there may be best practices, sometimes referred to as "process standards," these operate at a higher level of abstraction than traditional standards, such as in the consumer product safety model, and hence are difficult to precisely audit or confirm as to their actual impact.

The Coast Guard published its Cybersecurity Strategy concerning cyber risks at facilities regulated by the Maritime Transportation Security Act in 2015. The strategy went through Notice and Comment in 2017, and rules were made final in 2020. Five years is too long to develop rules for cybersecurity.

While the traditional regulatory model proved effective during the industrial age and may even be helpful in isolated areas of cybersecurity, as we discuss below, generally speaking, it is inappropriate for the digital age.

Cybersecurity Regulation

It is a common misconception that cybersecurity regulation has not been tried. As Clarke and Knake point out, "There is a mountain of cybersecurity regulation created by federal agencies. Banks, nuclear power plants, self-driving cars, hospitals, insurance companies, defense contractors, passenger aircraft, chemical plants, and dozens of other private sector entities are all subject to cybersecurity regulation by a nearly indecipherable stream of agencies including FTC, FAA, DHS, FERC, DOE, HHS, OCC, and so on."[3]

Clarke and Knake examine certain cases of cybersecurity regulation that demonstrate the faulty nature of the model in this space. For example, healthcare institutions were among the first entities regulated for cybersecurity, under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Yet they are one of the sectors that fares the worst when it comes to cybersecurity. In fact, data breaches are the number one regulatory challenge facing the healthcare sector.[4] Just because an entity is HIPAA compliant does not mean it is properly protected from cyberattacks, which increased at an alarming rate during the COVID- 19 pandemic.[5] In fact, a recent industry analysis showed that the number of confirmed healthcare-related data breaches had increased 71 percent since 2019.[6] As John Schneider, chief technology officer at Apixio, noted, "We shouldn't look to HIPAA to provide guidance. . . . Expecting regulations to fix data security problems is unrealistic."[7]

One of the deficiencies of the regulatory model is that its goal is compliance, which is generally a minimal accepted practice, and there is little incentive for entities to go beyond the compliance standard, even if more is required to provide actual security effectiveness. Put another way, compliance is helpful but not sufficient to combat today's cybersecurity challenges. In a post-COVID comprehensive study, ESI ThoughtLab found healthcare institutions ranked 11 of 13 critical sectors in terms of average loss compared to revenue.[8] Healthcare also ranked 11 of 13 sectors in terms of understanding cyber risk using state- of- the art quantitative methods and 13 of 13 sectors in terms of plans to increase spending. The study also found that on average healthcare institutions vastly underestimated the probability of a cyber breach and that less than half of the healthcare institutions had disaster recovery plans or cyber incident recovery plans or did regular cyber risk assessments or stress tests.

The heavily regulated financial services industry did better than healthcare but was empirically not the consensus industry leader, as might have been expected. In fact, among the 13 industry sectors analyzed, financial services led only in terms of plans to boost spending (followed closely in second place by the largely unregulated technology sector). This is consistent with the general understanding within the industry that regulations spur increased spending but not necessarily increased security. Financial services came out in the middle of the road in terms of losses compared to revenues: it was equivalent to healthcare in terms of vastly underestimating the likelihood of a cyber breach and was only slightly better than the healthcare sector in terms of cybersecurity effectiveness, with just over 50 percent of financial institutions having disaster recovery plans and cyber incident and recovery plans and conducting regular risk assessments and stress tests.

Overall, the ESI study found that heavily regulated sectors like finance and healthcare regularly ranked below generally unregulated sectors like the tech, general automotive, and manufacturing sectors in several critical cybersecurity measures.

Even government officials charged with implementing cyber requirements in heavily regulated sectors like telecommunications have come to the conclusion that traditional regulatory efforts have proven to be inadequate, not because they have not been tried, but because they are the wrong tool for this particular problem.

The former chair of the FCC under President Obama, Thomas Wheeler, and Rear Adm. (Ret.) David Simpson both worked in heavily regulated industries, telecommunications and defense, respectively, and are experienced regulators themselves. In 2019, they wrote for the Brookings Institution:

Current procedural rules for government agencies were developed in an industrial environment in which innovation and change—let alone security threats—developed more slowly. The fast pace of digital innovation and threats requires a new approach to the government-business relationship. As presently structured, the government is not in a good position to get ahead of the threat and determine standards and compliance measures where the technology and adversary's activities change so rapidly. A new cybersecurity regulatory paradigm should be developed that seeks to de-escalate the adversarial relationship that can develop between regulators and the companies they oversee. This would replace the detailed compliance instructions left over from the industrial era.

The Regulatory Compliance Model and Cybersecurity

Traditional compliance is essentially a pass-fail issue. You have either filed the forms or not. You have fulfilled the requirement or not. You can check the box or not. You are in compliance, or you are out of compliance.

Cybersecurity is not pass-fail. You are not secure or insecure. Security is a continuum with gradations of security. Moreover, not all entities, even within an industry sector, have the same security needs or the same threats to their security. As a result, a traditional check-the-box compliance system is inappropriate for the cybersecurity domain.

Traditional compliance is a backward-looking system. Did you do *x* or not? Cybersecurity is not a backward-looking exercise. Good cyber risk management is future-oriented. A critical step is to anticipate what sorts of threats you are likely to be subjected to and appropriately allocating your (usually meager) security resources accordingly. In today's compliance world, you can be compliant and not operationally effective. For example, every security compliance standard says an organization needs to have antivirus on the endpoint. However, there is no differentiation in the operational effectiveness of that solution. An organization can deploy the cheapest, simplest rule-based antivirus solution and get the "check" for having met the requirement. However, those that deploy a more sophisticated (and expensive) anti-malware, behavior-based" solution get no additional credit. So if compliance is the only goal, it can be met without gaining the necessary operational effectiveness needed in today's cyber threat environment. For a truly effective cybersecurity paradigm, security itself—properly measured—not checklist compliance, must be the goal. That is not currently the case with most government regulations.

In addition, the measurement systems that are the basis of most regulatory models is similarly inappropriate. In his excellent book, *How to Measure Anything in Cyber Risk,* Douglas Hubbard provides an extensive review of the statistical literature on the ordinal scales that are the standard measurement technique for much of the existing cybersecurity regulation. He determined that "there is not a single study indicating that the use of such methods actually helps reduce risk."[15]

A Waste of Resources

In addition to undermining security by setting a low minimal compliance bar, regulations may siphon valuable resources. As noted above, most regulations are not built around procedures that have been empirically shown to be effective in enhancing security, or in doing so, in a cost-effective fashion. In their 2020 report, MIT researchers Sean Atkins and Chappell Lawson note, "Because the value of specific cybersecurity investments is uncertain, government mandates tend to be both ineffective and economically inefficient. Firms may even cannibalize useful investments in order to comply with ill-conceived or inappropriate mandates."[16]

Numerous studies have indicated that we do not have enough cybersecurity professionals. It is estimated that as many as 3.5 million cybersecurity jobs will be unfilled by 2021.[17] As a result, the few professionals we do have are already stretched thin. Complying with regulations that have not been shown empirically to enhance security takes away precious time and resources that security practitioners could instead use to focus on their actual security mission. In addition, as discussed in the following chapters, the uncoordinated regulatory structure results in duplication of effort that wastes between 40 percent and 70 percent of these scarce resources (depending on the sector studied)—all without evidence of actually improving security.

When scarce security resources are sucked up by compliance costs, it means less time and money for actual security. Mandating compliance with outdated regulations is not only ineffective but actually counterproductive to enhancing cybersecurity. Also, organizations can overestimate the value of compliance and end up with an unjustified sense of security, which could lead them to take risks they assume are managed when, in fact, they are unknowingly vulnerable.

Undermining of Partnerships

The compliance/penalty culture, which is an inherent part of the regulatory structure, is especially problematic in the cyber domain. The mindset of the regulator tends to be like a parent who feels they must discipline their unruly, industry child. In cases of actual criminal or fraudulent behavior, this is appropriate. However, in cybersecurity, the problem is more often the unequal balance between the corporate (and governmental) defenders and the attackers who are focused on inherently vulnerable systems, have first mover advantage, and are often better resourced. This is especially the case for major cyber events, such as SolarWinds, which naturally are the ones of highest concern to the government.

Too many regulators feel the need to blame the victim of the attack, incorrectly presuming that severe penalties will drive better security. Moreover, the adversarial nature of the compliance/penalty culture is counterproductive to the sorts of collaborative partnership that industry and government need to evolve in order to create a sustainable collective defense model. Simply the perception of the big stick of penalties and enforcement will intensify the pre-existing attitude of fear and mistrust which undermines the widely accepted wisdom that neither government nor industry can maintain a secure cyber system unless they act together in true partnership. The former director of the Cybersecurity and Infrastructure Security Agency, Christopher Krebs, put this concept succinctly: “Protecting privacy is at the cornerstone of everything we do as an agency that depends entirely on maintaining the trust necessary to work with industry through our voluntary programs.”[18] Krebs’s view was echoed in the 2020 study by Atkins and Lawson: “For their part government officials lament that mandates encourage a ‘compliance mentality’ among firms leading to minimalist approaches rather than a concerted effort to secure their systems, cooperate with other firms in their industry or collaborate intensively with federal authorities.”[15]

In instances such as the Enron, WorldCom, and Volkswagen scandals, regulators stand in for consumers and protect them from malfeasant corporations—as they should. However, in today’s cybersecurity environment, the opponents are not mainly corporate cheats but rather vast criminal syndicates and increasingly nation-states and their surrogates that are stealing and corrupting personal data, corporate intellectual property, and national secrets. The reality, often articulated but rarely implemented, is that government, consumers, and industry are actually on the same side. They need to work together.

As we detail in chapter 5, a new paradigm that moves away from the traditional adversarial regulatory model and instead steers organizations to effectively use cybersecurity techniques based on empirical assessments of their legitimate business goals will lead to a more fulsome partnership between the public and private sectors—a social contract—is a more effective model for the digital age.

For the complete text of Chapter Four and additional resources on public-private partnership in cybersecurity, visit www.isalliance.org