# SUMMARY OF THE 2018 CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE STAKEHOLDER WORKSHOP

*Product of the*

SUBCOMMITTEE ON CRITICAL INFRASTRUCTURE SECURITY
AND RESILIENCE

COMMITTEE ON HOMELAND AND
NATIONAL SECURITY

*of the*
NATIONAL SCIENCE & TECHNOLOGY COUNCIL

FEBRUARY 28, 2018

## Key Takeaways

At the National Science and Technology Council (NSTC) 2018 Critical Infrastructure Security and Resilience (CISR) Stakeholder Workshop, held on February 28, 2018, in Washington, D.C., Federal, state, private, and academic stakeholders shared research needs, breakthroughs, and observations about emerging threats and challenges to the security and resilience of the Nation's critical infrastructure. Key takeaways include:

- Computational models, sensor networks, big data, and self-healing systems are promising approaches to solving CISR challenges;
- Techniques and technologies developed for one sector or system may be successfully adapted into others; and
- Research and development (R&D) into the dynamics of interdependent systems and into human and social factors in critical infrastructure systems are of particular interest.

## Background

The Federal Government has identified 16 critical infrastructure sectors[1] whose security and resilience are so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. While the security and resilience of this infrastructure is essential, ever-changing risks from natural hazards, human adversaries with growing capabilities, increasing automation, and systemic interdependence make constant advancements in R&D crucial. As the Trump Administration's 2019 Research and Development Budget priorities memo noted, "agencies should invest in R&D to increase the security and resilience of the Nation's critical infrastructure from both physical threats and cyber-attacks, which have increased rapidly in number and complexity in recent years."[2]

The NSTC Committee on Homeland and National Security's CISR R&D Subcommittee, which is co-chaired by the Department of Homeland Security, The White House Office of Science and Technology Policy, and the U.S. Army Corps of Engineers, organized the workshop to share insights and build relationships between the public and private sectors and across the critical infrastructure sectors. Representatives from every Federal agency with lead responsibility for a critical infrastructure sector plus public and private stakeholders from 13 of the 16 sectors participated.

[1] Per Presidential Policy Directive 21, the 16 Critical Infrastructure Sectors are: Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials, and Waste; Transportation; and Water and Wastewater Systems.

[2] https://www.whitehouse.gov/sites/whitehouse.gov/files/ostp/fy2019-administration-research-development-budget-priorities.pdf

## Event Focus

The workshop was organized around three high-priority topics:

### A. Science and Technology Strategies for Improving Resilience in Interdependent Systems

The growth of complex interdependencies within critical infrastructure systems can be partly attributed to technological advancements, including advanced sensors, wireless networks, and big-data dependent processes being coupled with legacy systems. Although greater connectedness and interdependence allow for improved performance, they also increase the number and types of vulnerabilities adversaries can exploit. Identifying and modeling interdependencies and their cascading effects was identified as a key challenge.

The risk of cyber-attacks continues to rise. Systems engineers should design to keep intruders out and also to mitigate the vulnerabilities intruders may target when they gain entry. More research is needed to advance detection, prevention, and mitigation capabilities. Novel approaches, including increased automation and artificial intelligence, are needed to develop security measures that balance functionality, reliability, and safety.

More R&D is needed to improve the understanding of "humans in the loop," including when it is better for an intelligent human to make a decision versus when it is better for a computer to assess an issue to avoid human error. Increased collaboration and coordination between researchers, operators, and owners across sectors can help ensure that the right research is undertaken, advances quickly, and is put to good use.

### B. Next-Generation or Emerging Technologies for Critical Infrastructure

New materials offer promise for addressing infrastructure life-cycle issues because of their potential to improve resilience and extend system life expectancies. Sensing technologies could allow for continuous system monitoring and more precise inspection.  Advancements in computing techniques promise new approaches for data-informed simulations to explore system performance in the face of changing conditions and threats, as well as more accurate anticipation of the performance of aging systems. Looking ahead, next-generation technologies may also include self-healing materials and buildings, widespread 3-D printing of complex materials, and increased use of robotics.

Strategies and standards should be reevaluated to more efficiently integrate innovative materials and technologies to improve infrastructure and move towards performance-based risk-management standards. Robust risk assessments are needed to better target investments and prioritize the maintenance and rebuilding of critical infrastructure.

### C. Working Across Public and Private Sectors to Advance Research, Development, and Dissemination

Public-private relationships foster information sharing, improve researcher diversity and appreciation for real-world challenges, and increase researcher access to data and field settings. New technologies that leverage communication and data sharing between the public and private sectors have been especially helpful in crisis situations, enabling stakeholders to coordinate and quickly disseminate critical information from public and private sources during regional disasters. Public-private collaborations allow large and diverse datasets to be formed, vetted, and integrated onto customized information dashboards for decision-makers and responders while ensuring data integrity.

International collaboration is also helpful, as other nations face many of the same infrastructure challenges as the United States, including cyber infrastructure resilience in areas such as optical networking, the "Internet of Things," and big data. Partnerships between stakeholders in the telecommunications and computing industries are examples of how resilience can be improved through better communication. However, key challenges remain, including developing and maintaining a robust, diverse workforce, and building and maintaining trust in relationships across sectors for increased information sharing.

## Summary

The workshop provided an opportunity to forge new relationships across critical infrastructure sectors and communities, increase cross-sector awareness regarding common challenges and research opportunities, and share information about emerging technologies and advances in R&D. Continued communication across sectors, agencies, and communities will help ensure timely, impactful integration of innovative solutions for common challenges going forward.

## About the National Science and Technology Council

The National Science and Technology Council (NSTC) is the principal means by which the Executive Branch coordinates science and technology policy across the diverse entities that make up the Federal research and development enterprise. A primary objective of the NSTC is to ensure science and technology policy decisions and programs are consistent with the President's stated goals. The NSTC prepares research and development strategies that are coordinated across Federal agencies aimed at accomplishing multiple national goals. The work of the NSTC is organized under committees that oversee subcommittees and working groups focused on different aspects of science and technology. More information is available at http://www.whitehouse.gov/ostp/nstc.

## About the Office of Science and Technology Policy

The Office of Science and Technology Policy (OSTP) was established by the National Science and Technology Policy, Organization, and Priorities Act of 1976 to provide the President and others within the Executive Office of the President with advice on the scientific, engineering, and technological aspects of the economy, national security, homeland security, health, foreign relations, the environment, and the technological recovery and use of resources, among other topics. OSTP leads interagency science and technology policy coordination efforts, assists the Office of Management and Budget with an annual review and analysis of Federal research and development in budgets, and serves as a source of scientific and technological analysis and judgment for the President with respect to major policies, plans, and programs of the Federal Government. More information is available at http://www.whitehouse.gov/ostp.

## Copyright Information

This document is a work of the United States Government and is in the public domain (see 17 U.S.C. §105). Subject to the stipulations below, it may be distributed and copied with acknowledgment to OSTP. Copyrights to graphics included in this document are reserved by the original copyright holders or their assignees and are used here under the government's license and by permission. Requests to use any images must be made to the provider identified in the image credits or to OSTP if no provider is identified. Printed in the United States of America, 2017.