RESEARCH, DEVELOPMENT, AND INNOVATION FOR ENHANCING RESILIENCE OF CYBER-PHYSICAL CRITICAL INFRASTRUCTURE: NEEDS AND STRATEGIC ACTIONS

RIPDWG White Paper

March 2023

Resilient Investment Planning and Development Working Group

NOTICE: This paper represents the consensus views of the RIPDWG and its recommendations to CISA, and as such does not necessarily represent the views, policy decisions, or findings of CISA, DHS, or the United States Government. The public release of this paper does not constitute or imply endorsement by the United States Government of the findings or recommendations, nor does it convey CISA's commitment to any specific future course of action with respect to the paper's findings and recommendations.

About the Resilient Investment, Planning and Development Working Group

Recommendations in this document were adopted by the Resilient Investment, Planning and Development Working Group (RIPDWG), a cross-sector coordination forum comprised of government and private-sector resilience and infrastructure experts Chartered in 2018 within the framework of the Critical Infrastructure Partnership Advisory Council (CIPAC). The mission of the RIPDWG is to provide advice and recommendations to enhance the development, coordination, and implementation of integrated security and resilience approaches for critical infrastructure. The RIPDWG is co-chaired by representatives from Government and Cross-sector Coordinating Councils. The Cybersecurity and Infrastructure Security Agency (CISA), Infrastructure Security Division (ISD) provides the administrative support for RIPDWG.

Member Organizations*

Government Coordinating Council Members

U.S. Army Corps of Engineers
U.S. Department of Agriculture
U.S. Department of Energy
U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security, Science & Technology Directorate
U.S. Environmental Protection Agency
U.S. General Services Administration

Sector Coordinating Council Members

Communications SCC
Information Technology SCC
Water SCC

Cross-Sector Coordinating Council Members

State, Local, Tribal and Territorial Coordinating Council

About this Document

This paper was developed by the Research and Development (R&D) Task Group of the RIPDWG to highlight research, development, and innovation (RD&I) gaps associated with the resilience of cyber-physical critical infrastructure systems. The task group began by reviewing existing federal research initiatives and policies and recent resilience literature from several disciplines. In addition, the task group held a listening session with local government and academic subject matter experts. Given the tendency for agencies or sectors to rely on a specific type of discipline, an effort was made to include social, physical, public administration, business, and geographic disciplines and sources. The R&D Task Group also consulted with CISA and DHS Science & Technology (S&T) to narrow the scope to topics not already addressed in other ongoing efforts. This paper was briefed to various cross-sector coordinating councils for feedback. RIPDWG members reviewed recommendations on October 26, 2022 and delegated final review of the paper to the RIPDWG Executive Committee, who approved it on March 13, 2023.

Acknowledgement

Development of this paper was led by RIPDWG R&D Task Group Lead, Dr. David Alexander (DHS S&T) with editing support from CISA staff, Dr. Sandra Pinel (ISD) and Dr. Natallia L. Diessner (ISD). Recommendations in this paper are consensus advice of RIPDWG Members only. Background information and content for findings in this paper were informed by subject matter experts serving on the RIPDWG R&D Task Group: Dr. Enrique Matheu (USACE), Dr. Paula Scalingi (Institute for Innovating Security and Resilience), Larry Clinton (Internet Security Alliance), Alex Cordova (USDA), David Winks (AcquSight), Annie Vest (Freese & Nichols), David Vaughn (Clemson University), and Dr. Derek Kauneckis (Desert Research Institute).

Representation on RIPDWG does not imply an organization's endorsement of this paper.

NOTICE: This paper represents the consensus views of the RIPDWG and its recommendations to CISA, and as such does not necessarily represent the views, policy decisions, or findings of CISA, DHS, or the United States Government. The public release of this paper does not constitute or imply endorsement by the United States Government of the findings or recommendations, nor does it convey CISA's commitment to any specific future course of action with respect to the paper's findings and recommendations.

Executive Summary

The Nation's health, safety, and economy depend on the functioning of complex and interconnected infrastructure systems that provide critical services to communities across the nation. The evolution and escalation of threats and stressors to critical infrastructure, combined with their increased reliance on cyber, have led to an exponential increase in risks to our national security. A key means of reducing these risks is the production of relevant and accessible, resilience-based critical infrastructure research and innovation. The federal government must undertake an integrated approach to research that is designed to effectively enable infrastructure partners at all levels to apply federally-funded research, development, and innovation (RD&I) to improve the resilience of critical infrastructure services.

National policy highlights the need for such research, however the federal research enterprise has yet to fully capitalize on the opportunity by collectively executing an integrated RD&I strategy to address critical infrastructure security and resilience challenges, particularly at the community level. Federal research is often sector-specific or fragmented by discipline, making it hard to see how they might effectively mitigate cross-cutting and systemic risks. In this paper, the Resilient Investment, Planning and Development Working Group (RIPDWG) identifies some specific RD&I needs and strategic actions focused around three major gaps it sees in federal research efforts: (1) An integrated analysis of consequences and risk reduction decision factors for critical services that depend on cyber-physical infrastructure systems; (2) An understanding of the societal dimensions of enhancing the resilience of cyber-physical infrastructure systems; and (3) User-engagement in cyber-physical infrastructure research to translate resilience knowledge into effective action at the local and regional level.

Key strategic RD&I actions identified herein include:

- Develop integrated models capable of identifying systemic risks to interconnected infrastructure and cascading impacts of disruptions.
- Establish interagency RD&I testbeds for cyber-physical infrastructure resilience.
- Develop methods to analyze and monitor cyber and physical infrastructure interoperability to identify points of intervention to sustain operations.
- Integrate decision theory into research to understand and account for how public versus private infrastructure entities assess and manage risk.
- Develop metrics, methodologies, and guidance for decision-makers on integrating green and gray infrastructure solutions.
- Analyze unanticipated vulnerabilities and implications of technology innovation on the security and resilience of critical infrastructure services.
- Understand the impact of workforce changes on critical infrastructure security and resilience to identify gaps in what is needed to support an infrastructure workforce into the future.
- Develop shared baseline information on how demographic, geographic, and institutional capacity stressors have resulted in vulnerabilities and inequitable impacts of critical service disruptions.
- Identify and empirically test principles of resilient design and adaptive risk management to determine effectiveness in meeting infrastructure resilience and sustainability outcomes/metrics.
- Work with private and public, place-based institutions to co-produce knowledge with users to improve the relevance and applicability of RD&I to infrastructure actions at the community level.

NOTICE: This paper represents the consensus views of the RIPDWG and its recommendations to CISA, and as such does not necessarily represent the views, policy decisions, or findings of CISA, DHS, or the United States Government. The public release of this paper does not constitute or imply endorsement by the United States Government of the findings or recommendations, nor does it convey CISA's commitment to any specific future course of action with respect to the paper's findings and recommendations.

- Examine the institutional and regulatory context of infrastructure risk management against the requirements for adaptive management of systems under a changing risk environment.
- Conduct comparative empirical resilience case studies of both federally supported and non-federal resilience initiatives.

Identified RD&I strategic actions can enhance the current federal research agenda and should be considered for holistic implementation by research partners across the interagency in collaboration with stakeholders.

NOTICE: This paper represents the consensus views of the RIPDWG and its recommendations to CISA, and as such does not necessarily represent the views, policy decisions, or findings of CISA, DHS, or the United States Government. The public release of this paper does not constitute or imply endorsement by the United States Government of the findings or recommendations, nor does it convey CISA's commitment to any specific future course of action with respect to the paper's findings and recommendations.

Contents

NOTICE: This paper represents the consensus views of the RIPDWG and its recommendations to CISA, and as such does not necessarily represent the views, policy decisions, or findings of CISA, DHS, or the United States Government. The public release of this paper does not constitute or imply endorsement by the United States Government of the findings or recommendations, nor does it convey CISA's commitment to any specific future course of action with respect to the paper's findings and recommendations.

Introduction

According to the 2022 Annual Threat Assessment of the U.S. Intelligence Community, the U.S. will face an increasingly complex and interconnected global threat environment amidst an evolving set of challenges ranging from geopolitical rivalry, ecological degradation and climate change, rapidly evolving technology, aging infrastructure, and shifting demographics (Office of the Director of National Intelligence, 2022). These challenges will intersect and interact in unpredictable ways posing great risk to U.S. security and resilience with significant implications to the Nation's critical infrastructure and services (U.S. Department of Homeland Security, 2021).

The Nation's health, safety, and economy depend on the functioning of an increasingly complex, interconnected set of cyber-physical infrastructure systems that provide essential services in the face of rapidly changing and overlapping threats, shocks, and stressors. Further digitization of societal activities and functions are driving the convergence and exacerbation of risks to these infrastructure systems and their subsequent vulnerabilities.

Congress has recognized these expanding risks with substantial recent investments in research, technology, and innovation to support cyber and infrastructure security and resilience, resulting in response by various federal agencies to address infrastructure, new technologies, and climate change mitigation (Cybersecurity and Infrastructure Security Agency, 2021; U.S. Department of Homeland Security, 2022). Recognizing the vast and disproportionate impact of climate, security, and other disruptions and technological changes to the most vulnerable and underserved communities, the Biden Administration has required that all federal expenditures address these disparities (The White House, 2021; Executive Order 13985; Executive Order 14008; Executive Order 14052).

The National Infrastructure Protection Plan (U.S. Department of Homeland Security, 2013) included an agenda of needed research to enhance critical infrastructure security and resilience. However, the homeland security and larger federal research enterprise has not yet fully capitalized on the opportunity to make its research relevant, equitable, accessible, and useful to those decision-makers that must address critical infrastructure challenges at the local and regional scales. This is especially evident in the case of federal research efforts pursuing innovative risk-reduction technologies for infrastructure systems without a full understanding of how those technologies could be leveraged by those who own, operate, and regulate those infrastructure systems and provide essential public services. In addition, most federal research efforts relevant to critical infrastructure resilience are driven by agency-specific missions and their corresponding priorities at the national level. As a result, those efforts may not always consider the social, economic, and institutional contexts linked to the implementation of the resulting technologies and the full spectrum of impacts on local communities and regional stakeholders. Furthermore, the quantification of local and regional resilience benefits resulting from federal investments on critical infrastructure security and resilience remains a challenging problem. Finally, the outcomes of federal research efforts on critical infrastructure resilience are often sector-specific or fragmented by discipline, making it difficult to develop a full picture of how those efforts may mitigate cross-cutting and systemic risks. It is imperative that the federal research, development, and innovation community develop an overarching framework to guide cyber-physical critical infrastructure research efforts and inform the development and implementation of related federal programs and policies.

NOTICE: This paper represents the consensus views of the RIPDWG and its recommendations to CISA, and as such does not necessarily represent the views, policy decisions, or findings of CISA, DHS, or the United States Government. The public release of this paper does not constitute or imply endorsement by the United States Government of the findings or recommendations, nor does it convey CISA's commitment to any specific future course of action with respect to the paper's findings and recommendations.

Historically, homeland security research and development activities have shown a tendency to narrowly focus on technological or operational solutions without an empirical understanding of how innovations are ultimately adopted and sustained. In general, there has been limited research addressing the socio-economic conditions characterizing the landscape where those innovations may be deployed. Ignoring or not fully accounting for these conditions may limit the effectiveness of science and technology advances and critical infrastructure investments aimed at improving security and resilience. Multiple disciplines, think tanks, universities, and federally-funded centers are modeling threats to interdependent systems to inform preparedness, response, recovery, mitigation, and design; however, recent events have caused a national awakening to the importance of questioning assumptions and rethinking the factors that influence security and resilience by considering the broader social, economic, governance, and environmental context of interventions and unequal capacities of communities and entities to apply research outcomes to enhance resilience and security (Hallegatte, Rentschler, & Rozenberg, 2019). The Nation must expand the scope of its research, development, and innovation (RD&I) approach to enhance the resilience of cyber-physical infrastructure systems by appropriately accounting for those conditions. This will serve to anticipate the challenges or unintended effects associated with implementation of new technologies and to understand the potential barriers that may hinder planning and decision-making at different jurisdictional levels.

This paper highlights some specific national RD&I needs to address the above challenges. It is important to highlight that these needs, and their corresponding strategic actions, do not represent an exhaustive list; therefore, they do not encompass the entire spectrum of RD&I requirements associated with the complex and evolving risks and challenges affecting critical infrastructure systems. The paper examines RD&I needs and actions with a focus on three primary areas: (1) Resilience of critical services that depend on cyber-physical infrastructure systems; (2) Societal dimensions of cyber-physical infrastructure resilience including considerations of equity, capacity, and economics; and (3) Applied and user-engaged research methods to address cyber-physical infrastructure resilience challenges at local and regional scales. This document primarily focuses on the federal R&D enterprise (federal departments and agencies, national laboratories, and federally-funded research centers) as the federal government holds the overall responsibility for coordinating national efforts to enhance the security and resilience of critical infrastructure. The paper concludes with recommendations for how to improve upon the current federal research and development process and structure.

The Challenge

Events continually demonstrate a lack of institutional capacity to adapt to changing threats and reduce vulnerabilities to critical services delivered by cyber-physical infrastructure systems. Those critical services are exposed not only to disruptions triggered by natural and human hazards, but also to underlying and pre-existing societal, economic, and operational conditions that may create barriers to implementing the most effective technological solutions that could enhance the resilience of the cyber-physical infrastructure systems delivering those services. Addressing these barriers will require an overarching approach focused not only on risk-reduction activities for cyber-physical systems but also on how those systems interact with the environment and surrounding communities to resiliently deliver critical services in view of ever-changing and overlapping threats and stressors.

Large bodies of important research conducted by social scientists, geographers, and ecologists remain largely disconnected from the body of knowledge that typically informs interventions to enhance the resilience of cyber-physical infrastructure systems. There is a clear need is to learn from these disciplines to improve our understanding and implement effective policies and programs for prevention, protection, mitigation, adaptation, response, and recovery. The optimal approach should seek to coordinate efforts across federal agencies to prioritize RD&I activities based on their potential to result in effective interventions that would enhance the resilience of critical services for communities and the Nation.

A new cross-cutting and synergistic RD&I approach is needed to:

- Reframe federal research priorities so they consider societal vulnerabilities and the contexts that lead to cascading and disproportionate consequences to communities, regions, and the Nation.
- Innovate research methods to apply multi-disciplinary risk assessment and applied research models that ensure the use of knowledge by stakeholders.
- Develop adaptive capacities for evolving and uncertain risks and underlying stressors to reduce disruptions to critical services from the local to national levels.
- Understand the barriers and enabling factors that influence stakeholders' decisions to adopt or implement innovations to enhance the resilience of cyber-physical infrastructure.
- Empirically understand the implications or benefits of adopting technology and innovations.

To effectively address overarching risks and underlying stressors, this RD&I approach requires a fundamental understanding of the dependencies linking cyber and physical systems; the geographic and demographic distribution of vulnerabilities, consequences, and capacities to address them; the role of social, cultural, environmental, and institutional values, contexts, and structures in achieving outcomes from programs intended to reduce risk; and the incentives necessary to motivate public and private collaboration at all scales to invest in security and resilience of existing and planned infrastructure.

Federal RD&I initiatives also require a shared lexicon for key concepts and definitions (such as *critical infrastructure*, *security,* and *resilience)* and a community of practice where different levels of government and the private sector can spur continuous innovation and better apply the latest RD&I outcomes toward building critical infrastructure resilience to changing conditions and future threats.

Scope and Intended Use

This paper is intended to inform federal priorities and actions on RD&I efforts aimed at enhancing the resilience of cyber-physical critical infrastructure systems. This document focuses on the federal R&D enterprise as the federal government holds the overall responsibility for coordinating national efforts to enhance the security and resilience of critical infrastructure. A primary objective of this paper is to spur collective action across the interagency to facilitate the implementation of new technologies and expand the benefits of federal research efforts.

The guiding question for this paper is:

> ***What are the cyber-physical infrastructure research priorities that should be addressed to achieve a more secure and resilient future for communities nationwide?***

This document highlights some specific areas of need that should be promptly addressed because of their importance. Therefore, it does not constitute an exhaustive list of all the gaps related to cyber-physical critical infrastructure systems. In addition, this document is only focused on the role of critical infrastructure systems as a necessary condition for community resilience. It is acknowledged that this is a necessary but not fully sufficient condition, as overall community resilience depends on a plethora of additional factors not directly linked to critical infrastructure.

Infrastructure Resilience RD&I Needs and Strategic Actions

This paper identifies key RD&I needs and strategic actions focused around three identified critical infrastructure resilience gaps in current federal research and development: (1) An integrated analysis of consequences and risk reduction decision factors for critical services that depend on cyber-physical infrastructure systems, (2) An understanding of the societal dimensions of enhancing the resilience of cyber-physical infrastructure systems, and (3) User-engagement in cyber-physical infrastructure research to translate resilience knowledge into effective action at the local and regional level.

Research Gap 1: An integrated analysis of consequences and risk reduction decision factors for critical services that depend on cyber-physical infrastructure systems

The rapidly escalating public and private use of "smart" technologies exponentially increases risk and vulnerability to the Nation's critical infrastructure systems and the essential public services they provide. Since 2013, the National Infrastructure Protection Plan and the 2013 Executive Order 13636 on cybersecurity require the Government to "consider the potential risks resulting from dependency on information and communications technology and inform preparedness planning and capability development" (U.S. Department of Homeland Security, 2013). While current research and policy recognize the increasingly interconnected nature of cyber and physical systems, government-sponsored and homeland security research continues to analyze cyber threats, protections, and innovations without integrally addressing the consequences to physical infrastructure operations and enabled essential public services. The research community needs to move toward a more holistic analysis of convergent cyber-physical infrastructure systems. RD&I needs range from how cyber systems and smart technologies are defined to understanding the economics that drive public versus private decisions to reduce cyber risks impacting critical infrastructure services.

RD&I Needs

Need 1.1 – A systemic understanding of interconnected cyber-physical infrastructure risk to critical services from the local to national scales

Essential social, economic, and public services such as water, transportation, manufacturing, and others increasingly rely on digital technologies to monitor and control operations, resulting in increasingly complex and vulnerable infrastructure systems. For example, the integration of industrial control systems into infrastructure increases access points for disruption and therefore, the risk of physical consequences resulting from either physical or cyber incidents (Grady, Rajtmajer, & Dennis, 2021). Our limited understanding of interconnected infrastructure systems can in essence become one of our main vulnerabilities (Heino et al., 2019). Escalating disruptions to supply chains and physical infrastructure operations demonstrate the need to map the interdependent relationship between the functional components of the larger cyber-physical infrastructure system.

Models are needed to characterize systemic risk extending across boundaries and scales and that provide for the integration of local and regional empirical and historical data to anticipate the cascading impacts of interconnected infrastructure disruptions to local, regional, and national security, economy, health, and the environment. The focus on cyber vulnerabilities should be done in tandem with vulnerability analyses of cross-sector physical infrastructure. Innovative communication methods are needed for public and private decision-makers to understand the impacts of cyber disruptions across reliant physical infrastructure systems that enable critical services.

NOTICE: This paper represents the consensus views of the RIPDWG and its recommendations to CISA, and as such does not necessarily represent the views, policy decisions, or findings of CISA, DHS, or the United States Government. The public release of this paper does not constitute or imply endorsement by the United States Government of the findings or recommendations, nor does it convey CISA's commitment to any specific future course of action with respect to the paper's findings and recommendations.

Need 1.2 – An understanding of system interoperability and management solutions for improved operational resilience to cyber disruptions

RD&I efforts have recently focused more on developing solutions to prevent cyberattacks and mitigate software supply chain vulnerabilities than on technologies to address cyber-physical infrastructure system resilience and adaptability, particularly how to maintain physical system operations when cyber systems are disrupted by either natural or human causes (The White House, 2023). Research to understand these systems will require going beyond the systems engineering discipline to model and forecast interoperability and interaction with social conditions, business practices, and human behavior (Reimann et al., 2017). Research needs include characterizing the integrated aspects of cyber and physical operational components, modeling the vulnerabilities of their operations to plausible and compounded threats and stressors, and developing methods for infrastructure owners and operators to evaluate the effectiveness of alternative actions to retain operability. Interoperability of cyber-physical systems also requires research that supports a new set of management approaches that enable the systems to more effectively collaborate and converse (Reimann et al., 2017). Finally, research is needed into the barriers facing small and under-resourced pubic and private entities in maintaining infrastructure operations with limited resources.

Need 1.3 – Models of economic decision-making that enable the design of effective public and private incentives for risk reduction

For the federal government to develop the right incentives to mitigate the risk and reduce the impacts of cyber disruptions to infrastructure systems and dependent services critical to the community or the Nation, research is needed to model the economic consequences resulting from these disruptions, the distribution of public and private costs, the economics of public and private risk mitigation decisions, and the externalities of costs and benefits for such investments. Private businesses and local governments that provide critical infrastructure services often lack the economies of scope and scale to address large-scale cybersecurity needs. Such models would be used to inform the development and structure of public incentives for private and state, local, tribal, and territorial (SLTT) government investment in cybersecurity for cyber-dependent critical infrastructure systems.

To inform the development of incentives and priorities for public and private critical infrastructure stakeholders, research should investigate the local/regional barriers to investment in cyber-physical resilience of publicly- versus privately-owned critical infrastructure, as well as the finance pathways and funding mechanisms for adequate and sustained cybersecurity of critical players in the infrastructure supply chain (Prysm Group, 2021). For example, there is a gap between traditional, commercial-level cybersecurity as practiced by the private sector and the cybersecurity needed to address emerging nation-state attacks on private systems (e.g., SolarWinds incident) that affect critical services across multiple sectors (SecurityWeek News, 2021).

Since increased cyber risk can also undermine the traditional economics of key critical infrastructure stakeholders such as public utilities, several additional issues require economic research to inform the federal government on how to encourage investments in system-wide security and resilience without stifling innovation. These issues include the unequal financial capacity of smaller businesses and governments to invest in cybersecurity, the market concentration of critical IT services, and the integration of risk mitigation into public utility commission rate requirements.

Need 1.4 – Common definitions, standards, and metrics for measuring effectiveness of infrastructure resilience interventions

The evolving risk landscape has rendered established design risk levels and current risk modeling inadequate for assessing and effecting the resilience of critical infrastructure. Research is needed to examine the risk levels, models, and other criteria necessary to determine effective metrics for evaluating all-hazards risks affecting cyber-physical systems. The explosion of new terminology such as "internet of things," "smart cities," and "green infrastructure" obscure a common understanding needed for integrated research to improve the resilience of these interconnected systems (Greer, Burns, Wollman, & Griffor, 2019). Development of a shared lexicon is required to share knowledge across sectors, governments, and academic institutions and to develop shared metrics to measure the effectiveness of actions for enhancing the security and resilience of interconnected cyber and physical systems across sectors using feedback from owners and operators (U.S. Government Accountability Office, 2021). Research is needed to develop a system to measure the effectiveness of risk-reduction and resilience-enhancing activities and action plans using meaningful indicators on a shared platform (Barker et al., 2017; Roshanaei, 2021).

Research should consider resilience performance standards that link the criticality of infrastructure components and interdependent systems with threat/hazard level and timeframe for returning to operations post event (Resilient Investment Planning and Development Working Group, April 1, 2022). Measures of effectiveness must be developed that consider multiple hazards and continuity of critical services and operations under future risk scenarios over time for the most vulnerable communities and systems. Most challenging is the development of infrastructure security and resilience indices and measures that can be implemented in the regulatory context to consider the overall societal impacts of interconnected infrastructure systems—human health, safety, security, the economy, and continuity of daily life.

Need 1.5 – Measurement of the contribution of green infrastructure and other innovations to reduce risk and lower the cost of disruptions

Research is needed to develop metrics for evaluating the combined effects of green and gray infrastructure investment alternatives. As a subset of nature-based solutions, "green infrastructure" has been adopted in federal policy to enhance adaptation to climate change and reduce the costs of gray infrastructure investment over time. However, the metrics for evaluating infrastructure investment alternatives do not account for green infrastructure, which may show benefits over a longer time period or require evaluation at a watershed, rather than asset scale. The National Institute of Science and Technology (NIST), International Standards Organization, and United Nations also note a lack of methods to assess the value of different frameworks for successfully managing risk and making investments that lead to greater resilience over the course of infrastructure lifecycle (Roshanaei, 2021). Variables might include contributions of green infrastructure solutions to enhance performance, cost-efficiency, community protection (Browder, Ozment, Bescos, Gartner, & Lange, 2019), and adaptive capacity over time (e.g., reducing flood damage or infrastructure operation and maintenance costs). Short-term mitigation actions that can reduce adaptive capacity also need to be investigated. Additionally, environmental vulnerabilities should be integrated into infrastructure dependency and interdependency assessments—further research is needed to better connect resilience of natural systems to that of physical infrastructure systems. Finally, there is a need for research activities focused on innovative approaches aligning the design, development, and retrofit of physical infrastructure with ecosystem benefits to support efforts such as the Engineering with Nature® initiative pioneered by the U.S. Army Corps of Engineers and the Building Community Resilience with Nature-Based Solutions effort being led by the U.S. Department of Homeland Security, Federal Emergency Management Agency. This approach supports the environment while also benefiting communities by promoting the development of engineering solutions designed to utilize natural systems. This leads to more sustainable results achieved through the effective integration of engineering and natural systems, potentially broadening the overall benefits while reducing the environmental footprint of physical infrastructure components.

Strategic RD&I Actions

Federal research should focus on systemic cyber and physical infrastructure risk analysis that applies across sectors and disciplines in supporting risk and resilience decision-making and investments. This more holistic approach to infrastructure security and resilience research on the probability and geographic and socio-economic distribution of consequences to "critical infrastructure" (as defined by statute[1]) functions and services will form the basis for collaborative risk management action by the Sector Risk Management Agencies and critical infrastructure partners. Recommended strategic priorities to address needs identified above include RD&I to:

1.A Develop integrated models capable of identifying systemic risk based on plausible future scenarios, while also underpinning stressors and the potential consequences of various scenarios to local, regional, and national critical functions that support the economy, security, health, and environment. Models should provide for the integration of local and regional empirical and historical data to anticipate the cascading consequences of disruptions to interconnected cyber and physical infrastructure operated by the public and private sector.

   a. Models should be designed to effectively communicate to public and private decision-makers the impacts of cyber disruptions across reliant physical infrastructure systems and enabled services.

   b. Risk assessment methods should be reviewed to identify gaps and align them to anticipate the cascading, cross-scale consequences of interconnected infrastructure disruptions to national security, economy, health, and the environment.

1.B Develop methods to analyze and monitor cyber and physical interoperability components, networks and systems, barriers, and the points of intervention to sustain operations under multiple threat scenarios including climate change, human attacks on physical systems, cyberattacks, and social or labor disruptions.

   a. Leverage existing and emerging operational/business continuity methodologies appropriate to convergent cyber-physical systems to recommend how to align standards, protocols, and interoperability mechanisms.

   b. Establish interagency RD&I empirical innovation testbeds to (1) analyze and identify the potential benefits and detriments of "smart technology" and use in "smart cities" on the resilience of infrastructure systems, and to (2) understand the factors for sustaining infrastructure operations across sectors under multiple hazards and threats. This research should support policy incubation and identify the barriers and regulatory environment needed to support equitable and effective use of technology innovations for operational resilience.

1.C Integrate decision theory and knowledge of decision-making into research to understand how public versus private entities (1) make cyber and physical risk tolerance, reduction, and

[1] Presidential Policy Directive 21

NOTICE: This paper represents the consensus views of the RIPDWG and its recommendations to CISA, and as such does not necessarily represent the views, policy decisions, or findings of CISA, DHS, or the United States Government. The public release of this paper does not constitute or imply endorsement by the United States Government of the findings or recommendations, nor does it convey CISA's commitment to any specific future course of action with respect to the paper's findings and recommendations.

mitigation decisions and (2) weigh tradeoffs between resilience objectives such as economics, operational efficiencies, and adaptation and recovery capabilities. This research can be used to identify intervention points that should be supported by federal, as well as state and local incentives for risk reduction.

a. Include an analysis of the investment needed to establish a social contract between the private sector and government to collectively implement sustainable cybersecurity that addresses nation-state threats while maintaining the core market economy system (Prysm Group, 2021).

1.D Develop metrics, methodologies, and guidance to integrate green and gray infrastructure solutions for use by public and private decision-makers at the local to national scales in evaluating long-term costs and benefits, weighing trade-offs, and making investment and prioritization decisions.

1.E Establish interagency RD&I testbeds for the resilience of physical and cyber infrastructure assets, systems, and networks to understand how to sustain operations across sectors under multiple hazards and threats to prioritize future security and resilience actions and investments and facilitate transitioning of capabilities to operations.

1.F Understand private and public risk management priority investment metrics for weighing tradeoffs between resilience objectives including economics, operational efficiencies, adaptation and recovery measures and the costs and benefits of actions to design federal to state and local incentives for risk reduction.

Research Gap 2: An understanding of the societal dimensions of enhancing the resilience of cyber-physical infrastructure systems

The resilience of cyber-physical infrastructure systems plays a key role in overall community resilience. Therefore, there needs to be a better understanding of the social dimensions of critical infrastructure systems and the critical services they deliver. Social dimensions range from understanding the causes and consequences of disproportionate impacts of disruptions to vulnerable communities, the factors that could enhance system resilience, the importance of the workforce in sustaining infrastructure operations, and how social behavior affects the feasibility and effectiveness of government policy and interventions. The National Science and Technology Council (NSTC) has developed a framework for understanding the societal dimensions of resilience to include the intrinsic characteristics of community including activities that contribute its functioning, quality of life outcomes, risks, and ability to handle hazards (chronic stressors as well as acute shocks) affecting safety, security, health, social cohesion, effective governance, and cross-cutting resources(National Science and Technology Council, 2023). Needs identified under this gap describe both how societal dimensions affect risk and how technology and innovations do or do not benefit different types of communities across urban and rural geographies.

RD&I Needs

Need 2.1 – An understanding of spatial inequities and elements of scale that affect community impacts and recovery from disruptions

Communities face increasing challenges in reducing risk from climate-related disasters such as floods and droughts, sustaining robust local economies, supplying drinking water to their growing populations, and preserving local ecosystems. The disproportionate impact of these challenges on the most vulnerable communities is being increasingly documented by research (National Academies of Sciences, 2022). In

NOTICE: This paper represents the consensus views of the RIPDWG and its recommendations to CISA, and as such does not necessarily represent the views, policy decisions, or findings of CISA, DHS, or the United States Government. The public release of this paper does not constitute or imply endorsement by the United States Government of the findings or recommendations, nor does it convey CISA's commitment to any specific future course of action with respect to the paper's findings and recommendations.

addition, geographers have studied the long-term spatial inequities that disadvantage communities (Connor, Gutmann, Cunningham, Clement, & Leyk, 2019) and make them more vulnerable to or unable to recover from disasters. Tracing the equitable or inequitable distribution of impacts or risk reduction outcomes will require a baseline of characteristics and spatial distribution of vulnerable communities and determining economic, technical, or social variables that impede or enhance recovery (Karakoc et al., 2020). A shared understanding is needed of the geographic and equity consequences of these disparities to inform appropriate policy and program design to address them.

Fundamental baseline research is needed to understand how changing demographic and economic concentrations affect the capacity of governments and the private sector to operate and maintain cyber-physical infrastructure systems and invest in their resilience. Similarly, a nationwide analysis is needed to understand recovery success, particularly among communities who did not receive federal disaster relief or assistance (Resilient Investment Planning and Development Working Group, April 1, 2022). To better define points of intervention, enhanced risk assessment models and approaches are needed that lead to a better understanding of how infrastructure interdependencies and cascading failures, when combined with underlying conditions, policies, and practices, can lead to the inequitable distribution of impacts across different geographic regions (e.g., how a government cybersecurity breach impacts delivery of housing, healthcare, or food to vulnerable populations) (Grady et al., 2021). In addition, spatial analysis has not been applied extensively to understanding stressors that threaten the capacity of communities to mitigate risk or to guide federal program priorities related to critical infrastructure resilience. There is a need for data-driven tools to better assess community vulnerabilities and more accurately evaluate the unique risks and challenges facing each community with the objective of supporting more equitable and environmentally just decision-making.

Need 2.2 – An understanding of human factors in applying technology innovations to cyber-physical infrastructure systems and their impacts to security and resilience

Cities have begun implementing “smart city solutions,” bridging cyber and physical infrastructure to advance and address resiliency challenges observed in the fields of healthcare, transportation, energy, utilities, safety, manufacturing, and environmental health (Habibzadeh, Nussbaum, Anjomshoa, Kantarci, & Soyata, 2019; Reimann et al., 2017). However, research has not adequately addressed both the positive and negative consequences to disaster response or resilience of using “smart systems” and “Big Data” in decision-making. While smart cities come with their benefits, such as safer roads and more efficient power generation, they also pose challenges related to increased vulnerability and risk, particularly as governments and private entities utilize increased data mining capabilities. Smart technology adoption will require tackling challenges around the use of “Big Data” and modeling or simulation tools that, for example, anticipate energy demands or personalize healthcare (Reimann et al., 2017).

Further inquiry is also needed into inequities and barriers associated with these complex urban environments, such as the “digital divide” between those who are able to utilize smart technology (e.g., older versus younger, rural versus urban), and ability for smart cities to engage all citizens (Reimann et al., 2017). RD&I initiatives focused on cyber-physical infrastructure systems should go beyond engineering and technocratic approaches and holistically integrate experts from the humanities and social science academic disciplines, as well as perspectives and participation from the public (Grady et al., 2021).

There is also limited research to identify how infrastructure system operations might benefit from “Big Data” in terms of sustainability, efficiency, and cost of delivering services. Digitization of decisions using “Big Data” and artificial intelligence (AI) has unknown impacts on social networks and raises ethical issues

NOTICE: This paper represents the consensus views of the RIPDWG and its recommendations to CISA, and as such does not necessarily represent the views, policy decisions, or findings of CISA, DHS, or the United States Government. The public release of this paper does not constitute or imply endorsement by the United States Government of the findings or recommendations, nor does it convey CISA’s commitment to any specific future course of action with respect to the paper’s findings and recommendations.

regarding privacy and transparency. Innovation should factor in people's concerns that may impact acceptance and applications of digital technologies (Reimann et al., 2017). Trust concerns further impact the feasibility of applying these technologies to their adoption and use in enhanced disaster response, recovery, or preparedness. An empirical understanding of how AI and related technologies operate in a real-life context would provide an evaluation of their impacts on existing municipal infrastructure, community acceptance, jobs, and local economies (Reimann et al., 2017).

Need 2.3 – Examination of workforce variables affecting the resilience of cyber-physical infrastructure systems

A National Counterintelligence and Security Center (NCSC) report (2021) identified humans as the biggest risk to the operation of cyber and physical systems, highlighting the need to identify workforce capabilities necessary to secure and maintain these increasingly complex systems and translate needed capabilities into training, educational curricula, and plans to sustain the workforce. (Hudnall, 2019). In addressing Climate Change, Executive Order 14008 (2021) also cites the vulnerability of infrastructure systems with an aging workforce and the need for a skilled workforce for sustainable infrastructure.

The COVID-19 pandemic revealed the importance of workers in sustaining and recovering the economy, health, and security of the Nation. Evident from this and other recent events, is the cascading consequences that can occur when the workforce is not considered as an important element in cyber and physical system operations. Important workforce factors that need to be understood through research include: a) mandated or voluntary absences that affect supply or delivery of essential goods and services; b) retirement of aging workers with operational knowledge of water, wastewater, and other infrastructure systems, especially in smaller and rural areas; c) workforce inequities widened by remote work; and d) shifting worker attitudes tied to a rapid escalation in trends such as automation and making workers contractors. There is also a need to research the impact of fragmented or conflicting state and federal regulatory regimes on worker and private sector locational choices and consequences of those changes to the delivery of critical supply chains, which were highlighted by the COVID-19 pandemic (Walsh, Haan, & Hewitt, 2021).

With the promise of federal infrastructure investment for growing a new skilled workforce, critical infrastructure RD&I must draw on a growing body of interdisciplinary research that tracks and anticipates changes to the workforce (Albertson, 2022), especially in small and rural communities and special districts with limited personnel. RD&I should also address the fiscal and other barriers to hiring and retaining cybersecurity and other infrastructure security professionals essential to the security and resilience of infrastructure systems, especially in regions with declining revenue.

Need 2.4 – Assessment of the consequences of underinvestment in infrastructure operation and maintenance on community security and resilience

A significant portion of the Nation's large infrastructure portfolio built in the previous century is at or beyond its originally expected lifespan, even as climate change, population growth, and other stressors increase demands on infrastructure systems. Achieving critical infrastructure resilience therefore requires confronting a multitude of stressors while addressing their impacts to already deteriorating infrastructure (USACE, 2021). Of particular concern is the underinvestment in infrastructure operation and maintenance, especially in underserved and rural communities where population declines have impacted the fiscal viability of public services. Research is needed to assess the implications of deferred maintenance from a systems perspective and understand the unequal capacity across communities to invest in the maintenance and operations of cyber-physical infrastructure providing essential public services. This research should address the causes, consequences, and geographic distribution of losses due to underinvestment in operation and maintenance of infrastructure systems.

Need 2.5 – Evaluation of the gap between intent and equitable delivery and outcomes of federal risk management and mitigation programs

Barriers are known to exist for achieving equitable outcomes with federal disaster and infrastructure investment programs (National Academies of Sciences, 2022). Place-based empirical research is needed on why technological innovations related to critical infrastructure resilience are or are not adopted or effective in different local and regional contexts. Research should also empirically examine the intended and unintended consequences and effectiveness of public and private preparedness, mitigation, response, and recovery programs. Research should evaluate pre- and post- disaster conditions in communities to measure the value of programs and the proper scale and timing of support, as well as the barriers to accessing and using these programs.

From such research, equity principles can be developed to measure equitable risk reduction by federal programs (Finucane, May, & Chang, 2021), which is essential to understanding whether those programs are meeting their functions to help build and improve resilience at the national scale. Research is also needed to identify any barriers that stand in the way of federal resources reaching vulnerable and low-capacity communities or limitations to equitable distribution of federal resources to make progress toward the enhanced resilience of communities. Achievement of more equitable outcomes also requires interrogating the application of the terms “whole community” and “community,” which are increasingly incorporated into federal disaster and resilience related program guidelines and funding requirements.

Applied research should correlate community equity-based vulnerability and the location of communities in relation to the cyber-physical systems that support critical services. Identified needs should then be compared to the distribution of federal and state resources with analysis to identify why any major gaps exist between policy and access.

Strategic RD&I Actions

National policy calls for prioritizing infrastructure investment and risk mitigation to reduce consequences to disadvantaged communities (The White House, 2021). Federal research should adopt a multidisciplinary approach to provide all federal agencies with the best understanding of how National security relies on the resilience of social and environmental systems, as well as physical and cyber infrastructure systems. This begins with an understanding of behavioral factors in risk management outcomes and the application of a societal resilience construct, such as the one recently developed under the auspices of the NSTC Subcommittee on Resilience Science and Technology (SRST) that frames science and technology needed in cyber-physical infrastructure research and development (National Science and Technology Council, 2023). Given the primary responsibility of state, local, tribal, and territorial governments for public services, research should investigate the impacts of current federal programs on SLTT actions to identify more effective roles for the federal government in overcoming barriers to the security and resilience of the critical services vital to communities. Strategic RD&I priorities should:

2.A Identify gaps in what is needed to support an infrastructure workforce into the future considering the aging workforce, licensing requirements, technical capacity, economic sustainability, and location of labor. This would include understanding the impact of workforce changes on critical infrastructure security and resilience within different regional economies.

NOTICE: This paper represents the consensus views of the RIPDWG and its recommendations to CISA, and as such does not necessarily represent the views, policy decisions, or findings of CISA, DHS, or the United States Government. The public release of this paper does not constitute or imply endorsement by the United States Government of the findings or recommendations, nor does it convey CISA’s commitment to any specific future course of action with respect to the paper’s findings and recommendations.

2.B Analyze unanticipated vulnerabilities and implications of technology innovation for preparedness, response, recovery, mitigation, and adaptation to emerging threats and stressors across different U.S. regions.

2.C Apply mixed qualitative, quantitative, and spatial analysis sources and methods to develop a shared baseline of information on how historic and current demographic, geographic, and institutional capacity stressors have resulted in vulnerabilities and inequitable consequences of hazard events and disruptions to essential services provided by state, local, tribal, and territorial governments, in addition to the private sector.

a. Assess the local and regional social and institutional barriers to addressing emerging threats/hazards to infrastructure and corresponding impacts to essential services in the context of “smart technology” trends.

b. Assess the causes and consequences of underinvestment in infrastructure operation and maintenance under future threat scenarios to define policy obstacles and preparedness intervention points for enhanced system security and resilience at the state and federal levels. Include in research the state, local, tribal, and territorial governments and associations of communities that have direct interests in infrastructure operations and financing.

c. Research questions should address interconnections between societal and physical resilience, such as how at-risk and vulnerable populations might be impacted by disruptions of different critical infrastructure sectors and the essential services they support.

2.D Examine how AI and related technologies operate in a real-life context to measure benefits and potential consequences to the security and resilience of infrastructure services provided by the public and private sector or regulated by municipalities, counties, state, and territorial governments.

2.E Identify and empirically test the principles of resilient design and adaptive risk management including private sector and local government trends, methods, and best practices. Identify case studies and examples of resilient design, construction, materials science, and investment innovations, principles, and applied research to test effectiveness for infrastructure resilience and sustainability outcomes and metrics defined at the national, state, and local levels.

Research Gap 3: User-engagement in cyber-physical infrastructure research to translate resilience knowledge into effective action at the local and regional level

The escalating pace of combined physical and cyber threats and the differences in public and private capacities to manage consequences requires a revised approach to RD&I that supports local and regional action across scales and sectors in real time. To broaden its ability to inform decision-making and action at the local and regional scales, federal infrastructure resilience RD&I needs to foster user-engaged research methods that include decision-makers and vulnerable communities in producing usable knowledge that facilitates inclusion and collaboration to address shared systems and vulnerabilities. The application of participatory and collaborative co-production research methods to climate change adaptation has demonstrated their utility for generating shared and usable knowledge to address a changing threat environment, thus closing the gap between knowledge and action. Principles of knowledge co-production have also been shown to foster inclusion and enable the development of collaborative relationships and trust needed for adaptive management to address the changing risk

NOTICE: This paper represents the consensus views of the RIPDWG and its recommendations to CISA, and as such does not necessarily represent the views, policy decisions, or findings of CISA, DHS, or the United States Government. The public release of this paper does not constitute or imply endorsement by the United States Government of the findings or recommendations, nor does it convey CISA's commitment to any specific future course of action with respect to the paper's findings and recommendations.

landscape across interests, jurisdictional boundaries, and scales. Effective risk management research and development requires application of these methods, referred to herein as "co-production," to address some of the following RD&I needs.

RD&I Needs

Need 3.1 – Evidence-based examination of co-production methods to support decision-making related to infrastructure resilience

Co-production refers to the process of involving diverse and non-academic stakeholders in the knowledge generation and research process to ensure that research is collaborative, context-driven, and problem-focused (Norström et al., 2020). Research guided by co-production principles promises to generate new knowledge, but will also lead to improvement in social capital, as well as network and capacity building (Norström et al., 2020). Such methods are largely missing in research priorities addressing the resilience of cyber-physical infrastructure systems, which limits the relevance of such research. Co-production methods are context-based, pluralistic (encompassing different ways of knowing and doing), goal-oriented, and interactive (Norström et al., 2020), include the data requirements of both impacted communities and system decision-makers, and involve participants that represent a range of skills and knowledge types (e.g., indigenous, experiential, technical, etc.) (Norström et al., 2020). The nature of co-produced research in this context means that it should be conducted jointly with communities who can bring not only their own technical, experiential, and other types of knowledge, but also help ensure that interests of their diverse citizenry are being considered throughout the research process (Norström et al., 2020).

In addition, there is a need to structure research designs to engage intermediary organizations, such as local non-profits and trusted groups that engage rural and low-capacity communities in resilience decision-making in the development and execution of this research, given inequities or documented mistrust of many communities to government "solutions" (Davis et al., 2022).

Need 3.2 – Empirical investigation to identify factors that enable community-driven resilience of cyber-physical infrastructure

Research is needed to understand institutional and social factors that influence how and why some communities sustain and/or recover critical infrastructure systems and supported services without federal intervention; recent empirical studies point to social capital and civic institutions that are not designed into policy and programs. Additionally, to empirically understand mechanisms that drive community success in recovery and resilience, research and development should also assess the sources of knowledge that communities rely on and trust for decision-making. For example, studies in rural settings have shown that local non-governmental organizations are often favored over state- or federal-level organizations as partners in post-hazard relief efforts (Davis et al., 2022)—additional empirical and comparative research would further understanding of this phenomenon. Such research could also identify trusted, effective, and long-term intermediaries that have or could be supported by federal initiatives to result in knowledge and solution sharing within and among communities and infrastructure owners and operators. Such intermediaries may include land-, sea-, and space-grant universities, Minority Serving Institutions, federally sponsored yet regionally oriented organizations (e.g., Regional Planning Commissions, Metropolitan Planning Organizations, Economic Development Councils, etc.), and other entities. Collaboration across these entities is needed to better understand the resilience of cyber-physical infrastructure systems from the perspective of communities and stakeholders operating at the local level.

Need 3.3 – Empirical investigation of how the regulatory system may constrain or enable enhancements to the resilience of cyber-physical infrastructure

Interdisciplinary resilience research has identified the importance of measures that balance regulation and requirements with flexibility to encourage innovation and adaption to changing conditions. Policies meant to provide for efficient and effective continuity or restoration of services, may under certain disaster scenarios either assist in improving infrastructure resilience or exacerbate restoration challenges because of interdependencies or other unforeseen factors. Differences in public utility commission or licensing rules and authorities affect the financing and workforce for system operation and maintenance in growing, as well as financially disadvantaged areas. Adoption of uniform building codes may be limited in effect when adoption is uneven (National Academies of Sciences, 2022) or affected by other regulations such as land use plans and zoning. Industrial legacy codes and public sector regulations can also impede innovation and the flexibility needed to adapt to changing risks. Research is needed to address the benefits and potential constraints, both intentional and unintentional, of state and local regulatory contexts and industry standards on innovations to enhance the resilience of cyber-physical infrastructure systems.

Empirical research should compare policy goals with outcomes in different contexts to inform improvements to current policies, programs, and regulations. Related research is also needed to understand the necessary incentives for risk reduction regulatory reform and investments across the national partnership, as identified in the FY 2021 National Defense Authorization Act Section 9002(b) Report (Cybersecurity and Infrastructure Security Agency, 2021). Similarly, research is needed to understand how a trend toward consolidated private sector ownership and operation of public goods may affect community and national resilience.

Need 3.4 – Identify the institutional conditions for effective infrastructure governance and adaptive capacity

The increased complexity of cyber-physical infrastructure systems necessitates coordinated actions and institutions not only at the national level, but among the public and private decision-makers that depend on shared cyber and physical infrastructure systems across sectors (e.g., public, private, non-governmental, and non-profit), scales (regional, state, national, and global), CI domains (water, energy, transportation, etc.), mission goals, and value chains (Reimann et al., 2017). Institutions for collective action are absent. Assets, systems, and networks are the responsibility of multiple public and private stakeholders and consequences of disruptions are unequally distributed. A growing body of research on collective action, conflict management, and adaptation to climate change should be applied to the governance of physical and cyber systems and critical services to address information sharing, cost-sharing mechanisms, sustaining transboundary cooperation, and adaptation to technological advancements and pace of innovation (OECD, 2019).

Effective governance for continually evolving threats requires a shared focus on retaining core societal functions and evolution of institutions to manage systems that cross authorities. A growing multidisciplinary body of resilience and climate change research has documented methods that support adaptive capacity—effective response to changing threats and stressors to retain core functions. Adaptive capacity is enhanced when knowledge is co-produced by scientists, impacted groups, and decision-makers across relevant jurisdictions and sectors (Innes and Booher, 2010; Margerum, 2011; Chaffin et al., 2014). Infrastructure resilience RD&I should incorporate political economy research on "polycentric"

NOTICE: This paper represents the consensus views of the RIPDWG and its recommendations to CISA, and as such does not necessarily represent the views, policy decisions, or findings of CISA, DHS, or the United States Government. The public release of this paper does not constitute or imply endorsement by the United States Government of the findings or recommendations, nor does it convey CISA's commitment to any specific future course of action with respect to the paper's findings and recommendations.

governance systems and institutions that can convene public and private entities across system geographies (Stephan et al., 2019; Ostrom, 2012).

For the development of shared principle and policies to build institutional capacity to govern cyber and physical risk, research should examine both successful and failed attempts to align decisions for ports, energy, transportation, and other critical systems on which continuity of services depend. In addition, because resilience in a changing threat landscape requires shifting the goals from threat prevention to retaining functions and reducing costs and consequences, research is needed to identify shared principles and the conditions that can help sustain collaborative risk management actions.

Ensuring participation of local communities and the role they play in larger decision-making carried out by governments and private sector owners and operators will require an in-depth look at risk governance approaches (OECD, 2019). Future research needs to address the barriers to participation in cyber-physical infrastructure policy, the extent to which existing policies meaningfully incorporate equity and interests of vulnerable populations, and opportunities for industry partners and communities to build trust and collaborate on shared goals.

In addition, research should consider how to apply governance flexibility and informal institution-building lessons learned from the COVID pandemic response to planning efforts focused on enhancing the resilience of cyber-physical infrastructure to other types of hazards. A synthesis of government evaluations of COVID response indicates that measures to coordinate a “whole-of-society response” need to be further analyzed to understand how governance decentralization mechanisms, including engaging stakeholders and cooperating across levels of government, in combination with national leadership can be adapted to prepare for and manage multiple types of future hazards (OECD, 2022).

Strategic RD&I Actions

To realize the security and resilience goals outlined in the National Infrastructure Protection Plan, federal RD&I addressing the resilience of cyber-physical infrastructure must more effectively build on existing multi-disciplinary knowledge to inform research questions, design, and methodologies. Inclusion of participatory and co-production methods can be used to engage the public and diverse disciplines (social as well as physical and natural sciences and engineering) in federal research to work across communities, sectors, and boundaries for shared knowledge and improved resilience outcomes. Federal RD&I activities should prioritize the following actions:

3.A Work with private as well as public academies and institutes in the full development of a research agenda to develop and apply methods to co-produce knowledge with communities and users to improve relevance and use of knowledge in decision-making. Innovative use of co-production methods with historically marginalized communities should be examined for applications to risk assessment and enhancing the application of research to critical infrastructure security and resilience investments and actions.

3.B Examine the institutional and regulatory context of risk management and long-term cyber and physical infrastructure decisions against the requirements for adaptive management of systems under a changing and complex risk environment.

a. Map the authorities, institutions, and entities responsible for governing and managing decisions to change infrastructure operations, location, and investments in security and resilience. Identify the institutions that the federal government could use to encourage

NOTICE: This paper represents the consensus views of the RIPDWG and its recommendations to CISA, and as such does not necessarily represent the views, policy decisions, or findings of CISA, DHS, or the United States Government. The public release of this paper does not constitute or imply endorsement by the United States Government of the findings or recommendations, nor does it convey CISA’s commitment to any specific future course of action with respect to the paper’s findings and recommendations.

the types of shared governance (public/private/geographic) necessary for overcoming fragmented authorities for action.

b. Assess and characterize existing programs, methods, and models of successful and effective collaboration and integration between levels of government, agencies, sectors, and disciplines that can be incorporated into the National Infrastructure Protection Plan.

c. Define and support research into how regulatory bodies and rules stymie or encourage innovation for enhanced cyber and physical infrastructure service resilience. Examine how fragmented or conflicting state and federal regulatory regimes affect infrastructure investment choices, such as where systems are constructed and availability of qualified workers. Also examine consequences of the regulatory environment on local and regional adaptation to multiple threats and the delivery of critical supply chains.

3.C Conduct comparative empirical resilience case studies of both non-federal and federally supported resilience initiatives. Such studies should identify context-based and transferable resilience enhancement facilitator and barrier factors by capturing the dynamic adaptation/response of communities to infrastructure disruption challenges. Studies should also identify successful approaches to cyber-physical resilience and adaption to technology (Reimann et al., 2017) toward identifying conditions contributing to security and resilience that can be supported by federal policy and programs.

Conclusion

Addressing the critical infrastructure resilience RD&I needs outlined in this paper is paramount for advancing national priorities in a holistic manner. It is of highest priority to conduct research and development necessary to achieve the policy goals of the Infrastructure Investment and Jobs Act and corresponding implementation guidance in Executive Order 14052 to achieve long-term and equitable national security and resilience. Exponential increases in risks to national security are due to the combined effects of escalating natural and human threats to both physical and cyber systems, the escalating reliance of operations and critical services on cyber systems, disparities in capacity to invest in operation and maintenance and upgrades due to social, economic, and educational disparities, and the escalating and unequal reliance on cyber systems. The federal government must undertake an integrated approach to research and development that is designed to build the capacity of infrastructure partners at all levels to understand and apply research to retain essential social, economic, health, and security functions in the face of constant change. With the added threats of climate change and cyber-attacks that escalate costs and derail old recovery strategies, the research and development paradigm must shift from each sector defining problems based on past events to collective establishment of priorities that can increase the capacity of the Nation at all levels to maintain essential services in the face of change—to adapt. Multi-disciplinary teams across the scientific community are developing this type of integrated, place-based, and applied research in tandem with vulnerable communities, governments, and the private sector. The strategic RD&I actions identified in this paper should be considered by mission partners across the interagency to position the federal government – in collaboration with stakeholders across all levels – to solve the most pressing current and future challenges facing the Nation.

References

Albertson, K. (2022). Labor pains reveal a ‘systems change’ for workforce: Supply chain industry scrambles to keep workers amid 'Great Resignation'. *ISE: Industrial & Systems Engineering at Work, 54*(7), 28-33. Retrieved from https://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=157451044&site=ehost-live

Barker, K., Lambert, J. H., Zobel, C. W., Tapia, A. H., Ramirez-Marquez, J. E., Albert, L., . . . Caragea, C. (2017). Defining resilience analytics for interdependent cyber-physical-social networks. *Sustainable and Resilient Infrastructure, 2*(2), 59-67. doi:10.1080/23789689.2017.1294859

Browder, G., Ozment, S., Bescos, I. R., Gartner, T., & Lange, G.-M. (2019). *Integrating Green and Gray: Creating Next Generation Infrastructure*. Washington, DC: World Bank Group and World Resources Institute.

Chaffin, B., Gosnell, H., & Cosens, B. (2014). A decade of adaptive governance scholarship: synthesis and future directions. *Ecology and Society.* 19(3):56. doi:10.5751/ES-06824-190356

Connor, D. S., Gutmann, M. P., Cunningham, A. R., Clement, K. K., & Leyk, S. (2019). How Entrenched Is the Spatial Structure of Inequality in Cities? Evidence from the Integration of Census and Housing Data for Denver from 1940 to 2016. *Annals of the American Association of Geographers, 110*(4), 1022-1039. doi:10.1080/24694452.2019.1667218

Cybersecurity and Infrastructure Security Agency. (2021). *FY 2021 National Defense Authorization Act: Section 9002(b) Report*.

Davis, C. R., Griffard, M. R., Burton, A., Weinberg, J., Kaneria, K., Smith, M., . . . Barnes, T. (2022). A Band-Aid fix to a problem that's going to be persistent: The influence of social place attachment on rural residents' perceptions of natural hazard relief efforts. *International Journal of Disaster Risk Reduction, 67*. doi:10.1016/j.ijdrr.2021.102640

Executive Order 13985. (January 20, 2021). *Advancing Racial Equity and Support for Underserved Communities Through the Federal Governmen*t. 86 Fed. Reg. 14

Executive Order 14008. (January 27, 2021). *Tackling the Climate Crisis at Home and Abroad*. 86 Fed. Reg. 19

Executive Order 14052. (November 15, 2021). *Implementation of the Infrastructure Investment and Jobs Act*. 86 Fed. Reg. 220

Finucane, M. L., May, L. W., & Chang, J. (2021). *A Scoping Literature Review on Indicators and Metrics for Assessing Racial Equity in Disaster Preparation, Response, and Recovery*. Retrieved from https://www.rand.org/pubs/research_reports/RRA1083-1.html

Grady, C., Rajtmajer, S., & Dennis, L. (2021). When Smart Systems Fail: The Ethics of Cyber–Physical Critical Infrastructure Risk. *IEEE Transactions on Technology and Society, 2*(1), 6-14. doi:10.1109/tts.2021.3058605

Greer, C., Burns, M., Wollman, D., & Griffor, E. (2019). *Cyber-Physical Systems and Internet of Things NIST (Special Publication 1900-202)*. Retrieved from https://doi.org/10.6028/NIST.SP.1900-206

Habibzadeh, H., Nussbaum, B. H., Anjomshoa, F., Kantarci, B., & Soyata, T. (2019). A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. *Sustainable Cities and Society, 50*. doi:10.1016/j.scs.2019.101660

Hallegatte, S., Rentschler, J., & Rozenberg, J. (2019). *Lifelines: The Resilient Infrastructure Opportunity (Vol. 2) (English)*. Retrieved from http://documents.worldbank.org/curated/en/111181560974989791/Lifelines-The-Resilient-Infrastructure-Opportunity

NOTICE: This paper represents the consensus views of the RIPDWG and its recommendations to CISA, and as such does not necessarily represent the views, policy decisions, or findings of CISA, DHS, or the United States Government. The public release of this paper does not constitute or imply endorsement by the United States Government of the findings or recommendations, nor does it convey CISA’s commitment to any specific future course of action with respect to the paper’s findings and recommendations.

Heino, O., Takala, A., Jukarainen, P., Kalalahti, J., Kekki, T., & Verho, P. (2019). Critical Infrastructures: The Operational Environment in Cases of Severe Disruption. *Sustainability, 11*(3). doi:10.3390/su11030838

Hudnall, M. (2019). Educational and Workforce Cybersecurity Frameworks: Comparing, Contrasting, and Mapping. *Computer, 52*(3), 18-28. doi:10.1109/mc.2018.2883334

Innes, J. and Booher, D. (2010). *Planning with complexity: An introduction to collaborative rationality for public policy*, 2nd edition. New York: Routledge.

Karakoc, D. B., Barker, K., Zobel, C. W., & Almoghathawi, Y. (2020). Social vulnerability and equity perspectives on interdependent infrastructure network component importance. *Sustainable Cities and Society, 57*. doi:10.1016/j.scs.2020.102072

Margerum, R. (2011). *Beyond consensus: Improving collaborative planning and management*. Boston: MIT Press

National Academies of Sciences, Engineering, and Medicine. (2022). *Equitable and Resilient Infrastructure Investments*. Washington, DC: The National Academies Press. https://doi.org/10.17226/26633

National Science and Technology Council. (2023). *Resilience Science and Technology Grand Pathways Framework*. Retrieved from https://www.whitehouse.gov/ostp/news-updates/2023/03/22/nstc-resilience-science-and-technology-grand-pathways-framework/

Norström, A. V., Cvitanovic, C., Löf, M. F., West, S., Wyborn, C., Balvanera, P., . . . Österblom, H. (2020). Principles for knowledge co-production in sustainability research. *Nature Sustainability, 3*(3), 182-190. doi:10.1038/s41893-019-0448-2

OECD. (2019). *Good Governance for Critical Infrastructure Resilience*. Paris: OECD Publishing.

OECD. (2022). *First lessons from government evaluations of COVID-19 responses: A synthesis*. Retrieved from https://www.oecd.org/coronavirus/policy-responses/first-lessons-from-government-evaluations-of-covid-19-responses-a-synthesis-483507d6/

Office of the Director of National Intelligence. (2022). *Annual Threat Assessment of the U.S. Intelligence Community*. Retrieved from https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2022/item/2279-2022-annual-threat-assessment-of-the-u-s-intelligence-community

Ostrom (2012). Nested Externalities and Polycentric Institutions: Must We Wait for Global Solutions to Climate Change Before Taking Actions at Other Scales? *Economic theory* 49 (2): 353–69.

Prysm Group. (2021). *Cybersecurity Economic Research Proposal: Cybersecurity Incentive Structures Analytical Model, Policy Recommendations Whitepaper, and Cybersecurity Financing Model*. Retrieved from Confidential and Internal Report.

Reimann, M., Rückriegel, C., Mortimer, S., Bageritz, S., Henshaw, M., Siemieniuch, C., . . . Juan Rico, J. A. (2017). *Road2CPS: Priorities and Recommendations for Research and Innovation in Cyber-Physical Systems*.

Resilient Investment Planning and Development Working Group. (April 1, 2022) *Research & Development Task Group Meeting*.

Roshanaei, M. (2021). Resilience at the Core: Critical Infrastructure Protection Challenges, Priorities and Cybersecurity Assessment Strategies. *Journal of Computer and Communications, 09*(08), 80-102. doi:10.4236/jcc.2021.98006

SecurityWeek News. (2021). Continuous Updates: Everything You Need to Know About the SolarWinds Attack. *SecurityWeek*. https://www.securityweek.com/continuous-updates-everything-you-need-know-about-solarwinds-attack/

NOTICE: This paper represents the consensus views of the RIPDWG and its recommendations to CISA, and as such does not necessarily represent the views, policy decisions, or findings of CISA, DHS, or the United States Government. The public release of this paper does not constitute or imply endorsement by the United States Government of the findings or recommendations, nor does it convey CISA's commitment to any specific future course of action with respect to the paper's findings and recommendations.

Stephan, M., Marshall, G., and McGinnis, M. (2019). An introduction to polycentricity and governance. In *Governing Complexity*. New York: Cambridge University Press, Chap. 1, 11-21-44.

The National Counterintelligence and Security Center. (2021). *Insider Threat Mitigation for U.S. Critical Infrastructure Entities: Guidelines from an Intelligence Perspective*. Retrieved from https://www.dni.gov/index.php/ncsc-newsroom/item/2197-insider-threat-mitigation-for-u-s-critical-infrastructure-entities-guidelines-from-an-intelligence-perspective

The White House. (July 20, 2021). *Justice40 A Whole-of-Government Initiative*. Retrieved from https://www.whitehouse.gov/environmentaljustice/justice40/

The White House. (March 2023). *National Cybersecurity Strategy*. Retrieved from https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

U.S. Army Corps of Engineers. (2021). Research & Development Strategy: Laying The Foundation For a New Bold Era of USACE R&D. Retrieved from https://usace.contentdm.oclc.org/digital/collection/p16021coll11/id/5457

U.S. Department of Homeland Security. (2013). *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*. Retrieved from https://www.cisa.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience

U.S. Department of Homeland Security. (2015). *National Critical Infrastructure Security and Resilience Research and Development Plan*. Retrieved from https://www.dhs.gov/sites/default/files/publications/National%20CISR%20R%26D%20Plan_Nov%202015.pdf

U.S. Department of Homeland Security. (2021). *National Preparedness Report*. Retrieved from https://www.fema.gov/sites/default/files/documents/fema_2021-national-preparedness-report.pdf

U.S. Department of Homeland Security. (2022). *Critical Infrastructure Security and Resilience Research, Development, Test, and Evaluation (CISRR) Strategy Framework.*

U.S. Government Accountability Office. (2021). *Critical Infrastructure Protection: CISA Should Assess the Effectiveness of its Actions to Support the Communications Sector*. (GAO-22-104462). Retrieved from https://www.gao.gov/products/gao-22-104462

Walsh, D., Haan, M., & Hewitt, C. (2021). Working Without Fixity: Accounting for a Mobile Workforce. *The Journal of Rural and Community Development, 16*(3), 133–156.