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

About the President's Council of Advisors on Science and Technology

The President's Council of Advisors on Science and Technology (PCAST) is a federal advisory committee appointed by the President to augment the science and technology advice available to him from inside the White House and from the federal agencies. PCAST is comprised of 28 of the Nation's thought leaders, selected for their distinguished service and accomplishments in academia, government, and the private sector. PCAST advises the President on matters involving science, technology, and innovation policy, as well as on matters involving scientific and technological information that is needed to inform policy affecting the economy, worker empowerment, education, energy, the environment, public health, national and homeland security, racial equity, and other topics.

For more information about PCAST see www.whitehouse.gov/pcast.

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

The President's Council of Advisors on Science and Technology

Co-Chairs

Frances H. Arnold
Linus Pauling Professor of Chemical Engineering, Bioengineering, and Biochemistry
California Institute of Technology

Maria T. Zuber
Vice President for Research and E. A. Griswold Professor of Geophysics
Massachusetts Institute of Technology

Arati Prabhakar
Director, Office of Science and Technology Policy
Assistant to the President for Science and Technology
The White House

Members

Dan E. Arvizu
Former Chancellor
New Mexico State University System

Dennis Assanis
President
University of Delaware

John Banovetz
Executive Vice President, Chief Technology Officer and Environmental Responsibility
3M Company

Frances Colón
Senior Director, International Climate
Center for American Progress

Lisa A. Cooper
Bloomberg Distinguished Professor of Equity in Health and Healthcare and Director of the Center for Health Equity
Johns Hopkins University

John O. Dabiri
Centennial Professor of Aeronautics and Mechanical Engineering
California Institute of Technology

William Dally
Chief Scientist and Senior Vice President for Research
NVIDIA

Sue Desmond-Hellmann
Former CEO
Bill & Melinda Gates Foundation

Inez Fung
Professor of Atmospheric Science
University of California, Berkeley

Andrea Goldsmith
Dean of the School of Engineering and Applied Science and the Arthur LeGrand Doty Professor of Electrical and Computer Engineering
Princeton University

Laura H. Greene
Chief Scientist, National High Magnetic Field Laboratory
Florida State University, University of Florida, Los Alamos National Laboratory
Marie Krafft Professor of Physics
Florida State University

Paula Hammond
Institute Professor, Vice Provost for Faculty, and member of the Koch Institute for Integrative Cancer Research
Massachusetts Institute of Technology

Eric Horvitz
Chief Scientific Officer
Microsoft

Joe Kiani
Chairman and CEO
Masimo

Jon Levin
Philip H. Knight Professor and Dean of the Graduate School of Business
Stanford University

Steve Pacala
Frederick D. Petrie Professor Emeritus in the Department of Ecology and Evolutionary Biology
Princeton University

Saul Perlmutter
Franklin W. and Karen Weber Dabby Professor of Physics and Director of the Berkeley Institute for Data Science
University of California, Berkeley
Senior Scientist
Lawrence Berkeley National Labs

William Press
Leslie Surginer Professor of Computer Science and Integrative Biology
The University of Texas at Austin

Jennifer Richeson
Philip R. Allen Professor of Psychology and Director of the Social Perception and Communication Lab
Yale University

Vicki Sato
Professor of Management Practice (Retired)
Harvard Business School

Lisa Su
President and CEO
Advanced Micro Devices (AMD)

Kathryn D. Sullivan
Former Astronaut
National Aeronautics and Space Administration
Former Administrator
National Oceanic and Atmospheric Administration

Terence Tao
Professor & the James and Carol Collins Chair in the College of Letters and Sciences
University of California, Los Angeles

Phil Venables
Chief Information Security Officer
Google Cloud

Catherine Woteki
Visiting Distinguished Institute Professor in the Biocomplexity Institute
University of Virginia
Professor of Food Science and Human Nutrition
Iowa State University

PCAST Staff

Lara Campbell
Executive Director

Reba Bandyopadhyay
Deputy Executive Director

Melissa Edwards
Assistant Deputy Executive Director

Bich-Thuy (Twee) Sim
Assistant Director for Transformative Medicine and Health Innovation

Kimberly Lawrence
Administrative Specialist

Riya Dhar
Intern

Sarah Domnitz
Former Principal Deputy Executive Director

Alexia Sare
Former Policy Analyst

Karin Saoub
Former AAAS Science and Technology Policy Fellow

Maya Millette
Former Intern

Working Group on Cyber-Physical Resilience

Working Group members participated in the preparation of this report. The full membership of PCAST reviewed and approved the report.

Co-Leads

Eric Horvitz*
Chief Scientific Officer
Microsoft

Phil Venables*
Chief Information Security Officer
Google Cloud

Members

Richard Danzig
Former Secretary
Department of the Navy

Kevin Fu
Professor
Electrical and Computer Engineering
Khoury College of Computer Sciences
Bioengineering
College of Engineering
Northeastern University

Dan Geer
Chief Information Security Officer
In-Q-Tel

Jon Levin*
Philip H. Knight Professor and Dean of the Graduate School of Business
Stanford University

William Press*
Leslie Surginer Professor of Computer Science and Integrative Biology
The University of Texas at Austin

Vicki Sato*
Professor of Management Practice (Retired)
Harvard Business School

Georgianna Shea
Chief Technologist of Transformative Cyber Innovation Lab
Foundation for Defense of Democracies (FDD)

Lisa Su*
President and CEO
Advanced Micro Devices (AMD)

Kathryn D. Sullivan*
Former Astronaut
National Aeronautics and Space Administration
Former Administrator
National Oceanic and Atmospheric Administration

** Denotes PCAST member*

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

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

Strategy for Cyber-Physical Resilience

Introduction

"The future is already here, it's just not evenly distributed."
— attributed to William Gibson

As America's digital revolution in the 1990s progressed, it shaped our modern cyber-physical infrastructure, initially shielding us from attacks due to the unfamiliarity of the digital systems' intricacies to both attackers and defenders. As the epigram above suggests, digital systems were installed at an uneven pace, and the effects of attacks were mitigated because attackers needed to comprehend a combination of new digital and old analog systems, making effects uncertain, minimal, and subject to mitigation. Cyber accidents and failures also had only isolated impacts, since computer controls were not universal and were less frequently interconnected.[7]

Today the situation is drastically different. Every system important to our modern existence now has cyber components and despite our best efforts, breaches and failures may occur. The key to protecting the services and infrastructure we rely on lies in developing systems that can not only defend against attacks but also minimize impacts on delivery of critical services.

What is Cyber-Physical Resilience?

Cyber-physical systems are physical systems that rely on computing technologies for sensing, analysis, tracking, controls, connectivity, coordination, or communications.[8, 9] Most of the systems we depend upon across sectors, spanning our electricity, water, healthcare, communications, transportation, manufacturing, and defense, are now cyber-physical in nature. For example, the electric grid relies on automated sensing, controls, and communication networks. This allows for real-time monitoring, predictive maintenance, effective coordination among multiple power sources and electricity-producing organizations, and efficient power distribution. Even systems that might not appear to be cyber-physical (e.g., financial services) have extensive cyber-physical dependencies on sectors that do, or per their reliance on their own data centers, which are inherently cyber-physical. Given their vital nature, the effective operation of cyber-physical systems is paramount and *the core functioning of systems must continue despite failures of one or more computational or physical components*.

Cyber-physical resilience is the capacity of an integrated system to keep running—even if not at peak performance—should it lose specific functions. Challenges include degradation or cessation of one or more aspects of the computational or physical functions due to component failures, human errors, natural disasters, or malicious attacks. For instance, if one or more of computer-based controls, sensors, or Internet communications employed in a water treatment plant fail, the system should still continue to operate, by relying on backup systems and plans, auxiliary sensors, or manual controls,

---

[7] Chadd, K. (2020 November 30). The History of Cybercrime and Cybersecurity, 1940 – 2020. *Cybercrime Magazine.*
[8] U.S. National Science Foundation. Cyber-Physical Systems (CPS). (Accessed 2024 February). This report defines cyber-physical systems more broadly than NSF's CPS efforts.
[9] Cyber-Physical Systems Working Group. (2017 June). Framework for Cyber-Physical Systems: Volume 1, Overview. NIST Special Publication 1500-201.

ensuring clean water is still delivered to homes. We should have an understanding *in advance* of *how* and *how well* such operations will proceed in light of one or more failures.

We urge prioritization of the following recommendations against a backdrop that we think is indisputable: despite our best efforts, breaches and failures of cyber components will occur, especially since w*idespread digital attack is easier to effect than widespread physical attack.*[10] Cyber-attacks can be conducted from a distance with little exposure for the attacker, they can be hidden and lie fallow for years before they are called to execute, they can simultaneously be conducted against an immense number of systems, and they can overwhelm operators whose expertise is focused on their physical—rather than digital—infrastructure.

Our key to success lies in developing systems that can not only defend against attacks but also minimize effects on delivery of critical services, regardless of the cause of failure. Since all of the Nation's critical infrastructure (Figure 1) is composed of cyber-physical systems, we have taken a broad approach that can benefit every sector.

Figure 1. Department of Homeland Security list of the 16 U.S. Critical Infrastructure Sectors.

Overarching Principles

Our examination revealed the following strengths and weaknesses of cyber-physical systems which provide key context and principles for our recommendations:

A physical system that depends on a digital system can be sabotaged by a digital attack. Digitally dependent physical systems are cyber-physical systems. They include: utilities, pipelines, power grids, transport systems, ports and many more. When Colonial Pipeline's digital infrastructure was penetrated by a ransomware attack in 2021, protective responses operators performed based on fears and lack of understandings of the overall cyber-physical system halted flows on 5,500 miles

[10] Li, Y., and Liu, Q. (2021 November). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports,* Vol. 7, 8176-8186.

of its pipelines, from Texas to New Jersey for four days, disrupting fuel supplies across the East Coast.[11]

Cyber-physical risk is high, while protections are disproportionately low. America's infrastructure systems were created and operated long before they acquired cyber dependencies, with sensing, computing, and networking dependencies developing in different ways over time. There is no systemic, pervasive protection against cyber risk since our protections and defenses for each cyber element have also evolved over time. Attacks against our water supply infrastructure illustrate these vulnerabilities.[12]

Future systems must be shaped by cyber-informed engineering.[13] Much of the technology that underpins cyber and cyber-physical systems was engineered without appropriate consideration of security needs. Consequently, security and resilience elements are tacked on after systems are deployed, often imperfectly and at considerable expense. Our approach must change to ensure that technology manufacturers are developing their systems to be secure and resilient by design to dramatically reduce the number of flaws that can fail or be exploited by threat actors. For instance, in Dec. 2022, Southwest Airlines was forced to cancel 16,700 flights, stranding ~2 million passengers, due to the collapse of an outdated system for reassigning flight crews.[14]

Present systems require us to cope with vulnerabilities that cannot be completely identified, much less eradicated. The current cybersecurity landscape is riddled with hidden fragility and flaws. Even with the most rigorous testing and meticulous engineering, some vulnerabilities inevitably slip through. 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.

Cyber-physical systems are often networked and depend on other cyber-physical systems that are themselves networked. Accordingly, our defenses must be systemic, but they are generally not organized this way. When a major attack or failure occurs, the most common response has been to try and make the specific component stronger or better defended. This provides a temporary sense of relief at having solved the problem, but paradoxically, the problem grows worse, because people then place more trust in the "reinforced" component and create even more dependencies. For each serious attack or failure, our answer is to "turn the screw" even harder and our systems become ever more brittle. Consider the Jan. 2023 failure of the FAA system that sends timely safety alerts to pilots which caused ~9,000 flight delays because pilots were not allowed to take off without receiving notices.[15] A resilient approach would have ensured that critical information could be delivered by other mechanisms and allowed for departure once information was received. As highlighted by the example, resilience is not about the reliability of a single system, it is the ability to continue to function, perhaps in a degraded state, when that system is unavailable.

---

[11] U.S. Government Publishing Office. (2021 June 9). Cyber Threats in the Pipeline: Using Lessons from the Colonial Ransomware Attack to Defend Critical Infrastructure.
[12] Levy, M. (2024 January 2). States and Congress wrestle with cybersecurity after Iran attacks small town water utilities. *AP News.*
[13] Idaho National Laboratory. Cyber-Informed Engineering. (Accessed 2024 February).
[14] U.S. Department of Transportation. (2023 December 18). DOT Penalizes Southwest Airlines $140 Million for 2022 Holiday Meltdown.
[15] Shepardson et al. (2023 January 11). Airlines hope for return to normal Thursday after FAA outage snarls U.S. travel. *Reuters.*

Responsibility for our Nation's systems is fragmented. This reflects our federal system, our competitive markets, our separation of private and public enterprises, and the complexity of relationships between enterprises controlling different technologies at different points in extended supply chains. This manifests as challenges of prioritization, inconsistencies in authority to regulate, and often insufficient speed and breadth of response to discovered vulnerabilities or incidents. We contend that the fragmentation of our systems and services is not necessarily detrimental. Rather, the heterogeneous, patchwork approach to a great deal of our infrastructure *can be a source of resilience* if systems are appropriately designed and operated in accordance with goals of making them robust to failures and attacks.

The improvement and proliferation of new technologies, especially Artificial Intelligence (AI) systems, will transform the landscape of cyber-physical security, amplifying capacities for both attack and defense. AI and other new technologies are advancing rapidly. Technical innovations are inherently dual-use: they benefit both attackers and defenders. The strategy must be to adopt them fast enough and well enough to benefit defenders more than attackers and to not base any defensive strategy solely on denying technologies to attackers.

Recommendation 1: Establish Performance Goals

As the foundation of resilience, we need to define and aspire to achieve vital operating capabilities for all critical systems, even when those systems are experiencing failure. Regardless of whether the cause of a failure is rooted in organic system breakdowns, natural events, or successful adversarial attacks, we must have clear performance goals, and a plan to achieve those goals. We must have a shared language around key concepts, principles, and measures of resilience to assess our current capacities and gaps. From there, we can aspire to clear goals and facilitate the Nation's trust by tracking and reporting on our progress.

First, we need to define *sector minimum viable operating capabilities and minimum viable operating delivery objectives*. These goals, defined collaboratively in each sector, should be built on clear characterizations of the bounded impact—the idea that we limit the "blast radius," meaning the extent to which services are lost due to failures caused by malicious, natural, or other events. We need to adjust critical infrastructure to meet those objectives, including developing plans for systems to operate in a degraded state for a defined period.

Second, we need an expressive and informative set of *leading indicators* of cyber-physical resilience. Many standards and goals today are expressed *as lagging indicators* of adverse past events. Resilience can be improved dramatically by developing and following guidance provided by leading indicators that show when systems and practices are mitigating future risks. We need to develop standardized, succinct metrics that can be made transparent and used as generally accepted performance goals (GAP Goals).

Third, we need transparency and sharing of information about minimum viable operating delivery objectives and status on achieving leading indicators, provided in a controlled context. We must work to balance secrecy about our vulnerabilities with incentivizing adherence to goals. Compartmentalization and secrecy limits opportunities and abilities for collective improvement and must be addressed by establishing new forms of transparency.

Recommendation 1.A Define Sector Minimum Viable Operating Capabilities and Minimum Viable Operating Delivery Objectives

Building on efforts to develop Cybersecurity Performance Goals and Physical Security Performance Goals, CISA should work with the Federal Emergency Management Agency (FEMA), with SRMAs, and their SCCs to create an integrated set of Critical Infrastructure Performance Goals that define sector-specific Minimum Viable Operating Delivery Objectives. As part of this effort, CISA should continue to work with the National Institute of Standards and Technology (NIST) to define performance testing standards that will serve as the basis for reporting and transparency that will allow each sector to share its status in meeting these objectives. The Minimum Viable Operating Delivery Objectives should include the set of critical services and the minimum capabilities required to provide each critical service or function. Objectives should include measures of bounded impact and bounded failure. Bounded impact expresses minimum delivery goals where no more than X people will be without a specific service (e.g., communications, electricity, water, food, healthcare) for more than Y days. Bounded failure is a characterization of the maximal impact of any single failure and measures how well a single failure is prevented from cascading across interconnected systems by creating independence and resilience of subsystems and components.

Recommendation 1.B Establish and Measure Leading Indicators

We need to formulate a set of *generally accepted performance* (GAP) goals for cyber-physical resilience that serve as gold standards of achievement. SRMAs need to understand and report on the status of the indicators. CISA, with NIST, should build upon existing resilience metrics frameworks to define a prioritized list of leading indicator metrics that are broadly applicable to all sectors. A candidate set of measures is provided in Appendix B (1B). We recognize many sectors and their SRMAs have taken strong leadership positions and are well positioned to facilitate.

Recommendation 1.C Commit to Radical Transparency and Stress Testing

Create a level of transparency that encourages every sector to improve outcomes, without setting specific targets in regulation or requiring other new authorities. This can be accomplished by designing creative mechanisms for designated systemically important entities to report their performance metrics and stress test results in appropriate ways. We note that the goal is not perfection but rather to identify the boundaries of an organization's resilience under stresses so that executive leadership (and perhaps regulators), can decide if minimum viable operating objectives can be assuredly reached. CISA, in collaboration with NIST, should work with SRMAs to provide a system for entities / organizations to voluntarily report their Cyber-physical-GAP metrics to their SRMA, and then for the SRMA to provide transparency to the broader public regarding who has reported and how the sector is performing overall. The specific metrics can be kept confidential and only aggregated and disclosed under coordination of the relevant Sector Coordinating Council. CISA should seek a legislative path to enforce disclosure more publicly as a way to encourage self-correction. CISA should work with the SRMAs to define an operational framework for cyber-physical resilience stress testing that can be adopted or adapted for use by SRMAs and associated sector regulators (as applicable).

Recommendation 2: Bolster and Coordinate Research and Development

Our adversaries understand our infrastructure and its dependencies and weaknesses better than we collectively do. This needs to change. We need to create and operate a *National Critical Infrastructure Observatory* so that we have clear and much more complete visibility into our risks.

We must revise our national research and development effort to advance the state of the art in cybersecurity and cyber-physical resilience to support both government and private sector objectives by taking the following actions:

Recommendation 2.A Establish a National Critical Infrastructure Observatory.

Developing a national critical infrastructure observatory will ensure that our understanding of our critical infrastructure and its inter-dependencies is at least as good as the understandings that our adversaries have. The observatory could also help develop information about risks and challenges based on common accidents or other non-adversarial challenges. CISA's National Risk Management Center (NRMC) should work with a federally funded research and development center (FFRDC), a university affiliated research center, or national laboratory to collaborate with the private sector to develop a classified mapping system to inventory critical infrastructure and identify risks such as high reliance on specific technology or resources ("critical concentration risks") and single point of failure risks. CISA, as the National Coordinator for critical infrastructure, and NSA's Cybersecurity Collaboration Center (CCC), working with the defense industrial base, should proactively work with SRMAs and Sector Coordinating Councils (specifically the Sector Executive Councils introduced as part of these recommendations) to resolve any identified weaknesses revealed by the observatory.

Recommendation 2.B Formulate a National Plan for Cyber-physical Resilience Research.

We need to coordinate and focus our research efforts within and across R&D agencies, academia, and industry. Such planning and attention will increase the likelihood of successful research results, but more importantly help ensure that such results will transition into actual use. We recommend that OSTP partner with the Networking and Information Technology Research and Development (NITRD) program (part of the National Science and Technology Council) to achieve this goal by extending existing work on the Federal Cybersecurity Research and Development Strategic Plan.[16] We encourage the development of an interim annex to the impending 2023 report that broadens the scope to include cyber-physical resilience and focus on coordinating research efforts across all the NITRD member agencies. The strategic plan should include a statement of grand challenges / hard problems on which to focus. Essential research and development should include exploration of the potential for leveraging advances in AI techniques as the basis for new forms of resilience as well as the potential use of AI tools by adversaries to develop innovative attacks on cyber-physical systems. The latter includes the use of AI methods for escalating the scope, intensity, and inventiveness of attacks, including for strategizing and executing multi-faceted, sequential attacks across various sectors. For further discussion of AI advancements and cyber-physical resilience, refer to Appendix A, on *Advances in AI and Cyber-Physical Resilience*.

[16] National Science and Technology Council. (2023 December). Federal Cybersecurity Research and Development Strategic Plan.

Recommendation 2.C Pursue Cross-ARPA Coordination.

Maximize the likelihood of successful research efforts by aligning or combining complementary research efforts at the Defense Advanced Research Projects Agency (DARPA), Intelligence Advanced Research Projects Activity (IARPA), Advanced Research Projects Agency—Infrastructure (ARPA-I), Advanced Research Projects Agency – Health (ARPA-H), and Homeland Security Advanced Research Projects Agency (HSARPA). OSTP could facilitate Cross-ARPA coordination to regularly align efforts, especially in the context of the proposed National Plan for Cyber-physical Resilience Research. This coordination could be reviewed as part of the NITRD effort of the National Science and Technology Council.

Recommendation 2.D Radically Increase Engagement on International Standards.

The U.S. can and should take a leadership role in setting standards that will help us achieve our cyber-physical resilience goals by quickly and enthusiastically working toward the objectives described in the May 2023 U.S. National Standards Strategy for Critical and Emerging Technology.[17] PCAST particularly praises Line of Effort #3 and urges that the U.S. greatly expand the number of meetings of standards bodies hosted in the U.S. in the coming years. We encourage the Department of State to grant timely visas to facilitate broad international attendance at these U.S.-hosted events.

Recommendation 2.E Embed Cyber-Physical Resilience Skills into Engineering Professions and Education Programs.

There is focus on creating more cybersecurity professionals through various national and sector-specific education initiatives. However, we are not doing enough to equip engineering and technology professionals with cyber-physical expertise. We should increase cyber-physical risk and cyber-informed engineering (CIE) competency in ABET certification and in engineering training across disciplines, and issue a call to action to universities to include cybersecurity and cyber-physical resilience modules in computer science, IT engineering, and similar degree programs. The goal is to increase the professional workforce familiar with cyber-physical resilience tools, which will in turn help build resilient systems from the start and thoughtfully improve the systems we have. The CISA National Initiative for Cybersecurity Careers and Studies effort[18] starts in this direction by providing a common lexicon for cybersecurity work, with a focus primarily on information technology, to help employers develop their cybersecurity workforce. However, much more needs to be done to help engineers who run the operational technology develop cyber-physical resilience skills.

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

We need to put capabilities and authorities close to the front lines. It is vital to keep expertise and decision making as close as possible to the organizations and activities that incur cyber-physical risk. This means that designated Sector Risk Management Agencies must be able to address the cyber-physical challenges faced by that sector, which in turn requires that the SRMAs have the necessary

[17] White House. (2023 May). U.S. Government National Standards Strategy for Critical and Emerging Technology.
[18] National Initiative for Cybersecurity Careers and Studies. (2023 August 28). Workforce Framework for Cybersecurity (NICE Framework).

resources and other capabilities to fulfill that responsibility. SRMAs have long-standing relationships and expertise to deeply understand priorities, operations, and interdependencies, but have uneven resources across sectors to enable effective execution of their work.

Allow CISA to focus on its manager, coordinator, and service provider roles. CISA plays a vital role today that will become even more crucial in the future. CISA can extend and enhance its role as National Coordinator for critical infrastructure resilience and security and provider of common services across government. This can be done by pushing sector risk management responsibilities out to an empowered set of SRMAs.

Learn aggressively from failures and close-calls. We need to continue to support and enhance public/private sector information, threat, and vulnerability sharing through Information Sharing and Analysis Centers (ISACs), the DHS Joint Cyber Defense Collaborative (JCDC), and the National Security Agency (NSA) Cyber Collaboration Center. It is also important to have a well-functioning national incident review board to ensure that major incidents or close calls only happen once. DHS's Cyber Safety Review Board is an excellent start but needs to be better resourced and empowered with authorities to conduct investigations more like the National Transportation Safety Board (NTSB).

The recommendations below seek to empower agencies and departments to improve resilience, focusing on the capabilities and authorities needed to effectively meet current and anticipated cyber-physical challenges.

Recommendation 3.A Establish Consistent Prioritization of Critical Infrastructure.

Promote a clear understanding of the Nation's most critical functions, dependencies, supporting systems, and components, so we can focus efforts and resources appropriately. CISA should reinforce and re-energize the role of the National Risk Management Center (NRMC) and, in collaboration with ONCD, work with SRMAs and SCCs to establish a clear and canonical national and sector-by-sector *list of Systemically Important Entities* that underpin the *National Critical Functions*. This list would include a clear prioritization of the capabilities that are critical for each sector, with mapping to the associated systems required to deliver them. This list would include which organizations and entities are part of the critical functions, most importantly explaining for what reason.

Recommendation 3.B Bolster Sector Risk Management Agency (SRMA) Staffing & Capabilities.

Ensure SRMAs are capable of working in and across their sectors to drive needed national cyber-physical resilience outcomes, including achieving minimum staffing (expertise, staffing levels, and authorities) to perform cybersecurity and cyber-physical resilience mission responsibilities already codified in 6 U.S.C. § 665(d). ONCD and NSC should reinforce this as part of the development of a PPD-21 successor policy, and in doing so, further liberate CISA to focus on its role as National Coordinator for critical infrastructure security and resilience and provider of common services across SRMAs.

Recommendation 3.C Clarify and Strengthen SRMA Authorities.

Identify the authority gaps between federal vs. state, local, tribal, and territorial (SLTT) responsibilities to be sure that legislators and regulators understand what is required for each

critical infrastructure in any location to achieve the minimum viable operating capabilities (see recommendation 1). SRMAs can collaborate with ONCD to identify the authority gaps. CISA should develop a report on gaps and challenges for each critical infrastructure category and distribute that information to relevant operational organizations and agencies, as well as to leads at NSC, SRMA heads, law enforcement and the intelligence community (e.g., FBI, ODNI for proactive threat monitoring purposes).

Recommendation 3.D Enhance the DHS Cyber Safety Review Board.

To support critical learning and adaptation, the Cyber Safety Review Board (CSRB) needs to be empowered and staffed to do more reviews, identify systemic weaknesses and causal underpinnings of breaches and failures, and improve indicators and warnings that will protect cyber and cyber-physical systems. The goal is to drive more impactful adjustments across systems and society so that every major event or close-call makes us more secure and resilient—and every catastrophic event only happens once. CISA should seek sufficient Congressional authorities and resources for the CSRB to function in this way.

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

There is a disconnect between the capabilities of organizations to prepare for cyber-physical failures and attacks and the potential extent of human impacts from system failures should those organizations suffer an incident. We need to make sure organizations whose failure would create the most societal impact have the capabilities to achieve the resiliency our society needs. As shown in Figure 2, there is a dynamic interplay between the potential impact of an event and the capacity to defend or prepare for that event and we need to support those organizations whose failure would have the most impact but are the least prepared.

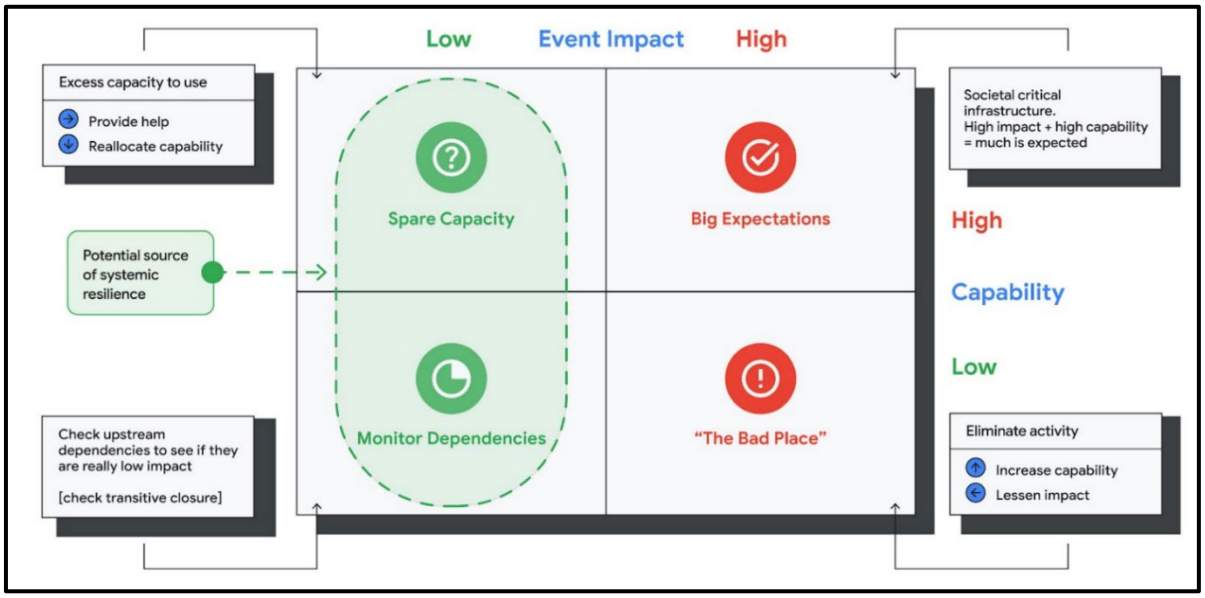

Figure 2. The dynamic interplay between the potential impact of an event and the capacity to defend or prepare for that event are represented here in a quadrant format. Each quadrant has unique implications for effective resilience and preparedness.

We encourage all organizations considering cyber-physical resilience to set ambitious goals. Achieving those goals will require understanding the gaps between reality and those goals and developing clear priorities to close those gaps. Understanding the gaps and prioritizing also permits an 80/20 approach to be taken, where we not only focus on the risks most likely to have the largest impact, but also identify and improve the 20% of risks or issues that can address 80% of the resiliency challenges.

In order to achieve better cyber-physical resilience across all critical services, we must amplify private sector executive engagement. Most of our national critical infrastructure is in private hands. Despite strong government efforts, incentives are insufficiently aligned, and regulatory and legislative dictates are inconsistent. This means that in the private sector, not enough is being invested in cybersecurity or broadly cyber-physical resilience. There are many potential reasons for this, but one solution is greater engagement with senior executives. It's clear that the "tone at the top" of organizations needs to be joined with "resources in the ranks" to make more progress in creating infrastructure that is modern, defensible, and secure by design.

These recommendations seek to empower critical private sector organizations to accelerate and prioritize cyber-physical resilience work as if their survival depended on it—as it indeed does.

Recommendation 4.A Enhance Sector Coordinating Councils (SCCs).

CISA should partner with SRMAs and other agency leadership to engage with private sector executives to achieve the following goals:

- All Sector Coordinating Councils (SCCs) should establish Sector Executive Committees to manage and coordinate council activities (some have already done this) and increase the seniority of membership in the corresponding Government Coordinating Council (GCC). Moreover, all SCCs should be chaired by critical infrastructure owners and operators.
- GCCs/SCCs implement Recommendation 1 (above) by establishing regularly updated performance goals focused on *leading* rather than *lagging* indicators and building on defined Sector Minimum Viable Operating Capabilities and Minimum Viable Operating Delivery Objectives; and commit to a path of appropriate transparency, including sharing results of stress testing to stimulate and incentivize every sector to improve outcomes.

Recommendation 4.B Promote Supply Chain Focus & Resilience by Design.

GCCs must partner with SCCs to identify the initiatives that will provide the greatest reward, often by helping providers of the most central (critical to many) resources improve their resilience. For instance, consider common vendors, shared infrastructure, communications and cloud / software services with the goal of identifying where risk is most concentrated in only a small number of common providers and then work with those providers to minimize the risks in their services. Consider expanding supplier diversity to avoid common-mode vulnerabilities.

Concluding Thoughts

Invigorating Incentives for Cyber-physical Resilience

Cyber-physical resilience, based on a marrying of cybersecurity, resilience, reliability, and recoverability in information systems, critical infrastructure, and operational technology, is vital to our societal functioning. As such, legislation and regulation at the national and state level to dictate the most effective approaches should be expected. Arguably the sectors that have proven better defended have been those with regulatory regimes and other oversight to compel such defenses and to consistently raise the bar.

But this does not tell the full story. Many large organizations work hard to improve their resilience not just because it is the right thing to do, but because it makes business sense. Protecting customers, driving security and resilience in supply chains, and being able to operate in adversity are what sets apart an organization that deserves customer trust and is more likely to not only survive, but thrive. Many of the approaches we recommend have significant commercial benefits, whether it is insurance benefits, increased agility, or a more stable base from which to innovate. In the development of this report, we heard calls from various sources to recommend the introduction of a federal cybersecurity insurance backstop. We rejected this as we believe it can create a moral hazard to disincentivize investment by companies in their own resilience. We think that there can be a vibrant and functional insurance market as our cyber-physical resilience improves and that insurers can drive improvements in security through standards associated with their policies and pricing. However, further work may be needed to look at concentration risks and the need for catastrophe risk approaches with federal government support.

We do not believe the implementation costs of the recommendations in this report targeted at government to be significant (in the context of agencies' budgets). We believe in many respects the goals can be met by reprioritizing existing activities. If the needed authorities are obtained, by Congressional action or otherwise, then the actions in this report can have even more effect. The cost impact to the private sector to implement this report's recommendations is higher, but dependent on their current state. We know many private sector organizations invest extensively, commensurate with their criticality, but others do not and so should direct more resources to the challenges of cyber-physical resilience. Increased cyber-physical resilience is usually fully aligned with commercial goals and is core to the mission and commercial objectives of public and private sector organizations. We see boards and executives driving such improvement in their own self-interest. However, as with any aspect of society, there need to be checks and balances—laws or regulations—to create the incentives to build resiliency that may slip in the face of occasional short-term thinking.

Private sector organizations need to also understand the benefits of partnership with government and across their sector. Partnering across the private sector and between public and government sectors is not just the right thing to do; it is the commercial and mission-essential thing to do. Sharing capabilities, intelligence, and approaches in effective and timely ways can act as a shared fate so that another organization's defense can become yours. But for that to happen, you have to participate. We need not just technical or cybersecurity leaders in this endeavor; we need boards, cabinet and agency heads, executives, and the engagement of all leaders so that we can collectively achieve greater resilience together.

Appendix A: Advances in AI and Cyber-Physical Resilience

AI technologies are advancing rapidly, based on a fifteen-year inflection with advances in deep neural network models, further bolstered by recent innovations with generative AI models. While this report's focus is not explicitly on AI, we underscore the crucial significance of this technology and recommend prioritizing a specialized analysis of its risks and applications for cyber-physical resilience.

In particular, it is crucial to recognize the dual nature of leaps in AI technology. We have an opportunity to harness AI advances for transformational applications. However, there is also potential for disruptive influences and risks, both known and unknown. The duality of the possibilities for advancement and for risk is especially at play with the goals of cyber-physical resilience.[19, 20, 21]

On the side of concerns, malicious actors could harness multiple dimensions of AI for new kinds of attacks, both on systems and via persuasive and deceptive influences on human operators. Attackers can leverage AI to create sophisticated malware, map an attack surface, and significantly amplify their capacity for denial, degradation, deception, disruption, and destruction. We expect malevolent nation states and criminal organizations to be able to harness AI technologies to assist with the design of multi-stage and multi-step exploit chains at an unprecedented pace.

Strategic preparation for such attack scenarios is imperative. Our report effectively portrays the current and near future state of the world. However, our planning efforts must reach beyond the present and actively anticipate the potential realities of the longer term, including the expectation that adversaries will have increasingly detailed maps of our infrastructure within and across sectors and be armed with AI-powered tools that are weaponized and aimed at attacking our critical cyber-physical infrastructure.

On the brighter side, AI is a powerful tool with immense opportunities to serve as a force multiplier to anticipate, sense, withstand, recover from, and adapt to adverse conditions. AI methods are already being harnessed to defend billions of people from malware and rogue websites; we are seeing AI used to decode attacks and respond with countermeasures. AI itself will come to play a critical role in ensuring the trust, safety, and security of how we use AI across all our systems. AI is a crucial resilience tool, emphasizing the need for a concerted public-private effort to proactively plan for its deployment.

---

[19] Horvitz, E. (2022 May 3). Artificial Intelligence and Cybersecurity: Rising Challenges and Promising Directions [Written Statement of Eric Horvitz], Hearing on Artificial Intelligence Applications to Operations in Cyberspace before the U.S. Senate Armed Services Subcommittee on Cybersecurity.
[20] Moore, A. (2022 May 3) Statement of Dr. Andrew Moore, Hearing on Artificial Intelligence Applications to Operations in Cyberspace before the U.S. Senate Armed Services Subcommittee on Cybersecurity.
[21] Lohn, A. (2022 May 3). Testimony before the Senate Armed Services Subcommittee on Cyber Artificial Intelligence Applications to Operations in Cyberspace, Hearing on Artificial Intelligence Applications to Operations in Cyberspace before the U.S. Senate Armed Services Subcommittee on Cybersecurity.

Beyond calling out the critical need to be ready for new forms of novel attacks and the opportunity to leverage AI in defense, we will not focus on details of AI and cyber-physical resilience. We note that advances in AI are relevant to many of the specific recommendations in this report and the commendable actions the administration is taking with AI. However, we emphasize important synergy between the public and private sectors, the technology community, and the research institutions on issues and directions with AI and cyber-security. It is also gratifying to see the early fruits of international cooperation as promising indicators of a united front against the multifaceted challenges of AI.

Specialized applications of AI for cyber-related activities demand skills beyond the typical scope of agencies like DHS, which traditionally concentrate on safeguarding existing systems from current threats. Our overall recommendation is the establishment of a dedicated and high-priority analytical initiative. This initiative should thoroughly explore both the technological implications of AI and, independently, the capabilities of potential adversaries. Importantly, the analysis must transcend mere examination and draw well-informed conclusions about the resulting implications.

We look forward to the results stemming from the work underway and will continue to advocate that the U.S. be bold but responsible in our adoption of AI. The fast-paced integration of AI by defenders becomes a crucial strategy to outpace potential attackers who will leverage the exponential capabilities of AI for nefarious purposes.

We particularly applaud the following actions and believe they should continue in full force:

- The Executive Order (Executive Order 14110 of October 30, 2023) on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. The EO has been widely received as a vital, global, contribution to defining a bold and responsible path forward for AI. We are pleased to see the directives to NIST to develop companion guidance to the AI Risk Management Framework, especially the callouts for the adoption of red team testing approaches. The directive that each Sector Risk Management Agency will conduct an assessment of AI risks to their sector is particularly important to contextualize risk and align it to cyber-physical resilience goals. We suggest as part of this that they consider how AI can *help* critical infrastructure be more resilient; that is, focus on the opportunities and the risks.

- DHS's proactive approach, following up on the Executive Order issuance, in publishing its CISA Roadmap for Artificial Intelligence. In particular, we endorse the prioritization of full utilization of AI technologies for cyber-defense in balance with ensuring appropriate risk management practices for the safe and responsible use of AI. We would further recommend DHS CISA partner closely with NSA's AI Security Center to share threat intelligence and AI security practices between critical infrastructure and National Security Systems / Defense Industrial Base use cases.

- The establishment of the NSA AI Security Center in its Cybersecurity Collaboration Center is an important step to bring AI insights to threat intelligence and cyber-defensive capabilities to protect the Nation, especially in the context of national security systems and the defense industrial base.

- Recommendations on trustworthiness, accuracy, and reliability of AI systems and concerns with adversarial machine learning presented in the final report of the Congressionally commissioned study authored by the National Security Commission on AI (NSCAI).[22]

- Efforts in the private sector and non-profit sector on AI safety, reliability, and security, including efforts within and across organizations as part of responsible AI efforts. As an example, methods are being shared among organizations via the industry-centric Frontier Model Forum (FMF) and by the non-profit, multiparty stakeholder organization, Partnership on AI (PAI). For example, the FMF has shared experiences and guidance on the testing of AI systems via maturing practices of "AI red-teaming."[23]

- NIST's ongoing work to enhance the AI Risk Management Framework for safety with generative AI models.

- We support MITRE's recent report on Principles for Reducing AI Cyber Risk in Critical Infrastructure: A Prioritization Approach—in particular, the need for mapping AI risks to national critical functions and ensuring Sector Risk Management Agencies collaborate with private organizations, public utilities, and regulators to ensure AI risk management within their sectors. [24] This is in line, broadly, with our call in Recommendation 1 for more consistent prioritization of critical infrastructure, and the related risks, and increasing SRMA capabilities.

[22] The National Security Commission on Artificial Intelligence (2021 March). Final Report
[23] Frontier Model Forum (2023 October). Frontier Model Forum: What is Red Teaming?
[24] C. Sledjeski (2023 October 25). Principles for Reducing AI Cyber Risk in Critical Infrastructure: A Prioritization Approach, *MITRE*.

Appendix B: Recommendation Details

The goal of this section is to provide significantly more detail for those tasked with implementation or for readers who wish to develop a deeper understanding of the problem and courses of action. We hope this section helps readers further refine their own specific strategies and tactics.

(1) Establish Performance Goals

Goal:

Create a small set of crisply defined, regularly updated, performance goals applicable across sectors that are biased toward leading versus lagging (retrospective) indicators of cyber-physical resilience. The aim should be to radically simplify and reduce the workload of reporting on hundreds of lagging indicators down to tens of goals that are more universally understandable and impactful. Push for and incentivize transparency regarding performance on those goals to facilitate follow-up that supports and incentivizes implementation and successful outcomes.

Setting the Scene

Cyber-physical resilience, cybersecurity, and critical infrastructure security have many risk assessment methodologies, standards, compliance regimes, and other attestation and certification frameworks. Many companies must undergo hundreds of regulatory assessments, certifications, and external auditor reviews, but too many of the metrics and more generally, performance goals, are lagging (retrospective). Even some of the potentially most promising work underway in government is still intrinsically biased toward large numbers of micro-metrics that are lagging not leading.

Reporting on what happened in the past does not necessarily help prepare for the future. We need to minimize rote burdens to favor high-impact, leading indicator goals that facilitate resilience to future challenges, along with processes to bring along the stragglers.

We encourage the development of standardized, succinct metrics that can be made transparent and used as leading indicators of cyber-physical resilience. We call these cyber-physical resilience Generally Accepted Performance Goals (GAP Goals).

Because of the large number of metrics that are required for many regulatory assessments, certifications, and auditor reviews, there are few (if any) metrics that are considered important to the most senior personnel in public or private sector organizations. This makes it harder for senior personnel to clearly understand where to assign resources. Additionally, many metrics are kept close-hold and are not subject to disclosure. Greater transparency can incentivize improvements in resilience, but we do not propose "target levels" of metrics become stipulated or otherwise regulated. Rather we simply propose some metrics or, more generally, performance goals, be publicized, perhaps after an initial 12-month period of disclosure only to SRMAs.

Currently, companies publish their GAAP (generally accepted accounting principles) standardized financial statements. This information helps investors and creditors understand the strengths, weaknesses, and risks associated with the companies with which they work or invest. **In contrast, almost no information is currently available to indicate how an organization is preparing for future cyber-physical challenges. This has to change.**

Recommendation: Formulate Cyber-physical Resilience Generally Accepted Performance Goals (GAP Goals)

We need to develop standardized, succinct performance goals that can be made transparent and used as leading indicators of cyber-physical resilience. We call these the Generally Accepted Performance (GAP) Goals. These are more focused, and more ambitious, than the performance goals we see currently being pursued. With sufficient standardization, we expect company boards and others to use these goals to drive transparency and comparability.

The Transportation Security Administration (TSA) instituted performance goals in its first-ever mandates for pipelines,[25] rail,[26] and aviation.[27]. The FDA pushed the PATCH Act, which (among other things) strengthens cybersecurity guidance for medical devices.[28] The country needs to reinforce the importance of these new requirements by adding minimum viable delivery objectives.

Conformance with these proposed performance goals is not necessarily expected to be 100%; instead, these aspirational metrics indicate where improvement is needed. These goals should substantially replace other more numerous metrics. This work can be built upon existing Cyber Performance Goal work—but should become more succinct and focused on leading indicators of good practices for achieving *cyber-physical resilience* versus serving as lagging indicators of outcomes. We believe that if good practice is adopted then good outcomes will follow.

Recommendation 1A: Define Sector Minimum Viable Operating Capabilities and Minimum Viable Delivery Objectives

Identify for each critical function what the minimum organizational capabilities must be to provide that critical service/function. Overlay existing critical function identification with an additional cyber-physical resilience notion of Minimal Viable Operating Capabilities and require organizations to be able to sustain those capabilities under more / most scenarios.

Establish a set of quantifiable and replicable **measures of performance** for each of the National Critical Functions, and a repeatable **methodology** for organizations to use within a sector to identify their most critical systems. Now is an ideal time to work on these measures, since CISA is updating the 2013 National Infrastructure Protection Plan which should include updating goals and strategies for the National Critical Functions framework.[29] The measures of performance could be effectively developed by a group such as the Federal Senior Leadership Council using a team with representatives from many SRMAs (ideally including at least five that are not DHS) and representatives from the respective Sector Coordinating Councils, ONCD, NSA, and NIST. NIST or

[25] U.S. Department of Homeland Security. (2023 December 6). DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators [Press Release].
[26] DHS Transportation Security Administration. (2023 October 23). Renewal with revisions to the Security Directive 1580/82-2022-01 series: Rail Cybersecurity Mitigation Actions and Testing [Memorandum].
[27] DHS Transportation Security Administration. (2023 March 3). TSA issues new cybersecurity requirements for airport and aircraft operators [Press Release].
[28] H.R.7084. (2022 March 15). Protecting and Transforming Cyber Health Care Act of 2022 or the PATCH Act of 2022.
[29] U.S. Government Accountability Office. (2022 March 1). Critical Infrastructure Protection: CISA Should Improve Priority Setting, Stakeholder Involvement, and Threat Information Sharing.

CISA could develop the methodology to identify critical systems in collaboration with an FFRDC. The critical system identification methodology should at least include identification of needs required to support minimum viable operating capabilities for that organization. Specifically, there is a need to develop and define quantitative goals for public services, even when functioning under challenging conditions. The goal is to set measurable targets and then test to ensure that level of reliability.

Defining sector-specific **Minimum Viable Operating Capabilities** will be essential. CISA could partner with SRMAs and FEMA to define each sector's Minimum Viable Operating Capabilities. NIST could define a performance testing standard with the goal of providing transparency on the ability of sectors to meet those objectives.

Minimum Viable Operating Capabilities should include a specification of one or more critical services and, for each critical service or function, measures of *bounded impact* and *bounded failure*.

Examples of **Minimum Viable Operating Capabilities** include:

- **Bounded Impact:** Expressions of minimum delivery goals e.g., no more than 50,000 people will be without X (e.g., communications, electricity, water, food) for more than 7 days. See the framework developed by the Global Resilience Federation as an illustrative basis for efforts on characterizing impact.
- **Bounded Failure:** Characterization of the maximal impact of any single failure via containment of spread. This requires creating independence and resilience of subsystems and components to failures of other components. This measure can be defined in terms of estimates of the time to reboot or rebuild all affected components of critical infrastructure capabilities from scratch. What is the maximum recovery time to bring up the full service when considering all single points of failure and how they might cascade to impact other components? Bounded failure can be extended to characterization of the maximal impact of any *tuple* of failures, such as for any *pair* of independent failures (i.e., consider the maximal impact of all combinations of dual failures for the most common failures).

Recommendation 1B: Establish and Measure Leading Indicators

Drive better outcomes with less effort by creating a concise and prioritized list of the leading indicator metrics applicable across all sectors that can be adapted to each sector's context. These leading indicator metrics should replace many of the myriad specific lagging indicators and represent an 80/20 opportunity, i.e., identify the 20% of cyber-physical challenges that, if addressed by these indicators, can provide 80% of the risk reduction and deliver 80% more commercial benefits (cost savings, agility, reliability, mission assurance) and so can be seen as broadly valuable.

CISA, in collaboration with NIST, should build upon existing cybersecurity performance goals and resilience metrics frameworks to define a "Top 10" list of leading indicator metrics that are broadly applicable to all sectors. This will increase focus on those metrics, even as metrics are adapted to the context of each sector. We recognize many sectors and their SRMAs have taken strong leadership positions and are already moving in this direction. Continued partnerships among SRMAs, facilitated by CISA in its national coordinator role and in partnership with NIST and ONCD, will be vital to creating viable metrics and facilitating their adoption.

The leading indicator metrics should include strong consideration of the following concepts as candidates. The intent is to identify an organization's most critical systems which in turn support its critical functions. Part of the definitions should include guidance on grouping and scoping to produce a meaningful metric in the context of that organization.

(1) Hard-Restart Recovery Time: the time to reconstitute/rebuild a system from scratch (as distinct from backup and recovery time objectives). This metric is intended to assess an organization's ability to remove circular dependencies during a restart, to assure backups can survive fully destructive shutdowns or attacks, and that software and data can be restored to service. The application of this concept will vary across different sectors.

(2) Cyber-Physical Modularity: a system-wide measure, computed as the mean of the impact of single points of failure. The measure considers the additional failures and impacts that come as cascades via dependencies on each initial single-point failure. This can be captured by a summary measure of the impacts of each primary point of failure. Alternatively, the measure can be computed as the mean operational capability of the service, even if degraded, summed over all single points of failure. For example, given that each single point of failure may cause a temporary outage or reduction of quality of service, what is the consequent median tested recovery time for all single points of failure to be repaired/recovered? For how many single points of failure is the defined minimum viable operating delivery objective sustained?

(3) Internet Denial / Communications Resilience: Internet denial testing: consider loss of Internet connectivity as a special notable point of failure. Explicitly test the impacts, nature of degraded service, and disruptions vs. operational continuity in the face of Internet disconnection. Some services are so critical that they should be operable safely, even in some degraded state, in the absence of network connectivity. Consider backup communication channels to diverse modes of communication in the event of Internet failure.

(4) Fail-over to Manual Operations: for physically actuated systems typically controlled by cyber operational technology, what is the degree of local manual control that can sustain a minimum viable operational delivery objective when automation is lost? How frequently is manual control practiced to sustain organization muscle-memory of its use? Additionally, to what extent is there a broader primary or back-up analog "control plane" to the system or components? While digitization is inevitable and valuable, maintaining some degree of analog control may be necessary and warranted for certain highly critical systems.

(5) Control Pressure Index: the extent to which defense-in-depth[30] is applied by measuring how much of a critical security or resilience objective is carried by a single control (that if failed would put the whole system at risk).

(6) Software Reproducibility: extent of software in a particular system that can be repeatedly and continuously built and distributed while maintaining conformance with the Office of

[30] Defense-in-depth is a cybersecurity approach in which several independent layers of security controls are used so that if one fails another will still be operative to provide security.

Management and Budget's (OMB) June 2023 Secure Software Development Framework (SSDF) requirements, including disclosing software bill of materials (SBOMs) and supply chain levels for software artifacts (SLSA) conformance levels. It is especially critical for vendors of software to critical infrastructure sectors to provide vital patches in a timely manner that will work with an infrastructure organization's updated IT environment and for software providers to assure the continuity of the build environments throughout that software's supported life. Critical infrastructure (e.g., hospitals, water) must be able to update legacy systems without losing additional software tools. A software reproducibility metric could be contextualized as "time to support" surrounding updates. Modern software lifecycle management practices in DevSecOps approaches are highly applicable.

(7) Preventative Maintenance Levels: percentage of the overall cost of systems operations that is devoted to preventative maintenance (e.g., upgrades, security patching, reducing technical debt).

(8) Inventory Completeness: extent of the universe of an organization's operations – including information technology (IT), operations technology (OT), and supply chain (to 4th party as well as 3rd party)—that is encapsulated in a validated and managed inventory or asset register.

(9) Stress-Testing Vibrancy (Red Teaming): extent of systems that have been subjected to an extreme offensive, adversarial security test (possibly AI augmented), to test defenses against reliable operation (this could be against an especially constructed "cyber range" and might be achieved with "chaos engineering" principles. This should include explicit testing against multi-point attacks—where an adversary is coming after multiple points in a system with multiple tactics, potentially both physical and cyber.

(10) Common Mode Failures and Dependencies: Identify organizations (and others in their supply chain) that in the event of failure would represent significant harm to a whole sector—because of the concentration they represent. As part of this, finding and eliminating circular dependencies is vital i.e., organization X depends on Y to cover and vice-versa.

These leading indicators are not to be relied upon as static measures. Any indicator can become stale quickly in the evolving world. Thus, recurrent studies will be needed for each measure, and tracking and reporting should be associated with a freshness indication, *referring to the date when the indicator was last assessed or computed* with a new analysis or study. Recency of the measures is particularly important when there has been a significant updating of components and connectivity of systems, even if the updates are aimed at increasing security or resiliency.

The objective is not that each of these metrics reach some specific threshold of quality, but rather for the measures and their values *to serve as assessments of the current state of affairs and to be used to focus attention and plans for action to remedy challenges to resiliency.* The assessments can be employed to track progress over time with improved cyber-physical resilience. The specific target values of these quantitative and qualitative assessments should be determined according to risk in the context of each organization, but under a universal goal that any measure should continuously improve.

Recommendation 1C: Commit to Radical Transparency and Stress Testing

Create a level of transparency that encourages every sector to improve outcomes, without setting specific targets in regulation or requiring other new authorities. This can be accomplished by designing creative mechanisms for designated systemically important entities to report their Cyber-physical-GAP metrics in appropriate ways.

Transparency in tracking and reporting of performance goals and outcomes is important for (a) intra-organizational alignment and communication, (b) for sharing externally to promote the learning and growth of other organizations, and (c) to provide incentives that assure energy and attention is invested on defining, collecting, and tracking meaningful metrics and outcomes.

SRMAs should provide a system for entities / organizations to voluntarily report their Cyber-physical-GAP metrics to their SRMA, and then for the SRMA to provide transparency to the broader public regarding something as simple as who has reported. The specific metrics can be kept confidential and only aggregated and disclosed under coordination of their Sector Coordinating Council. SRMAs should publish aggregate numbers for their sectors. Consideration should be given to publishing on performance.gov for public sector entities.

Transparency can enable benchmarking to help organizations share the most effective practices that lead to the best outcomes over time. This can incentivize participation as an important economic driver, since organizations that participate will be most able to identify the prioritization of investments that will most improve their overall cyber-physical resilience. Additionally, transparency can reveal how comparatively good or bad an organization is, which will help the SRMA prioritize the support it provides and identify incentives to help the worst improve. The best would be incentivized to stay the best. This pressure drives progress.

In addition to promoting voluntary reporting, recent incident reporting rules implemented by the Securities and Exchange Commission (SEC) may encourage self-correction. Separately, the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), which was passed into law in March of 2022, mandates that critical infrastructure entities report significant cyber incidents to CISA, which will enable CISA to leverage such information through alerts and advisories to proactively protect the larger critical infrastructure ecosystem. The Toxic Release Inventory, instituted in 1986 provides a useful case study on the value of public disclosure. This is the U.S. government's requirement that every factory releasing hazardous air pollutants report those emissions publicly every year. Communities can find out precisely what is coming out of the smokestacks and other facilities in their town, which compels actions from those plants and other facilities to self-remediate. Citizen outrage is good, but corporate shame can be even more effective at promoting improvement.

Additionally, we recommend driving organizations to develop an understanding of the limits of their resilience through **stress testing**. To that end, we recommend that CISA could work with the SRMAs to define an operational framework for cyber-physical resilience stress testing that can be adopted or adapted for use by SRMAs and associated sector regulators (as applicable). Stress testing should minimally include explicit validation of some of the metrics covered in recommendation 1b, specifically:

- Testing capabilities under conditions of simulated Internet failure for periods of at least 24 hours.
- Testing emergency management capability of physical infrastructure under manual control where Supervisory Control and Data Acquisition (SCADA) systems or other OT capabilities are not available for periods of at least 24 hours.
- Identifying the adequacy of supply chain stockpiles and buffers to cope with disruption.
- Testing of operational resilience under plausible but more severe scenarios, beyond the scope of existing expected events in current business continuity plans. These scenarios may not be as unlikely as risk planning hopes.
- Balancing Mean Time Between Failures (MTBF) and Mean Time to Repair/Recover (MTTR) noting that approaching 100% availability is equivalent to driving MTBF to infinity or MTTR to zero. In many complex and highly distributed cyber-physical systems a path of reducing MTTR is more optimal than reducing component MTBF.

(2) Bolster and Coordinate Research and Development

Goal:

Enable a national research and development effort to advance the state of the art in cybersecurity and cyber-physical resilience.

Setting the Scene

Research and development in cybersecurity and particularly cyber-physical resilience is fragmented and unfocused. We are not marshaling our academic and private sector R&D capabilities with the force we could, even as we see many advances in capabilities across hardware security, software security, formal analysis, AI, and many other disciplines.

The federal government should create increased impetus and focus to harness the wider research community to deliver more outcomes against a set of defined cyber-physical resilience grand challenges.

Recommendation 2A: Establish a National Critical Infrastructure Observatory

Ensure that our understanding of our critical infrastructure and its inter-dependencies is at least on par with or better than the understandings that our adversaries have. Ensure that we take into consideration U.S. intelligence about adversarial understanding of our infrastructure, including history of probes of infrastructure, so that we can test against likely capabilities for single and multipoint adversarial disruptions. The goal is to provide a platform where we can see our risks and deficiencies faster than our adversaries can. This observatory can also help us anticipate where natural disasters or accidents might have the most impact so we can mitigate in advance.

Our adversaries too often understand our critical infrastructure and its inter-dependencies better than we do. As part of increasing our awareness, we need to better map extended supply chains from customers to suppliers. Better supply chain mapping will help us to continuously identify dependencies, single points of failure, concentrations of capabilities in only one

service/supplier/product, or other issues. With AI we can enhance the analysis and sense-making of key issues waiting to be revealed by the observatory.

CISA's National Risk Management Center (NRMC) should work with a federally funded research and development corporation (FFRDC), a university affiliated research center, or national laboratory to collaborate with the private sector to develop a classified mapping system to inventory critical infrastructure and identify risks such as high reliance on specific technologies or resources ("critical concentration risks") and single point of failure risks. CISA, as the National Coordinator for critical infrastructure security and resilience, should proactively engage with SRMAs and SCCs (specifically the Sector Executive Councils introduced as part of these recommendations) to resolve any identified weaknesses revealed by the observatory, and collaborate with NSA's Cybersecurity Collaboration Center (CCC) to facilitate inclusion of the defense sector in the observatory. The key is to have a single national system that can support the overlay of key elements like active incidents, indications and warnings and act as a national virtual fusion environment for coordination.

Recommendation 2B: Formulate a National Plan for Cyber-Physical Resilience Research

Partner across federal agencies to define priorities and support research in those areas. The goal is to create focused research across programs that increase the likelihood of successful research results, but more importantly help ensure that such results will transition into actual use.

This goal can be accomplished by extending existing work of the NITRD Federal Cybersecurity Research and Development Strategic Plan.[31] We encourage the development of an interim annex to the 2023 report that broadens the scope to include cyber-physical resilience and an increased focus on coordinating cyber-physical relevant research efforts across all the NITRD member agencies and including academia and industry. We recommend that the strategic plan include a statement of grand challenges / hard problems on which to focus. We expect valuable focus areas could include:

- Definitions and study of foundational principles of resiliency of complex systems and designs for resilience.
- Defining uniqueness of cyber-physical systems and developing an ontology of research challenges and opportunities.
- Developing modeling and simulation tools for studying resiliency.
- Exploration of the use of AI methods by adversaries to employ, and defenders to thwart, multipoint and sequenced attacks within and across systems and sectors,
- Defining leading indicator metrics, and the automated assessment of metrics, such as those called out in Recommendation 1b.
- Developing digital twin simulation / security tools for critical systems and use-prognostics to model weaknesses.
- Develop tools for risk assessment that are easier to apply and use. For example, the ongoing improvements to the NIST Cybersecurity Framework 1.1 from 2018 should further simplify application of this framework.
- Develop common definitions, standards, and metrics for measuring effectiveness of infrastructure resilience interventions.

[31] National Science and Technology Council. (2023 December). Federal Cybersecurity Research and Development Strategic Plan.

- Develop approaches to enhance field upgradability of operational technology and improve legacy system management.
- Explore new techniques to adopt memory-safe programming, including migration of legacy code (e.g., C++) to memory-safe languages (e.g., Rust) with possibilities of leveraging capabilities of AI coding assistance to facilitate large-scale migration.
- Investigate chaos engineering as applied to security.
- Pursue mechanisms to apply segmentation, micro-virtualization, and zero trust technologies to ease the burden on defensive efforts.
- Explore crypto-agility technologies that may enable reliable and timely transition to post-quantum cryptography standards.
- Advance secure operating systems research for systems-on-a-chip technologies.
- Explore the use of AI to radically advance anomaly detection, especially to identify threats/attackers in low signal environments such as "living off the land" attacks.[32]

Recommendation 2C: Pursue Cross-ARPA Coordination

Create an overlay of cyber-physical resilience research across ARPAs to ensure focused research and effective implementation. The goal is to maximize the likelihood of successful research efforts by aligning or combining complementary research efforts.

We need to coordinate across the ARPAs (DARPA, IARPA, ARPA-I, ARPA-H, and HSARPA) on related efforts on cybersecurity and cyber-physical resilience research. Research outcomes could be accelerated if complementary efforts are aligned and focused, especially where there are opportunities for technology transfers to the private sector and other branches of government.

OSTP could form a Cross-ARPA coordination effort to regularly align efforts in the context of the proposed National Plan for Cyber-physical Resilience Research. This could be part of the cross-agency efforts of the NITRD program of the National Science and Technology Council. Cross-ARPA coordination would benefit from input from a selection of additional organizations including:

- NSA Cybersecurity Directorate (drawing in NSA Research Directorate as needed)
- CISA
- NIST
- National Science Foundation (NSF)
- FFRDCs in this space
- Idaho National Laboratory (INL) and other relevant National Lab efforts
- Select SRMAs
- Academic institutions with expertise in engineering and cybersecurity
- Select cybersecurity experts

The proposed cross-ARPA coordination would ideally include commissioning the development and codification of leading practices for engineering cyber-physical systems with a central emphasis on ensuring resilience. By considering insights from sources like NIST's Secure Systems Engineering and INL's Cyber-Informed Engineering, practices can be codified and measurable resilience attributes identified.

[32] Living off the Land attacks create malicious actions using software and functions available in the systems that are being attacked, making them difficult to detect.

Recommendation 2D: Radically Increase Engagement on International Standards

Engage international standards organizations and foreign stakeholders to ensure the U.S. more deeply drives standards across key technologies globally. This should include rapid advancement of programs to issue visas for appropriately vetted foreign nationals to attend U.S.-hosted standards meetings and other conferences, with the goal of stimulating even more local hosting and participation in global standards development. The goal is to drive standards closer to our cyber-physical resilience goals.

China and other nations are driving standards across an array of technologies. We are re-engaging but much more needs to be done.

This recommendation can be achieved quickly by enthusiastically accomplishing the goals described in the May 2023 U.S. National Standards Strategy for Critical and Emerging Technology.[33] PCAST particularly applauds Line of Effort #3 and encourages significantly more standards bodies meetings be hosted in the U.S. in the coming years and that the Department of State grant more timely visas to people seeking to attend these U.S.-hosted conferences and standards meetings.

Recommendation 2E: Embed Cyber-Physical Resilience Skills into Engineering Professions and Education Programs

Ensure cyber-physical risk and cyber-informed engineering (CIE) competency in engineering training across disciplines as well as ABET certification. The goal is to increase the professional workforce familiar with cyber-physical resilience tools. This will help build resilient systems from the start and thoughtfully improve the systems we have.

The focus on strengthening the cybersecurity workforce is evident in national and sector-specific education initiatives, including the National Cyber Workforce and Education Strategy.[34] While the National Cyber Workforce Coordination Group[35] has made commendable efforts to incorporate cybersecurity into early education, a crucial gap exists in equipping engineering professionals, including those in both information technology and operational technology, with the necessary skills to ensure cyber-physical resilience. To bridge this gap it is essential to enhance cyber-physical risk and cyber-informed engineering (CIE) criteria in engineering training across disciplines. A strategic call to action is recommended for accreditation bodies, universities, and cybersecurity education researchers to integrate cybersecurity and cyber-physical resilience criteria into relevant engineering, computer science, and IT engineering degree programs.[36, 37]

---

[33] White House. (2023 May). U.S. Government National Standards Strategy for Critical and Emerging Technology.
[34] White House. (2023 July). National Cyber Workforce and Education Strategy.
[35] NCWCG was established by ONCD in Dec. 2022 as noted in the National Cyber Workforce and Education Strategy.
[36] National Science Foundation. (2023 April). Dear Colleague Letter: Supporting Cybersecurity & Privacy Education and Workforce Development
[37] Special Interest Group Computer Science Education. sigcse.org

(3) Break Down Silos and Strengthen Government Cyber-Physical Resilience Capacity

Goal:

Ensure that all agencies and departments are equipped to drive resilience, focusing on the capabilities and authorities that position for rapid results.

Setting the Scene

Cyber-physical resilience, and within it, cybersecurity, continues to be a priority for the nation. The Biden-Harris administration has made significant strides in bolstering public-private sector partnerships while setting a tone of increased expectations from owners and operators of critical infrastructure.

The NSC has convened industry on topics such as Internet-of-Things and software supply chain security, and also put in place the first-ever mandates for multiple critical infrastructure sectors. Other notable developments included the release of a National Cybersecurity Strategy by the ONCD and the ongoing transformation of CISA, including its Joint Cyber Defense Collaborative (JCDC) and the Cyber Safety Review Board (CSRB). There is similar transformative work ongoing through the Critical Infrastructure Partnership Advisory Council (CIPAC), incorporating Sector Coordinating Councils and other constructs, that is increasing the operational tempo of public / private partnership.

It is because of this progress showing what can be done that we push for more to be done. Our recommendations are intended to amplify the great work happening so that we can achieve greater alignment, focus of effort, clear priorities, and ensure that SRMAs have the right authorities and capabilities to protect their sectors.

All agencies need to ensure that enhancing the cyber-physical resilience of the Nation's critical infrastructure is an integrated effort, working toward the goals of the Biden/Harris Administration's 2023 National Cybersecurity Strategy.[38] These efforts should include ensuring that agencies are effectively identifying and prioritizing each sector's most critical services, ensuring cross-sector coordination exists to protect critical services that depend on each other, that the staffing capacity and capability of the cyber-physical resilience teams in agencies meets mission need, and that SRMAs have the requisite authorities or can influence regulatory capacity to ensure sustained private sector focus. These recommendations should be incorporated into a potential successor policy to PPD-21.

Recommendation 3A: Establish Consistent Prioritization of Critical Infrastructure

Create a clear understanding of what our most critical functions, dependencies, and supporting systems are so we can focus efforts and resources appropriately. Create impetus for a more integrated and continuously updated process for infrastructure prioritization across government / SRMAs. This can be accomplished by establishing a clear rationale for specific prioritizations in the National Essential Functions / National Critical Functions / Systemically Important, or other prioritization frameworks.

[38] White House (2023 March). National Cybersecurity Strategy.

CISA has an opportunity to establish a clear and canonical national and sector-by-sector list of Systemically Important Entities that underpin the National Critical Functions, including which organizations and entities and which systems are part of the critical functions and for what reason. The National Risk Management Center (NRMC) is wellpositioned to use this clarification to help organizations understand their important roles. The Systemically Important Entities list will need to be reviewed periodically and revised as needed. It should be analyzed to detect and resolve cross-sector discrepancies, i.e., functions not designated as critical in one sector but depended on by functions in other sectors that are critical. The intra-sector prioritization framework will need to align with the overall National Critical Functions but have enough flexibility for each sector's specific needs and be aligned with the National Defense Authorization Act (NDAA)-required agency driven risk assessments. The process will ideally seek to identify intra- and inter-sector common-mode failures i.e., failure points that could have widespread effects.

To achieve the goal of identifying and supporting the organizations that are part of the National Critical Functions list, it will be essential to designate which private sector organizations are systemically important to supporting those national critical functions. We recommend that CISA establish a methodology to identify critical technology products/service providers and SRMAs use that methodology to identify and designate technology service providers that provide critical capabilities as systemically important organizations also. The National Critical Functions will also need to be reconciled with FEMA Mission Areas and Core Capabilities.

Recommendation 3B: Bolster Sector Risk Management Agency Staffing and Capabilities

Ensure SRMAs are capable of working in and across their sectors to drive needed national cyber-physical resilience outcomes. This will require achieving minimum capabilities (expertise, staffing levels, and authorities) for SRMAs to perform cybersecurity and cyber-physical resilience mission responsibilities already codified in 6 U.S.C. § 665(d). Increase SRMA intelligence processing capabilities and partnerships with the Intelligence Community (IC) to ensure more timely distribution of information that allows proactive steps across each sector.

This recommendation builds on the June 2023 OMB and ONCD Memo instructing agencies to consider budget requests with cybersecurity goals and objectives in mind, including staffing requirements. This recommendation also builds on the August 2023 OMB and OSTP Memo which notes that, "Agencies should fund world-leading research, development, and innovation activities that: […] Mitigate cybersecurity risks through resilient architectures; building in security by design; strengthening security and resilience for critical infrastructure, and integrating social, behavioral, and economics research." The fact that PCAST is also highlighting the challenges of inadequate SRMA staffing and capabilities points to the continuing challenge of marshaling these essential resources.

NSC in partnership with ONCD and CISA, as the National Coordinator for critical infrastructure security and resilience, should evaluate and define, as we believe they are doing as part of the development of a PPD-21 successor policy, what constitutes an effective SRMA. This should include:

1. Ensuring sufficient staffing levels and skills / capabilities to enact the responsibilities of an SRMA.

2. Establishing the reporting line of the lead official of the SRMA to be at a sufficiently senior executive level.
3. Broadening focus beyond cybersecurity to explicitly include resilience overall, and specifically cyber-physical resilience. Consequently, strategic objectives and performance goals should be stated primarily in resilience terms. Additionally, while we need national cyber-physical resilience (and related pure cybersecurity) performance goals, it is important that there are also sector-specific goals and metrics that capture the precise risks and needs of that sector.
4. Ensuring that the lead official of the SRMA has visible support of the Cabinet Secretary to direct the activities of that sector's Government Coordinating Council and to be able to marshal the executive leadership from representative private sector owners/operators in that sector—to encourage them to take leadership roles in their Sector Coordinating Council's newly constructed Executive Council.
5. Formally defining the relative roles and responsibilities of that agency to:
    a. Marshal support from CISA for common services like incident response, vulnerability assessments, and other elements delivered from programs like the JCDC.
    b. Establish intelligence requirements and operational usage, in partnership with the intelligence community, for example: NSA CCC and DHS Intelligence & Analysis.
    c. Be subject to sufficiently independent oversight from the CISA National Coordinator function.

We note that CISA has been resourced and authorized to fulfill the SRMA roles for many sectors (for example: Communications and IT, Emergency Services, chemical, and others). CISA has taken on this responsibility and executed it well, and has delivered significant progress in those sectors on cybersecurity and in some cases physical security. We encourage their increased focus on resilience and specifically cyber-physical resilience to build on this.

However, we want to call to attention the structural issue that exists in government, where each of our 16 critical infrastructure sectors is not sufficiently covered by a dedicated cabinet agency. Some like the Dept. of Treasury and Dept. of Energy have mature and growing SRMA functions (although they could benefit from more resources), while other agencies are still maturing their teams and should be better resourced. Some sectors are regulated by organizations like the Federal Communications Commission or the Nuclear Regulatory Commission, that are independent from the executive branch and therefore cannot serve as an SRMA. Nevertheless, those organizations could valuably broaden efforts to include more focus on cyber-physical resilience, providing sector-specific insights to supplement CISA's SRMA role for those sectors.

Recommendation 3C: Clarify and Strengthen SRMA Authorities

Identify the authority gaps between federal and state, local, tribal, and territorial (SLTT) responsibilities to be sure that legislators and regulators understand what is required for each critical infrastructure in any location to achieve the minimum required cyber-physical resilience. Gaps may include legislative gaps and shortfalls in sector-specific regulation.

Early on in the Biden Administration, the NSC identified numerous gaps in the required legislative authorities for SRMAs in different sectors. The Biden Administration proceeded to address many of them by fully utilizing existing regulatory authorities (specifically for the pipelines, air, rail, and water

critical sectors). Nevertheless, not all sectors have mandates for minimum cybersecurity practices, notably those where CISA is currently acting as SRMA. These gaps in authorities limit the ability to assure critical infrastructure owners and operators adhere to cyber-physical resilience (including, by definition, cybersecurity) requirements and goals. We recommend that ONCD undertake an SRMA review to assess the role of agencies, CISA, and independent commissions to identify opportunities for improvement as part of overall resource plans. The goal will be to ensure that agency heads and budget processes assign or prioritize the budget needed to fulfill SRMA requirements. Indeed, just clarifying what is spent on SRMA efforts in each agency and organization, rather than lumping SRMA efforts into a broader category, would valuably help clarify which efforts may be limited by insufficient staff or other resources.

PCAST recommends that under the leadership of ONCD, DHS should engage with Congress on new powers that are needed to fill gaps in SRMA's authority. This includes mandating minimum practices and outcome measurements that advance resilience and cybersecurity. Additionally, efforts to enhance resilience and cybersecurity should continue to build upon and ensure permanence of NSC-established mandates including the following:

- **Pipelines**. Initial Security Directive: June 9, 2022, Latest Modification: July 26, 2023.[39]
- **Rail**. Initial Security Directive: June 9, 2022, Latest Modification: October 23, 2023.[40]
- **Aviation**. Emergency Amendment for Airport and Aircraft Operators: March 7, 2023.[41]
- **Water Systems**. Cybersecurity rules for water systems put in place in March 2023 were withdrawn in October 2023[42] under Department of Justice (DOJ) guidance to the EPA after three state attorneys general sued. The Administration should continue to work with Congress on new authorities for EPA to resolve this issue.
- **Ports**. The February 12, 2013 Executive Order 13636[43] asserted that cybersecurity standards for ports and other infrastructure should progress to more effectively counter significant cyber threats from criminals and adversarial nation-states. Potential obstacles to military mobilization and deployment demand the greatest attention. The United States Coast Guard echoes a similar sentiment in its Cyber Strategic Outlook published in August of 2021.[44]
- **Hospitals**. The Centers for Medicare and Medicaid Services (CMS) will need to continue its efforts to improve cyber-physical resilience by developing new incentives or adjusting the Conditions of Participation to ensure hospitals act with speed to improve cybersecurity.

ONCD is well placed to work with leads at CISA to develop an integrative "Gaps and Challenges'' report for each critical infrastructure category. This collaborative effort would identify where

[39] DHS Transportation Security Administration. (2023 July 26). Renewal with revision to the Security Directive (SD) Pipeline-2021-02 series: *Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing* [Memorandum].
[40] DHS Transportation Security Administration. (2023 October 23). Renewal with revisions to the Security Directive 1580-21-01 series: Enhancing Rail Cybersecurity [Memorandum].
[41] DHS Transportation Security Administration. (2023 March 3). TSA issues new cybersecurity requirements for airport and aircraft operators [Press Release].
[42] Environmental Protection Agency. (2023 October 11). Withdrawal of Cybersecurity Memorandum of March 3, 2023 [Memorandum]. (Alternative link).
[43] Executive Order 13636, 78 FR 11739. (2013 February 12). "Improving Critical Infrastructure Cybersecurity".
[44] United States Coast Guard. (2021 August). Cyber Strategic Outlook.

minimum practices and outcomes should be mandated and also establish where requirements for metrics and measures are needed. Subsequently, the report should be disseminated to pertinent operational organizations and agencies, as well as to leads at NSC, Sector-Specific Risk Management Agency (SRMA) heads, as well as law enforcement and the intelligence community so that they can understand where and why critical infrastructure may not be achieving the minimum standards needed for reliable and resilient functioning.

Recommendation 3D: Enhance the DHS Cyber Safety Review Board

The Cyber Safety Review Board (CSRB) should be empowered and staffed to do more reviews, identify more causal factors, and improve indicators and warnings that will protect cyber and cyber-physical systems. The goal is for the CSRB to help the many systems that could have been impacted learn from every major event or close call.

CISA should seek sufficient Congressional authorities and resources for the CSRB to enable it to:

- Conduct more frequent reviews, and orient those to cyber-physical resilience consequences and causal factors. For example, the FAA outage of 2023 is an example of a need to examine an incident not just from the frame of how the system failed but, more importantly, to consider how system-wide brittleness led to such widespread consequences when one system did fail.
- Possess a staff of full-time investigators and a committee of overseers or commissioners. The CSRB staff will need to be sufficiently independent from the sectors and government systems that might be the subject of CSRB reviews to conduct an impartial evaluation, but still possess sufficient expertise to effectively guide the reviews and frame the outputs of investigations. A robust recusal process could help facilitate the needed expertise if such overseers must be drawn from specific industries.
- Partner with SRMAs, sector regulators, Sector Coordinating Councils, and Sector Information Sharing and Analysis Centers (ISACs) to improve sharing of identified themes.
- Include close-calls / near-misses in reviews to examine the risk of potentially large events occurring in the future—i.e., identify where we just got lucky in having limited impact.
- Partner with the Federal Cyber Centers (e.g., National Cyber Investigative Joint Task Force, National Cybersecurity and Communications Integration Center, National Threat Operations Center) to identify additional sources of incidents for potential review.
- Subpoena authority would enhance the CSRB's ability to assess root causes.

(4) Develop Greater Industry, Board, CEO, and Executive Accountability

Goal:

Aim to assure that systemically important and other critical private sector organizations are accelerating and prioritizing cyber-physical resilience work as if their survival depended on it—as it indeed does.

Setting the Scene

The bulk of our national critical infrastructure is owned and operated by the private sector. To ensure the reliability of that infrastructure, the federal government must engage boards, CEOs, and other executive leadership more deeply, directly, and collaboratively in sector risk management activities.

Government continues to foster crucial public / private partnership and is increasingly effective at developing shared outcomes. White House summits have prompted extensive private sector action and commitments. CISA has an excellent drive toward secure by design and secure by default approaches, and many SRMAs are supporting sector exercises and vulnerability resolution through their SCCs and Sector ISACs.

However, there are still extensive vulnerabilities, security issues, and pervasive cyber-physical resilience challenges across our critical infrastructure. This has many causes including the challenges of legacy systems, inadequate funding and incentives for technology modernization, shortfalls in workforce expertise, and lack of security and resilience by design approaches in building organizations' processes and technology.

One significant limit to resilience is the extent to which boards, CEOs, and other executives turn their responsibility and accountability into actual action. True resilience requires long term focus and prioritization of organization-wide resources, not just a good security team.

The federal government should employ existing frameworks, and, where necessary, establish new approaches, to more deeply and directly engage boards, CEOs and executives of private sector organizations and other infrastructure owners / operators. The objective of this engagement is to bolster each organization's cyber-physical resilience as well as to increase intra- and inter-sector collaboration to defend the Nation's infrastructure. We appreciate that boards, CEOs, and executives have a myriad of priorities, but cyber-physical resilience is so fundamental to the functioning of their organizations and the Nation that we believe it merits significant personal engagement and leadership.

Recommendation 4A: Enhance Sector Coordinating Councils (SCC)

Drive private sector infrastructure companies to articulate strategies to improve their cyber-physical resilience. This can be accomplished by ensuring that each SCC has established a Sector Executive Committee to manage and coordinate council activities under the Critical Infrastructure Partnership Advisory Council (CIPAC). Existing councils / sub-councils, devoted to specific work, can be made up of CIOs, CISO/CSOs, and other leaders that currently do the work in SCCs. This elevated engagement of executives in SCCs should be complemented with an increase in the seniority of membership in the corresponding Government Coordinating Council (GCC).

CISA should work with SRMAs to establish or strengthen Sector Executive Committees for each of the 16 critical infrastructure sectors such that each Committee is composed of organization CEOs or equivalent executive leaders, and/or a designated board member. This top-level Sector Executive Committee could oversee the efforts of one or more sub-sector councils, which would continue to be more operationally and technically engaged in important sector-wide security and cyber-physical

resilience issues. We appreciate that the government currently has no direct authority to dictate the composition of SCCs, so we expect that this recommendation will require agency head / principals to reach out to executives at organizations. We believe the private sector will be responsive to this call to action, especially as benefits to them and their sector are articulated.

Membership of the Sector Executive Committee should be constructed to represent a broad subset of the organizations in a particular sector, balancing large and small organizations, periodically rotating membership, and including all the types of owner / operator organizations that may be present in that sector. The goal should direct senior / executive leader engagement in addition to existing security leaders, trade associations, and government affairs team engagement.

Community engagement plans that support relevant industry initiatives and promote public / private partnerships on cyber-physical resilience or related cybersecurity issues can be developed by updating the National Infrastructure Protection Plan[45] and the SRMA sector-specific plans. This engagement and cooperation should also include not-for-profit organizations dedicated to enhancing security capabilities, for example, the Open Source Security Foundation.

SRMAs authorities may not currently facilitate engagement with CEOs and boards, but agency heads and other principals have tremendous convening power and relationship capital with leaders of private sector organizations in their sectors, which can be utilized to enhance shared goals.

Recommendation 4B: Promote Supply Chain Focus & Resilience by Design

Improve cyber-physical resilience among the shared service providers who provide the technology underpinnings of many sectors with the goal of hitting the "80/20" mark—that is, improve the security and resilience of the 20% of technology that can reduce risk for 80% of the systems. This can be accomplished if SCCs for each sector can identify and prioritize the technology service providers and product vendors that are most frequently used for critical tasks in that sector.

A small number of service providers may provide capabilities to nearly every organization in a sector. This is a risk, but is also an opportunity—a leverage point. We recommend that CISA develop a methodology and work with SRMAs to identify, for each sector, the technology service providers and product vendors (including IT and OT) that represent over 20% of the service provision "concentration" in a particular sector. SRMAs could request Sector Coordinating Councils convene those organizations to define and publish a charter for the long-term improvement of cyber-physical resilience according to accepted Security-by-Design and -Default principles, building on those defined by CISA in April 2023.[46] This should include:

- Enhancing vulnerability disclosure and rewards (a.k.a. "bug bounty") programs to explicitly include a new concept of "brittleness bug bounties" to encourage and reward the identification of cyber-physical resilience issues and security issues.
- Publishing a secure by design and secure by default roadmap including "attack surface" reduction.

[45] U.S. Department of Homeland Security. National Infrastructure Protection Plan. (Accessed 2024 February).
[46] Cybersecurity & Infrastructure Security Agency. (2023 April 13). U.S. and International Partners Publish Secure-by-Design and -Default Principles and Approaches.

- Pushing service providers and technology vendors to publish software bills of materials (SBOMs) and vulnerability exploitability exchange (VEX) information that provides security advisory information about known vulnerabilities. Vendors should also publish Supply Chain Levels for Software Artifacts (SLSA) to recipients of their shipped products, which provides a checklist of standards and controls to prevent tampering and improve product integrity and security.
- Partnering between SRMAs, sector service providers, and relevant industry foundations to improve the security of open-source product components (e.g., Open Source Security Foundation).
- Pushing vendors to commit to field upgradability to help organizations improve the interoperability and long-term resilience of their legacy systems.

The identification and involvement of widely used service and technology providers should be organized so as to not violate any laws or be deemed to be offering any preferential treatment to those vendors. Rather the goal is to expect more of them.

Appendix C: External Experts Consulted

Our working group sought input from a diverse group of additional experts and stakeholders. We are grateful to many who shared their insights and guidance at different phases of the study, from research and discovery to the formulation and review of recommendations. Experts did not review drafts of the report, and their willingness to engage with PCAST on specific points does not imply endorsement of the views expressed herein. Responsibility for the opinions, findings, and recommendations in this report and for any errors of fact or interpretation rests solely with PCAST.

Morgan Adamski
Chief of Cybersecurity Collaboration Center
National Security Agency

David Alexander
Co-Chair, Resilience Science and Technology Subcommittee
National Science and Technology Council

Bob Bastani
Senior Adviser for Critical Infrastructure Cybersecurity
Administration for Strategic Preparedness and Response
Department of Health and Human Services

Mark Billinger
Supervisory IT Specialist
Department of Health and Human Services

Andrew Bochman
Senior Grid Strategist
Idaho National Laboratory

Deb Bodeau
Senior Principal Cybersecurity Engineer
MITRE

Austin Bonner
Deputy U.S. Chief Technology Officer for Policy
The White House Office of Science and Technology Policy

Mary Brazier
Director of Mission Assurance, Office of the Secretary of Defense for Policy
Department of Defense

Clara Bulux
Incident Coordinator and Regional Coalition Liaison Department of Treasury

Vint Cerf
Vice President and Chief Internet Evangelist
Google

Frank Cilluffo
Director, Institute for Cyber and Critical Infrastructure Security
McCrary Institute, Auburn University

Ewa Clark
National Counterintelligence Officer Critical Infrastructure
National Counterintelligence and Security Center

Chris Clearfield
Co-Founder
The Clearfield Group

Valerie Cofield
Chief Strategy Officer
Cybersecurity and Infrastructure Security Agency

John Cohen
Executive Director of the Countering Hybrid Threats Program
Center for Internet Security ISAC

Kathryn Condello
Senior Director, National Security/Emergency Preparedness
Atlantic Council

Todd Conklin
Deputy Assistant Secretary, Office of Cybersecurity and Critical Infrastructure Protection
Department of Treasury

Kimberly Denbow
Vice President, Security and Operations and Acting Executive Director
Downstream Natural Gas ISAC
American Gas Association

Chris DeRusha
Senior Cybersecurity Analyst
The White House Office of Management and Budget

Jen Easterly
Director, Cybersecurity and Infrastructure Security Agency
Department of Homeland Security

Paul England
Software Architect
Microsoft

Kathleen Fisher
Director
Defense Advanced Research Projects Agency

Sarah Freeman
Senior Advisor on Patient Safety Policy and Industrial Control Systems Cybersecurity Analyst
Idaho National Laboratory

John Galer
Chief of Government Relations
The Aerospace Corporation

Gregory Garcia
Executive Director, Cyber Security
Health Sector Coordinating Council Cybersecurity

Eric Goldstein
Executive Assistant Director for Cybersecurity
Cybersecurity and Infrastructure Security Agency

Jeff Gottschalk
Assistant Division Head, Cyber Security and Information Sciences
Lincoln Labs
Massachusetts Institute Technology

Jeff Greene
Senior Director, Cybersecurity Programs
Aspen Institute

William Henagan
Director, Critical Infrastructure
National Security Council

Edwin Hirleman
Professor of Mechanical Engineering and Executive Director for International Advancement
Purdue University

LeAnne Jackson
Co-Chair of the Food and Agriculture Sector Government Coordinating Council
Food and Drug Administration

Debra Jordan
Chief, Public Safety and Homeland Security Bureau
Federal Communications Commission

Steven Kelly
Special Assistant to the President and Senior Director for Cybersecurity and Emerging Technology
National Security Council

Puesh Kumar
Director, Office of Cybersecurity, Energy Security, and Emergency Response
Department of Energy

Michael Lashlee
Chief Security Officer, Certified Information Systems Security Professional
Mastercard

Nicholas Leiserson
Assistant National Cyber Director for Cyber Policy and Programs
Office of National Cyber Director

Suzanne Lemieux
Director, Operations Security and Emergency Response Policy
American Petroleum Institute

Thomas Littleton
Director of Cyber Security and Commercial Space
Department of Transportation

Francesca Lockhart
Cybersecurity Clinic Program Lead
Strauss Center for International Security and Law
University of Texas at Austin

Will Loomis
Assistant Director, Cyber Statecraft Initiative
Atlantic Council

Adrienne Lotto
Senior Vice President of Grid Security, Technical and Operations Services
Electricity Sub-sector Coordinating Council

Keith Marzullo
Dean, College for Information Studies
University of Maryland

Pauline Matthews
Policy Analyst, Office of Cybersecurity and Critical Infrastructure Protection
Department of Treasury

Brian Mazanec
Deputy Assistant Secretary, Intelligence, Security, and Information Management
Administration for Strategic Preparedness and Response
Department of Health and Human Services

Therese McAllister
Community Resilience Group Leader
Materials and Structural Systems Research Division
National Institute of Standards and Technology

Erin Miller
Executive Director, NCC
Space ISAC

Mark Montgomery
Executive Director
Cyberspace Solarium Commission

Kevin Morley
Manager, Federal Relations
American Water Works Association

Jonathan Murphy
Director, Critical Infrastructure Cybersecurity
National Security Council

William Nelson
Chair
Global Resilience Federation

Anne Neuberger
Deputy National Security Advisor for Cyber and Emerging Technology
The White House

Maggie O'Connell
Director of Security, Reliability, and Resilience
Interstate Natural Gas Association of America

Mark Orsi
Chief Executive Officer
Global Resilience Federation

Ronald Pavlik
Surface Operations Deputy Assistant Administrator
Transportation Security Administration

Jennifer Pedersen
Senior Technical Advisor
Department of Homeland Security

Nicholas Polk
Director for the Center for Quality
Senior Advisor, Federal Chief Information Security Officer
The White House Office of Management and Budget

Austin Randazzo
Associate Bureau Chief, Public Safety and Homeland Security Bureau
Federal Communications Commission

Russell Richardson
Vice President and Chief Security Officer
Calpine Corporation

Aaron Rinehart
Global Cybersecurity Leader
Security Chaos Engineering
Verica

Eric Rollison
Assistant Director, Risk Analysis, Resilience, and Recovery
Office of Cybersecurity, Energy Security, and Emergency Response
Department of Energy

Randy Rose
Senior Director, Operations and Intelligence
Center for Internet Security

Ron Ross
Computer Scientist and Fellow
National Institute of Standards and Technology

Megan Samford
Nonresident Senior Fellow
Atlantic Council

Matthew Scholl
Chief, Computer Security Division
National Institute Standards and Technology

Ryan Schrader
Energy Industry Specialist
Office of Cybersecurity, Energy Security, and Emergency Response
Department of Energy

Suzanne Schwartz
Director of the Office of Strategic Partnerships and Technology Innovation
Food and Drug Administration

Brian Scott
Deputy Asst. National Director for Cyber Policy and Programs
Office of National Cyber Director

Yossi Sheffi
Director of the MIT Center for Transportation and Logistics,
Director of the MIT Supply Chain Management Program
Professor, Civil and Environmental Engineering
Massachusetts Institute Technology

Kelly Shortridge
Security Chaos Engineering
Senior Principal, Office of the Chief Technology Officer
Fastly

Lucian Sikorskyj
Senior Director, Resilience and Response
National Security Council

Steven Silberstein
Chief Executive Officer
Financial Services Information Sharing and Analysis Center

Joshua Silverstein
Senior Counselor and Policy Adviser
Office of Strategy, Policy, and Plans
Cybersecurity Infrastructure Security Agency

Hailey Siple
Director, National Security Policy
Electricity Subsector Coordinating Council

Christopher Sledjeski
Senior Principal, Cyber Infrastructure Protection Innovation Center
MITRE

Suzanne Spaulding
Senior Adviser, Homeland Security
International Security Program
Center for Strategic and International Studies

Amanda Sramek
Senior Manager, Security
American Gas Association

Shane Steiger
Principle Cybersecurity Engineer
MITRE

Nushat Thomas
Cybersecurity Branch Chief
Environmental Protection Agency

Natalie Thompson
Risk and Resilience Analyst Berkshire Hathaway

David Travers
Director, Water Security Division
Environmental Protection Agency

Zachary Tudor
Associate Laboratory Director
Idaho National Laboratory

Steve Welby
Deputy Director, National Security
The White House Office of Science and Technology Policy

Timothy Weston
Director, Strategy and Risk
Transportation Security Administration

Tarah Wheeler
Chief Executive Officer
Red Queen Dynamics

Craig Wiener
Technical Fellow
MITRE

Jessica Wilkerson
Senior Cyber Policy Advisor
Food and Drug Administration

Andrew Wills
Senior Advisor of Staff
Office of Cybersecurity, Energy Security, and Emergency Response
Department of Energy

Mara Winn
Deputy Director for the Preparedness, Policy, and Risk
Office of Cybersecurity, Energy Security, and Emergency Response
Department of Energy

Guido Zarrella
Research Program Leader
Decision Science and Senior Principal
Artificial Intelligence Engineer
AI and Autonomy Innovation Center
MITRE Labs

Appendix D: Acronyms

AI	artificial intelligence
ABET	Accreditation Board for Engineering and Technology, Inc.
ARPA	Advanced Research Projects Agency
CCC	Cybersecurity Collaboration Center
CIE	cyber-informed engineering
CIPAC	Critical Infrastructure Partnership Advisory Council
CISA	Cybersecurity and Infrastructure Security Agency (of DHS)
CMS	Centers for Medicare and Medicaid Services
CSRB	Cyber Safety Review Board
DARPA	Defense Advanced Research Projects Agency
DHS	Department of Homeland Security
DOJ	Department of Justice
FAA	Federal Aviation Administration
FEMA	Federal Emergency Management Agency
FFRDC	federally funded research and development center
FMF	Frontier Model Forum
GAP	generally accepted performance
GCC	Government Coordinating Council
HSARPA	Homeland Security Advanced Research Projects Agency
IARPA	Intelligence Advanced Research Projects Agency
IC	intelligence community
INL	Idaho National Laboratory
ISACs	Information Sharing and Analysis Centers
IT	information technology
JCDC	Joint Cyber Defense Collaborative
MTBF	mean time between failures
MTTR	mean time to repair/recover
NDAA	National Defense Authorization Act
NIST	National Institute of Standards and Technology
NITRD	Networking and Information Technology Research and Development (program of the NSTC)
NRMC	National Risk Management Center
NSA	National Security Agency
NSCAI	National Security Commission on AI
NSF	National Science Foundation
NTSB	National Transportation Safety Board
NSTC	National Science and Technology Council
ONCD	Office of the National Cybersecurity Director
OSTP	Office of Science and Technology Policy
OT	operations technology
PAI	Partnership on AI
PCAST	President's Council of Advisors on Science and Technology
R&D	research and development

SBOM	software bill of materials
SCADA	supervisory control and data acquisition
SCC	Sector Coordinating Councils
SLSA	supply chain levels for software artifacts
SLTT	state, local, tribal, and territorial
SRMAs	Sector Risk Management Agencies
SSDF	Secure Software Development Framework
TSA	Transportation Security Administration
UARC	university affiliated research center
VEX	Vulnerability Exploitability Exchange

Acknowledgments

The Cyber-Physical Resilience Working Group and greater members of PCAST wish to thank the insightful and helpful staff at the White House Office of Science and Technology Policy (OSTP), leaders at the National Security Council, and the Office of the National Cyber Director for their contributions to our understandings and thinking throughout the preparation of this report. We wish to thank the Institute for Defense Analyses (IDA) Science and Technology Policy Institute (STPI) team, especially Christopher Cannizzaro, for assistance with research and analysis. We also thank our many colleagues who provided insights in addition to the formal consults listed in Appendix C, including:

- Fahad Abdulrazzaq
- Chris Buthe
- Dawn Cappelli
- Sheila Casserly
- Danell Castro
- Caitlin Clarke
- Cassie Crossley
- Ernie Edmonds
- Jason Ellis
- Robert Erbacher
- Annie Fixler
- Marcus Fowler
- Andrew Ginter
- Colin Gounden
- Steve Griffing
- Frank Honkus
- Maxine Inman
- Danno Kay
- Kelley Kiernan
- Alexander Kott
- Max Lesser
- Bryan Owen
- Travis Parker
- Steve Pitcher
- Lala Qadir
- Stephen Raio
- Sidney Smith
- Randi Tomasek
- Michael Weisman
- Joe Weiss