EXECUTIVE SUMMARY OF THE REPORT TO THE PRESIDENT

Strategy for Cyber-Physical Resilience:
Fortifying Our Critical Infrastructure for a Digital World

Executive Office of the President

President's Council of Advisors on Science and Technology

February 2024

EXECUTIVE OFFICE OF THE PRESIDENT
PRESIDENT'S COUNCIL OF ADVISORS ON SCIENCE AND TECHNOLOGY
WASHINGTON, D.C. 20502

President Joseph R. Biden, Jr.
The White House
Washington, D.C.

Dear Mr. President,

While cyber and physical systems were once distinct, they have now become deeply interwoven. These *cyber-physical* systems are at the core of the critical services that underpin our lives—our water, electricity, banking, communications, air traffic, maybe your home heating system or refrigerator, and much more. Cyber-physical systems are increasingly vulnerable to threats from nation states, terror groups, criminals, a range of natural disasters, as well as accidents and failures. Vulnerable and underserved populations may feel these consequences of disruption most acutely. For instance, consider the winter of 2021 Texas power crisis. While this was primarily a failure of physical systems due to extreme cold leading to unexpected demand for electricity for electric heat, the lack of resilience built into the overall system, including its cyber elements, contributed to the catastrophe that left more than 4.5 million homes without power in sub-freezing temperatures, and communities facing shortages of water, heating, and food.[1] A study after the event discovered that the state's electrical grid came remarkably close to a cascade of failures that would have damaged equipment and brought down the grid in the state for *weeks to months*.[2] As another example, a ransomware attack on the billing systems of the Colonial Pipeline led to an extended shutdown of an otherwise operational system, leading to scarcity of gasoline and jet fuel affecting cities across the Eastern seaboard.[3]

We must continue to ensure effective cyber defenses and, at the same time, acknowledge that we cannot make all our infrastructure impervious to every threat or hazard. Instead, we must make our cyber-physical infrastructure *resilient*. Fortifying the resiliency of our critical infrastructure will require a substantially deeper partnership between the public and private sectors to focus attention and to unleash deeper investment.

Your Administration is making great progress on this front. The Office of the National Cybersecurity Director (ONCD) has put a bold strategy into action.[4] The National Security Council (NSC) took vital steps to bolster resilience across critical infrastructure. The Department of Homeland Security Cybersecurity and Infrastructure Security Agency (DHS/CISA) and the National Security Agency (NSA) are energizing the Nation to improve cybersecurity. The private sector has responded with greater commitment, delivering innovations in security and resilience in products and services, by

---

[1] Schwartz et al. (2021 February 22). "Power companies get exactly what they want": How Texas repeatedly failed to protect its power grid against extreme weather. *The Texas Tribune.*
[2] Humphreys, B.E. (2021 March 4). "Texas Power Outage: Implication for Critical Infrastructure Security and Resilience Policy. *Homeland Security Digital Library.*
[3] U.S. Government Publishing Office. (2022 June 8). Threats to Critical Infrastructure: Examining the Colonial Pipeline Cyberattack [Hearing]. *Homeland Security Digital Library*
[4] White House (March 2023). National Cybersecurity Strategy.

default and by design. We applaud these efforts and early successes while also recognizing that many vulnerabilities remain.

This report recommends a series of actions to fortify the resilience of our Nation's critical infrastructure as follows:

1. **Establish performance goals.** We recommend that you task CISA, building off its efforts to develop both Cybersecurity Performance Goals and Physical Security Performance Goals, to work with Sector Risk Management Agencies (SRMAs) and their Sector Coordinating Councils (SCCs) to create an integrated set of Critical Infrastructure Performance Goals that define *minimum viable delivery objectives* for services that are integral to our daily lives.

2. **Bolster and Coordinate Research and Development.** We recommend that you ask CISA, in partnership with SRMAs and SCCs, to task the National Risk Management Center to develop a *National Critical Infrastructure Observatory* to enable us to better understand the weaknesses and strengths of our infrastructure, helping us to outmatch adversarial attacks and prepare for accidents and catastrophes. We further recommend that you task the National Science and Technology Council to formulate a more coordinated national research and development (R&D) agenda on cyber-physical resilience.

3. **Break Down Silos and Strengthen Government Cyber-Physical Resilience Capacity.** We recommend you direct cabinet secretaries of the agencies responsible for our national critical infrastructure to fully resource their SRMAs with greater capabilities to support the cyber-physical resilience goals of our critical infrastructure sectors, ensuring that they can reliably deliver the services that Americans need.

4. **Develop Greater Industry, Board, CEO, and Executive Accountability and Flexibility.** We recommend you direct CISA to work with SRMAs and SCCs to increase the expectations that boards, CEOs, and other executives, as the owners and operators of our critical infrastructure, contribute more time and resources to ensure that infrastructure is reliable and resilient. The private sector should further augment its "tone at the top'' with "resources in the ranks" to increase operations and activities aimed at strengthening resilience. In addition, CISA should work with local utility commissions and overseers (especially for water and electricity) to ensure that necessary investments for cyber-physical resilience are made.

Executing these recommendations will amplify and extend the bright lights of efforts already underway to achieve resilience in the critical services that are integral to the daily lives of every American. It is what our country needs and deserves.

Sincerely,

Your President's Council of Advisors on Science and Technology

Executive Summary

Today's digital revolution is continuously remaking communications, utilities, transport, military, and commercial systems. Digital tools have provided immense gains in control, effectiveness, and efficiency, but digital dependencies also increase risks of national disruption through accidents and particularly, in the 21st century security environment, from malevolent attacks.

With the accelerating pace of technological innovation and the increasing sophistication of cyber threats, the traditional approach of developing cybersecurity defenses with the sole purpose of keeping attackers out, while still essential, is no longer sufficient. Acknowledging the inevitability of cyberattacks due to advances in technology, the potential for human error, and complexity of our systems makes it imperative to shift our focus towards building *resilient* systems. Resilience entails the ability of a system to anticipate, withstand, recover from, and adapt to cyberattacks and natural or accidental disruptions.[5] Our approach must shift from a futile quest for absolute invulnerability to a more realistic strategy of resiliency in which we control the impacts of failures.

This report describes why we must do more, and how we *can* do more, to protect ourselves where the cyber and physical interact. It conveys PCAST's endorsement for relevant initiatives underway in the public and private sectors, and particularly our applause for efforts to coordinate the two—and our need to go further.

The goal of the recommendations herein is to radically improve our ability to address the challenges facing government and all of our critical infrastructure, which is typically in private hands. We encourage both public and private sector organizations to use this report as a foundation to broaden and intensify their resilience initiatives.

Recommendations

Recommendation 1: Establish Performance Goals

Set *minimum viable delivery objectives* for critical services, even in the face of adversity, and establish more ambitious performance goals to measure every organization's ability to achieve and sustain those.

- **1.A Define sector minimum viable operating capabilities and minimum viable delivery objectives**
- **1.B Establish and measure leading indicators**
- **1.C Commit to radical transparency and stress testing**

Recommendation 2: Bolster and Coordinate Research and Development

Put in place a more coordinated national R&D agenda, including delivering a *National Critical Infrastructure Observatory* to outmatch our adversaries in knowing and resolving our weaknesses and concentrations of risk.

---

[5] Ross et al. (2021 December). Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. *NIST Special Publication 800-160,* Vol. 2, Rev. 1.

2.A Establish a National Critical Infrastructure Observatory
2.B Formulate a national plan for cyber-physical resilience research
2.C Pursue cross-ARPA coordination
2.D Radically increase engagement on international standards
2.E Embed content on cyber-physical resilience skills into engineering professions and education programs

Recommendation 3: Break Down Silos and Strengthen Government Cyber-Physical Resilience Capacity

Clarify the what and why of the national critical functions list to help each sector prioritize. Enhance the staffing and capabilities of Sector Risk Management Agencies[6] so that they can perform their critical role in increasing resilience across their sector in close partnership with CISA as the designated National Coordinator for critical infrastructure and resilience.

3.A Establish consistent prioritization of critical infrastructure
3.B Bolster Sector Risk Management Agencies staffing and capabilities
3.C Clarify and strengthen Sector Risk Management Agency authorities
3.D Enhance the DHS Cyber Safety Review Board (CSRB)

Recommendation 4: Develop Greater Industry, Board, CEO, and Executive Accountability

Increase the expectation that boards, CEOs, and other executives, as the owners and operators of our critical infrastructure, will lead from the front. More of the private sector should augment their "tone at the top" with "resources in the ranks" to be prepared for adverse events. This will require greater engagement with and from the most senior members of private sector organizations.

4.A Enhance Sector Coordinating Councils
4.B Promote supply chain focus and resilience by design

Download the full report

[6] Cybersecurity & Infrastructure Security Agency. Sector Risk Management Agencies. (Accessed 2024 February).