Public Meeting of the

President’s Council of Advisors on Science and Technology (PCAST)

November 9, 2022

Meeting Minutes

Meeting Participants

PCAST Members

1. Frances Arnold, Co-Chair
2. Arati Prabhakar, Co-Chair
3. Maria T. Zuber, Co-Chair
4. Dan E. Arvizu
5. Dennis Assanis
6. John Banovetz
7. Frances Colón
8. Lisa A. Cooper
9. John O. Dabiri
10. William Dally
11. Sue Desmond-Hellmann
12. Inez Fung
13. Andrea Goldsmith
14. Laura H. Greene
15. Paula Hammond
16. Eric Horvitz
17. Joe Kiani
18. Jon Levin
19. Steve Pacala
20. Saul Perlmutter
21. William Press
22. Penny Pritzker
23. Jennifer Richeson
24. Vicki Sato
25. Lisa Su
26. Kathryn Sullivan
27. Terence Tao
28. Phil Venables
29. Catherine Woteki

PCAST Staff

1. Lara Campbell, Executive Director
2. Reba Bandyopadhyay, Deputy Executive Director
3. Sarah Domnitz, Principal Deputy Executive Director and PCAST Designated Federal Officer
4. Bich-Thuy Sim, Assistant Director for Health Policy Innovation
5. Kevin Johnstun, Research Analyst
6. Quinn Anex-Ries, White House Intern

Invited Speakers (in order of presentation)

1. Solomon Hsiang, University of California, Berkeley
2. Alice Hill, Council on Foreign Relations
3. Carlos Martín, Harvard University and The Brookings Institute

4. Deb Bodeau, MITRE
5. Therese P. McAllister, National Institute of Standards and Technology
6. David Mussington, Department of Homeland Security
7. Jim Platt, Department of Homeland Security
8. Kathleen Fisher, Defense Advanced Research Projects Agency

START DATE AND TIME: WEDNESDAY, NOVEMBER 9, 2022, 11:15 AM Eastern Time

LOCATION: Virtual Meeting via Zoom.gov

WELCOME

PCAST Co-chairs: Frances Arnold, Arati Prabhakar, Maria Zuber

The PCAST co-chairs—Frances Arnold, Arati Prabhakar, and Maria Zuber—called the public session to order.

SESSION: FINANCIAL IMPACTS OF EXTREME WEATHER

Arnold introduced the first session by noting that climate change is amplifying the frequency and severity of extreme weather events with ever-greater loss of life, damage to property, and destruction of American communities. The rising rate of extreme weather events also affects Americans in terms of depreciating property values and increasing costs for insurance, and this pattern has major implications for local governments and for the federal funding needed for adaptation and resilience.

Solomon Hsiang, University of California, Berkeley

Solomon Hsiang began his presentation by noting that Hurricane Maria undid approximately two decades of economic progress in Puerto Rico in just 12 hours. The devastation in Puerto Rico had a greater negative economic effect than the Great Recession of 2007-2009 had on Nevada, Arizona, and Michigan, which were among the hardest hit states during the Great Recession. The United States, said Hsiang, is particularly vulnerable economically to extreme events because it spends less per capita to protect its infrastructure and people compared to countries like Japan and Australia.

Climate change, said Hsiang, is a distribution shift in the types of extreme weather events that the nation will experience. Data on daily temperatures and income per capita for U.S. counties shows that, between the 1980s and 2010, economic activity in U.S. counties decreased as daily temperatures increased. This effect, he added, has been observed worldwide. Current models project that people who live in warm or temperate locations will face increased health impacts as temperatures rise, which affect both wellbeing and financial costs. Extreme temperatures even affect the development of children over the long term. In the United States, extreme fluctuations in temperatures are strongly associated with self-harm, suicide rates, and increases in violence.

Hsiang said that the fiscal costs of an extreme weather event go beyond disaster relief payments from the Federal Emergency Management Agency (FEMA). The costs include increased outlays from unemployment insurance, Medicare and Medicaid, income maintenance programs such as food stamps and supplemental Social Security, as well as foregone earnings that will affect retirement benefits. Extreme weather events can also cause property values to decline. Financial risks from extreme weather events, he added, are not distributed equally, with low-income populations bearing the largest costs, which means that climate change is likely to increase preexisting economic inequality.

The United States, said Hsiang, does not have a good system for overseeing the development and deployment of adaptation technologies or data. For example, financial institutions are now using proprietary datasets to reprice mortgages, but there is no federal oversight to ensure these datasets are accurate. Similarly, there are methods for estimating the social cost of greenhouse gases used to inform the public, but a system for reevaluating this figure needs to be codified and systematized in a way that does not introduce additional volatility into the market. Hsiang suggested that the federal government could index budgets and financial systems against climate change to ensure fiscal sustainability. Ad hoc discretionary risk management systems, such as presidential disaster declarations, are not guaranteed to be financially sustainable and should have a sunsetting provision. Moreover, adaptation to climate change will occur in a decentralized manner, so coordination failures will be costly, Hsiang said in closing.

Alice Hill, Council on Foreign Relations

Alice Hill said most policymakers do not have the training or knowledge background to understand all of the economic costs associated with climate change, such as disruptions to supply chains and missed healthcare appointments that lead to poorer health outcomes. She listed five areas for which the Biden-Harris administration could make quick progress, with some requiring congressional action:

1. Shore up infrastructure to prepare for future, rather than historic, climate conditions. This should include developing climate-resilient building codes and standards, spending money from the Inflation Reduction Act in a climate-resilient manner, preparing for cascading failures, and adjusting cost-benefit analysis to value the extra investment needed to build climate-resilient infrastructure.

2. Develop property insurance solutions that are actuarially sound, include risk mitigation, have longer coverage periods, require stress-testing insurers, and reduce federal subsidies for at-risk areas.

3. Attend to security risks by strengthening the nation's emergency response system, enhancing assistance for community disaster planning, and identifying and supporting areas for migration.

4. Develop a national adaptation plan that would provide goals for adaptation, roles and responsibilities, metrics for measuring adaptation, and spending priorities.

5. Develop a trained workforce that has the skills necessary to devise and implement climate adaptation plans.

Carlos Martín, Harvard University and The Brookings Institute

Carlos Martín noted that Hurricane Katrina, aside from being the costliest extreme weather event in the United States, had a huge effect on households and communities. At the household level, there were deaths, adverse effects on physical and mental health, job losses, gaps or changes in children's schooling, changes in social networks, and relocation expenses. He said that U.S. disaster policy is based on property, not people, so these impacts are inequitably distributed by a range of demographic traits, including financial wealth.

Martín said he has examined the financial effects of disasters of different severity on different populations and found that the negative effects that disasters have on households, such as lowering credit scores, persist and even grow over time. The initial decline in credit scores, for example, leads to higher costs for credit and other financial services that can limit a household's ability to recover from a disaster. This trend of declining credit scores is more pronounced following medium-sized disasters: While long-term assistance is provided after the most severe weather events, a lack of long-term support following medium-sized disasters appears to account for this finding. The effect on credit scores is more pronounced for households that had lower credit scores prior to the disaster and in communities of color, which exacerbates preexisting disparities in credit access.

The timing of federal relief matters, said Martín. FEMA assistance, for example, generally expires within six months after the disaster, but might extend for another 12 months in certain cases. However, it often takes more than a year after the disaster for state and local governments to launch their Community Development for Block Grant Disaster Recovery (CDBG-DR) programs. This means that many families may wait three years or longer before CDBG-DR funds become available. This gap in assistance can create an extended period of financial challenges for households. Moreover, the CDBG-DR program requires special congressional appropriation, a legislative reality that can lead to inconsistent aid delivery that can exacerbate capacity gaps in staff, knowledge, and resources.

Martín said the disparities seen in post-disaster recovery are mirrored in the provision of pre-disaster mitigation efforts. For example, there are disparities by income and community in terms of insurance coverage and access to insurance, including the National Flood Insurance Program administered by FEMA. There is also inconsistency in home preparations, delivery of mitigation systems to structurally assist households, and provision of long-term infrastructure and land use planning to these communities. He concluded his remarks by recommending that the federal government prioritize tools that narrow disparities for vulnerable people and eliminate the gaps in services that the federal government provides. He noted that many current federal interventions may increase social and economic vulnerability for many communities.

ARNOLD MODERATED THE Q&A AND DISCUSSION BETWEEN PCAST MEMBERS AND HSIANG, HILL, AND MARTÍN.

SESSION: CYBER RESILIENCE

Deb Bodeau, MITRE

Deb Bodeau said that cyber resilience is a systems engineering problem, where the systems are sociotechnical and comprised of people, processes, technology, and large governance issues. Contemporary society has a pervasive dependence on cyber—software running on microprocessor chips that communicate with the larger world—and that dependence comes with pervasive risk in the form of bad actors exploiting that dependence and the vulnerabilities inherent in software and hardware. The result of adversarial exploitation can be severe in the physical and information realm, which includes security breaches to steal information and use that information to manipulate people.

Cyber resilience, said Bodeau, operates under the assumption that adversaries will establish a presence in cyber systems that may not be detected for some time. As a result, critical components will be flawed or unable to handle changing uses, and critical functions and operations will fail when attacked or challenged. That leads to a formal definition of cyber resilience as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources." While *cyber resilience* focuses on assuring that critical functions and properties can withstand challenges or attacks and may never detect bad actors or system flaws, *cybersecurity* focuses on protecting information and authorized use. Cyber resilience, said Bodeau, can make the most critical cybersecurity functions more resilient.

Bodeau said that assuring adequate cyber resilience starts with determining what matters to stakeholders and considering the risks that result from cyber dependence. Cyber resilience, then, entails leveraging operational practices and technology to make it hard for an adversary to succeed with an attack using unpredictability, deception, redundancy, and other techniques. Each of these cyber resiliency techniques has been interpreted and applied to different environments that involve critical functions and include cyber elements. The bottom line, said Bodeau, is that cyber systems need safety, reliability, security, and resilience in the presence of threats that are hard to predict and understand.

Theresa McAllister, National Institute of Standards and Technology

Theresa McAllister said that cyber resilience addresses adverse conditions, stresses, attacks, or compromises of systems enabled by cyber resources. Resilience builds upon well-established concepts that include urban planning, hazard characterization, reliability, life safety, risk management, mitigation, and emergency response, and it provides a framework to integrate these and other concepts, such as functional recovery.

Key concepts for infrastructure resilience, said McAllister, include context, which refers to the role of infrastructure in the community; recovery of function, both in the short-term through temporary measures and in the long-term to meet a community's social needs; and reducing any interdependencies between infrastructure and other systems. Context, she added, includes how well a system recovers the functions or services it provides as well as the metrics to measure whether goals of recovery are being met and which mitigation and recovery concepts provide optimal resilience.

McAllister provided examples of two events that exposed critical infrastructure resilience or lack thereof. The first event was when Hurricane Sandy hit New York and New Jersey in 2012. The electric utility had proactively turned off power to two data centers. One center had batteries in place to provide power until fuel arrived for generators. The second site did not prepare in advance and all of its mechanical and electrical equipment was destroyed, leading to a long delay in its recovery. Wastewater treatment plants, which are always near a body of water, had pre-event plans to de-energize systems to reduce damage, but the 12-foot storm surge inundated the plants before they could take proactive action and the plants suffered extensive damage. While power was restored within two days, damaged power systems at the plants required the extended use of emergency power. Gas stations were also affected because their data systems had been damaged, so people could not pump gas because payments couldn't be processed.

The second event was the 2021 cyber-attack on the Colonial Pipeline. In this case, there was no physical damage, but the pipeline operators proactively shut down the pipeline for five days to ensure the pipeline's safety. This triggered a disruption in fuel supplies, which led to consumers spending many hours waiting in gas lines. Subsequently, Congress passed the Cyber Incident Reporting for Critical Infrastructure Act that requires critical infrastructure firms to alert the federal Cybersecurity and Infrastructure Security Agency (CISA) within three days if they are hacked and within one day if they pay a ransom to hackers. This information, said McAllister, will provide a better understanding of the recovery process and guide efforts to increase resilience.

McAllister noted there are challenges to measuring cyber resilience. Data, for example, arrives over many spatial and temporal scales, and there is a lack of data, especially for recovery efforts. Data is key because it informs models that can identify dependencies and potential impacts that result from damage to a connected system. Model outputs and metrics can then provide decision support to system managers and communities.

David Mussington, Department of Homeland Security

David Mussington discussed CISA's focus on infrastructure risk, and particularly, risks to systems that deliver vital digital and other services to the U.S. economy. This is a challenging risk environment, he said, that empowers particular adversaries—nation-states and otherwise—to interrupt the availability and accessibility of critical data and services. To address this threat, CISA and its colleagues from the Sector Risk Management Agencies (SRMAs) organized a collective infrastructure risk mitigation activity underpinned by the National Infrastructure Protection Plan.

Mussington said SRMAs are federal agencies. Each of 16 critical infrastructure sectors has a designated SRMA to coordinate risk mitigation for that particular sector. CISA serves as the national coordinator for all of the SRMAs. When a risk appears in one sector, CISA communicates information on the risk to all SRMAs and coordinates collective action to mitigate the risk where possible, given that many vulnerabilities are only apparent after-the-fact. Because the risk environment is complex, risk mitigation emphasizes advance assessment of critical infrastructure to see how prone it might be to exploitation, a process CISA facilitates or conducts itself.

Jim Platt, Department of Homeland Security

Jim Platt noted that CISA's National Risk Management Center (NRMC) partners with the private sector to provide secure and resilient infrastructure. This is critical because the private sector owns and operates the vast majority of U.S. infrastructure. Platt said that companies tend to care more about whether a function stops working than whether the cause is a cyber incident or a physical attack, so companies think about operational resilience rather than cyber resilience. Therefore, risk mitigation efforts are focused on trying to identify the function(s) that critical infrastructure sectors provide and examine them from an all-hazards perspective.

Platt explained that for the communications sector, "Primary, Alternate, Contingency, and Emergency (PACE)" communication plans exist to mitigate risks to critical infrastructure since it would be too expensive to build security and resilience to protect all communication functions. Defining what is critical enables the NRMC to make a business case that it is in a company's best interest to protect their critical systems because a failure is likely at some point.

Platt also noted that the cause of a disruption is irrelevant to the response. What is important is to prepare to continue providing a critical function in an environment that is not the normal operating environment and how to restore those functions quickly. Sometimes, restored operations might have degraded capacity that are deemed acceptable in a predefined planning scenario. Platt concluded his remarks by noting the importance of considering the holistic resilience of the nation's critical systems and capabilities and the importance of focusing on all-hazards planning, not just cyber planning.

Kathleen Fisher, Defense Advanced Research Projects Agency (DARPA)

Kathleen Fisher discussed DARPA's High-Assurance Cyber Military Systems (HACMS) program, which sought to build software for vehicles that would be difficult to hack. The study began when a skilled DARPA "red team"—a group tasked with playing the role of an adversary to test the security of a system—was given six weeks to try to remotely hack into an open-source quadcopter and Boeing's Unmanned Little Bird helicopter. The red team easily hacked into the quadcopter, and Boeing engineers were surprised that the red team was able to take over control of the Unmanned Little Bird. Over the next 16 months, formal methods researchers rewrote most of the quadcopter's software. The red team was given full access to the source code and all information about the system, but this time, the red team could not hack into the quadcopter. Similarly, after the Boeing aviation engineers were taught how to use formal methods tools, they changed parts of the Unmanned Little Bird helicopter's flight control software. This time, the red team was unsuccessful in their hacking attempts. In fact, when the red team tried to hack the flight control software, test pilots reported no degradation in the aircraft's performance while running the secure code. This result, said Fisher, shows that with judicious use of formal methods, a highly secure software kernel, and high-assurance code, it is possible to build systems that are much more resilient to attack without having to rewrite all of a system's code.

A key lesson from HACMS, said Fisher, is that it is critical to validate messages and data originating outside a system or from untrusted sources. DARPA's Safe Docs program has developed state-of-the-art protections for rich data formats that are used pervasively, such as the PDF format, and works with the appropriate standards body to incorporate security-related changes into the PDF specification. Microsoft's EverParse project has also developed message parsers that verify incoming information in real-time.

Fisher said that since it is impossible to build all cyber-physical systems to HACMS or SafeDocs standards anytime soon, it is important to understand how to detect when an adversary has infiltrated a cyber-physical system and how to remove the hostile code. For example, the software that monitors the balance of power produced versus the power consumed in a power grid will trigger a timed shutdown sequence to protect the turbines if that balance is disrupted. While that protects the turbines from being destroyed, it takes weeks or months to restart the grid following a shutdown. So, if an adversary has an embedded agent in the software, it could cause a massive disruption by accelerating the shutdown sequence and providing false information to system monitors.

DARPA researchers, said Fisher, developed the Rapid Attack Detection, Isolation and Characterization Systems (RADICS) grid-sensing tools to identify cyber-attacks, and they created an algorithm to model power grids in real time. Utilities and independent grid operators are now using this algorithm. Because adversaries can also compromise communications networks, RADICS tools can also remove a complex cyber-physical system from the internet and connect it to encrypted channels that run on National Guard radios.

Fisher said that removing an adversary from a system requires deep forensic analysis, but most cyber-physical system vendors do not provide forensic ports on their equipment to enable such analyses. RADICS tools also enable operators to conduct the necessary forensics and to restore systems more reliably than is possible when using a vendor's factory reset setting. These tools detected 86 percent of a red team's cyber-attacks on a test power grid in three days instead of the usual 10 days. While RADICS is a good start, more work remains to develop fast modeling capabilities based on sensors that can provide reliable situational awareness and deep forensic analysis capabilities, as well as enable continued partnerships between power engineers and cyber experts with opportunities to practice during live exercises.

ZUBER MODERATED THE Q&A AND DISCUSSION BETWEEN PCAST MEMBERS AND BODEAU, MCALLISTER, MUSSINGTON, PLATT, AND FISHER.

SESSION: DISCUSSION AND CONSIDERATION FOR APPROVAL OF PCAST REPORT TO THE PRESIDENT: *BIOMANUFACTURING TO ADVANCE THE BIOECONOMY*

Paula Hammond and Catherine Woteki, PCAST Members

Paula Hammond noted the bioeconomy is an emerging and rapidly expanding economic sector representing the portion of the economy based on products, processes, tools, and services derived from biological sources. A recent National Academies report estimated that the total economic impact of the U.S. bioeconomy, including direct and indirect effects, was $959.2 billion in 2016. And a 2020 McKinsey Global Institute report estimated that the global bioeconomy is expected to grow to a future value between $2 and $4 trillion in the next 10 to 20 years. Biomanufacturing is the engine by which the innovative products of the bioeconomy are brought to commercial scale.

Hammond said that Executive Order (EO) 14081, *Advancing Biotechnology and Biomanufacturing Innovation for a Sustainable, Safe, and Secure American Bioeconomy*, calls on PCAST to issue a report on the bioeconomy with recommendations to maintain global competitiveness. PCAST's working group on advanced biomanufacturing determined that for the United States to achieve the bioeconomy's enormous potential, the nation needs to address three key gaps: insufficient manufacturing capacity, regulatory uncertainty, and an outdated national strategy. The working group proposed several recommendations to fill these gaps.

The first recommendation, said Hammond, is for the President to direct the Secretary of Commerce to establish biomanufacturing infrastructure hubs with the authorities and resources necessary to scale up from prototype components in a production relevant environment (Manufacturing Readiness Level 6) to low-rate production capability (Manufacturing Readiness Level 8). These hubs would expand the capability and capacity of the Manufacturing USA Institutes and leverage the Regional Technology Hubs authorized in the CHIPS and Science Act. Furthermore, the Office of Science Technology and Policy (OSTP)

Director and the Secretary of Commerce should work in consultation with the Secretary of Defense, Director of the National Science Foundation (NSF), and Secretary of Energy to develop a plan to implement these hubs and develop a competitive process for determining the specific focus of each hub, funding allocations, and geographic locations.

Hammond said that the report puts forward suggestions for establishing a geographically diverse set of hubs that would leverage the potential across the country to produce biomass and build a biomanufacturing workforce. The hubs should be connected in a network that would allow developers to share knowledge, capabilities, and infrastructure. The network should include Manufacturing USA Institutes, Regional Technology Hubs, the Defense Department's biomanufacturing initiative, and NSF's Regional Innovation Engines. Along these lines, the working group also suggested that the President instruct U.S. science agencies to coordinate with these biomanufacturing infrastructure hubs, form partnerships, and create funding opportunities that will enable the biomanufacturing developments of the future and address some of the challenges in biomanufacturing. The resulting research opportunities will enable workforce training, including hands-on learning experiences.

Catherine Woteki said the second recommendation focuses on regulatory uncertainty. Specifically, the Environmental Protection Agency (EPA) Administrator, Secretary of Agriculture, and Food and Drug Administration (FDA) Commissioner should establish a standing Rapid Response Team of key agency representatives that meets frequently to vet new, cross-cutting products and provide developers with recommended regulatory routes for bioproducts that fall under the purview of two or more agencies. This team would implement the Unified Website for Biotechnology Regulation that EO 14081 requires, and it would provide opportunities to cross-train regulatory staff members in ombudsman positions, residing within each agency, to act as guides for bioproducts. In addition, the recommendation calls for the FDA, EPA, and the Agriculture Department to develop streamlined and model pathways for regulatory review and approval of emergent bioproducts of similar type by either drawing from the evolution of pathways from the past review processes or by creating an open-access searchable library.

The third recommendation, said Woteki, calls for the National Science and Technology Council to prepare a 10-year strategy for the bioeconomy within 18 months. This strategy should consider the long-term economic, environmental, and social benefits and liabilities of the proposed actions and policies as well as any implications for national security. In addition, by 2023 the OSTP Director should include research needs of the bioeconomy as a key component of the National Biotechnology and Biomanufacturing Initiative (required by EO 14081), the National Engineering Biology Research and Development Initiative, and the five-year coordinated research reports required under the CHIPS and Science Act. These plans should emphasize the fundamental and translational research needed to accelerate growth in the bioeconomy as well as other objectives for maintaining our international competitiveness.

Finally, said Woteki, there is a need for data and metrics to be part of the national strategy. Therefore, there is a recommendation that the Secretary of Commerce direct the Bureau of Economic Analysis to establish a "satellite account" for the bioeconomy as soon as possible and no later than 2024. The federal statistical agencies should plan to provide the data for both the long-term strategy and for the satellite account, and they should identify the resources needed in their budget request for fiscal year 2025. This plan should provide the data necessary for the metrics in the recommended long-term strategic plan.

Zuber moderated the Q&A and discussion between PCAST Members and Hammond and Woteki.

Following the discussion, Zuber asked for a voice vote to approve the report, and PCAST voted to approve the report.

PUBLIC COMMENT

No public comments were presented.

CLOSING COMMENTS

Arnold congratulated the biomanufacturing team for the report. Zuber then adjourned the public session.

MEETING ADJOURNED: 4:00 PM Eastern Time

I hereby certify that, to the best of my knowledge, the foregoing minutes are accurate and complete.

Frances Arnold, Ph.D.
Co-Chair
President's Council of Advisors on Science and Technology

Arati Prabhakar, Ph.D.
Co-Chair
President's Council of Advisors on Science and Technology

Maria Zuber, Ph.D.
Co-Chair
President's Council of Advisors on Science and Technology