NIAC The National Infrastructure Advisory Council

PROMOTING INFRASTRUCTURAL HEALTH:

Proactive strengthening of investment strategies, analytic capabilities, training paradigms, and performance standards to bolster preparedness across public infrastructure

December 2024

Table of Contents

About the NIAC

The President's National Infrastructure Advisory Council (NIAC or the Council) is composed of senior executives from industry and state and local government who own and operate the critical infrastructure essential to modern life. The Council was established by executive order in October 2001 to advise the President on practical strategies for industry and government to reduce complex risks to the designated critical infrastructure sectors.

At the President's request, NIAC members conduct in-depth studies on physical and cyber risks to critical infrastructure and recommend solutions that reduce risks and improve security and resilience. Members draw upon their deep experience, engage national experts, and conduct extensive research to discern the key insights that lead to practical Federal solutions to complex problems.

For more information on the NIAC and its work, please visit: https://www.cisa.gov/niac.

1. Executive Summary

By centering efforts on the paradigm of health and its relationship to preparedness, we can better articulate the necessity for national commitments that prioritize prospective risk assessment and threat mitigation as a guide to strategic targeting of resource allocation, while continuing to enhance our crisis response capabilities.

Promoting infrastructural health, much like promoting human health, requires altering traditional focus from reactive responses at a particular time and place to interventions aimed at continuous prevention across the national physical and digital footprints. This approach calls for a collective mindset shift in how we think about, invest in, and manage our nation's critical infrastructure. The concept of infrastructural health promotion offers a powerful framework that can engage multiple stakeholders—from high-level policymakers to local citizenry—in meaningful discourse and decision-making processes.

Enhancing the readiness of our infrastructure to avoid or withstand incursions requires a proactive, rather than reactive, approach, one that harnesses the opportunity to incentivize and support stronger private sector engagement, addresses the complex interdependencies between sectors, emphasizes structured training and highly reliable insight sharing, and implements Federally mandated capability standards and performance metrics.

The approach to solution-building for these challenges contains the following five interwoven initiative categories that also reflect points of cross-linkage and overall continuity with other NIAC reports published in 2023 and 2024:

1) ***Enhancing insights*** into threats, risks, and capabilities in relation to preparedness
2) ***Establishing insight-driven standards of performance*** within and across sectors
3) ***Training formally and regularly*** on insight-driven standards, targeting iteratively refined, baseline cross-sector functionalities
4) ***Asserting the Federal government's direction*** consistent with standards, harmonizing with state, local, tribal, and territorial (SLTT) entities
5) ***Realigning incentives for private sector investments*** of capital and capabilities

The recommendations submitted in this report do not express a unidirectional, linear process that, once launched, runs to some point of completion and awaits future reactivation of the same sequence after an interlude of quiescence. Instead, they constitute elements of an ongoing, virtuous cycle of continuous learning and adaptation fueled by feedback loops between each element and every other.

2. Introduction

2.1 The NIAC's Charge

The National Security Council (NSC) tasked the NIAC to address the theme of infrastructural health and investigate key questions as indicated below:

> *The NIAC will develop a framework for promoting proactive infrastructure health that is crosslinked to national standards priorities and leverages public and private sector collaborative investments, innovative financial instruments, and analytics to anticipate vulnerabilities in service to broadly enhancing preparedness and, by extension, reliability across critical infrastructure:*
>
> - *What can the Federal government do to incentivize and support private sector investments in resilient infrastructure?*
> - *How can those investments be linked to existing and future national standards?*
> - *How can artificial intelligence (AI) and related technological innovations be leveraged to support these efforts?*

The Promoting Infrastructural Health Subcommittee was established to undertake this task. The Subcommittee consisted of 21 members; a full list of whom can be found in Appendix A. Dr. Conrad Vial was designated as the Subcommittee Chair.

2.2 Subcommittee Activities

The Subcommittee held meetings on the following dates:

February 12, 2024 – Planning meeting

February 20, 2024 – Virtual kickoff meeting

March 8, 2024 – Planning meeting

March 22, 2024 – Subcommittee meeting featured briefings by Phillip Hinson, Professional Engineer (P.E.), M.ASCE (Member, American Society for Civil Engineers); and David Totman, Infrastructure Industry Strategist.

April 5, 2024 – Subcommittee meeting featured a briefing by Tyler Reeder, Managing Partner, Energy Capital Partners.

April 19, 2024 – Subcommittee meeting featured briefings by Josh Corman, Founder, I Am The Calvary; Jackie Monson, Senior Vice President and Chief Integration Officer, Sutter Health; and Eva Lerner-Lam, President, Palisades Consulting Group.

May 3, 2024 – Subcommittee meeting featured a briefing by Ben Djiounas, Managing Director, J.P. Morgan.

May 17, 2024 – Subcommittee meeting featured a briefing by Deneen DeFiore, Vice President and Chief Information Security Officer (CISO), United Airlines.

May 31, 2024 – Subcommittee Report Discussion

June 14, 2024 – Subcommittee meeting featured a briefing by Lisa Einstein, Chief Artificial Intelligence Officer, CISA.

June 27, 2024 – Subcommittee meeting featured a briefing by Manny Cancel, Chief Executive Officer, Electricity Information Sharing and Analysis Center (E-ISAC).

August 9, 2024 – Subcommittee meeting featured briefings by Brian Mazanec, Deputy Director, Administration for Strategic Preparedness and Response (ASPR) Center for Preparedness; and CDR Thomas Christl, Director, Office of Critical Infrastructure Protection.

August 23, 2024 – Subcommittee meeting featured briefings by Jeffrey Thompson, CEO, DC Water; and Eric Rollison, Assistant Director for Risk Analysis, Resilience and Recovery, Department of Energy.

September 6, 2024 – The Subcommittee met to have a general discussion.

September 20, 2024 – The Subcommittee met to discuss the topic of finance.

September 24, 2024 – The Subcommittee met to discuss the topic of threat modeling.

September 30, 2024 – The Subcommittee met to discuss the topic of standards.

October 2, 2024 – The Subcommittee met to discuss the topics of data and analytics.

October 10, 2024 – The Subcommittee met to discuss the topic of public/private partnerships.

October 18, 2024 – The Subcommittee met to review the current draft of the report.

November 1, 2024 – The Subcommittee met to discuss final report edits and review for submission.

2.3 Organization of this Report

The remainder of this report is organized into the following sections:

Key Themes and Findings: This section introduces:

- A framework to guide discovery and analysis, including:
  - The concept of health in relation to resilient infrastructure
  - Brief case studies illustrating gaps in infrastructure health
- Considerations and lessons from key perspectives, including:
  - Public and private sector collaboration
  - Data management and analytical capabilities
  - Cross-sector considerations
  - Synthesis of research findings

Recommendations: This section presents the NIAC's recommendations in detail.

Call to Action: This section offers a final word on the significance and impact of promoting infrastructural health.

3. Key Themes and Findings

3.1. Framework to Guide Discovery and Analysis

3.1.1. The concept of health in relation to sustainably resilient infrastructure

Applying the paradigm of health promotion to the domain of infrastructure resilience is not intended merely as an attractive metaphor but rather as a strategic approach that galvanizes diverse stakeholders—ranging from policymakers at every level to the public—into a unified effort to strengthen national infrastructure readiness. By comparing infrastructure to a living system that requires ongoing care, maintenance, and proactive measures to ensure its "health," we can foster a more compelling commitment to the importance of preparedness as a key input to enhanced resilience.

As early in recorded human history as the 5th century BCE, Hippocrates (whose name still proclaims the physician's oath in medical tradition) advised that to learn about the health of a population one must "look to the air they breathe, to the water they drink, and to the places where they live." Human health thus reflects the resilience of sociobiological systems in the face of acute and chronic threats – whether they emerge from disease, injury, or environmental stressors. That resilience, in turn, hinges not merely on sociobiological response to adversity but, perhaps even more crucially, on capabilities to avoid and mitigate such adversity in the first instance. Just as the human body relies on a complex, interconnected ecosystem to maintain health, so too does our societal infrastructure revolve around an interdependent network of physical assets, digital capabilities, and partnerships to sustain the well-being, security, and prosperity of our nation. The resilience of our country's infrastructure is therefore largely a reflection of how prepared it is to better resist, withstand, and recover from multifaceted challenges—ranging from the impacts of climate change to physical and cyberattacks, from mitigating human process gaps to responsibly implementing technological advances, and from equitably engaging community needs to prioritizing coordination of investments and resource utilization. In this context, preparedness, at the core of infrastructure health, is about implementing novel tools and methodologies while bolstering interdependent relationships. It is also about framing the conversation compellingly in terms of the urgency of replacing or upgrading aging infrastructure sustainably and comprehensively, rather than through the deployment of well-intended but ultimately uncoordinated point solutions. For example, the Hippocratic concept of community or population-level health might well initiate progress via predictive analytical methodologies permitting anticipation of the socioecological effects of climate change. These would then provide impetus for a holistic engineering analysis that includes, for instance, adaptive building code changes[1]. Establishing a curated set of new standards for guiding asset enhancement or replacement would, in turn, inform thoughtful civic decision-making regarding setting targets for new construction and retrofit alternatives and, ultimately, would be complemented by incentive-alignment paradigms to activate coordinated public and private sector investments of capital and expertise. The end goal is to bring about a healthier status with focused rigor, accountability, and pace. Similar approaches to all sectors – essentially, all composed and guided by what we might think of as the anatomy, physiology, and psychology of a living system or, more appropriately, a system of systems – would benefit the preparedness of our nation's portfolio of physical assets and that of its digital infrastructure.

[1] "ASCE NOAA Taskforce." 2024. ASCE.org. 2024.

3.1.2. Brief case studies illustrating gaps in infrastructure health

Although the World Health Organization has expressly defined health as “more than the mere absence of infirmity,” illustrations of ill-health often serve the purpose of bringing into relief what the healthy state can hope to avoid. The following case studies portray different types of inputs and outputs for failure analysis. However, they are ultimately related by the same underpinning dynamic; namely, the erosion of dynamic systems fostered by inattention to sources of predictable vulnerability and relative absence of proactive risk mitigation strategies.

Inattention to unintended consequences of well-intentioned but misguided resource management policies:

To be sure, wildfires have impacted multiple regions of the national footprint such that the implications reach beyond any single segment of our communities. However, to illustrate key aspects of a more general case, California’s recent experiences are notable in multiple ways. California wildfire incidents, often described as an "epidemic," have reached unprecedented frequency and severity in recent years, with devastating impacts on communities, ecosystems, and economies across the state. Contrary to what is most loudly publicized, these wildfire incidents have not been driven solely by the widely acknowledged factors of climate change and the mismanagement of electrical power lines by energy companies. Instead, they are also deeply rooted in a broader set of deficiencies across multiple sectors, revealing significant gaps in ecological stewardship as well as infrastructure health. Ill-conceived forestry practices have been a critical determinant in escalating wildfire risk. Historical ecosystem mismanagement, including the suppression of natural fires and a lack of proactive forest thinning, has led to overly dense forests that are primed for catastrophically amplified blazes. Failing to implement more sustainable forest management practices, such as controlled burns and selective logging, has left California’s forests in a precarious state, where small sparks can quickly escalate into massive infernos.

Environmental policies have also contributed to this crisis. In many cases, these policies have been overly restrictive, limiting the ability to perform necessary forest maintenance. An essentially “no-touch” ecosystem ethos often has neglected the need for active management, leading to the buildup of flammable materials. Additionally, single-minded efforts to protect endangered species has sometimes inadvertently increased fire risk by preventing necessary clearing operations. Finally, poor land use planning has permitted, in many instances, overdevelopment in areas prone to fire risk based on emergent climate change impacts, among other drivers, thereby straining the availability of fire risk mitigating resources, interventions, or conditions. The human toll of these wildfires is staggering. Scores of communities have been directly affected, with tens of thousands losing their homes and businesses, and many more facing health impacts from smoke and pollution. The economic costs are similarly immense, with billions of dollars in property damage, firefighting expenses, and economic disruptions. Moreover, the environmental costs are severe, with significant damage to water supplies and aquatic ecosystems, as runoff from burned areas pollutes rivers and reservoirs, affecting both human consumption and wildlife.

Constraining vulnerabilities on inputs while avoiding single points of failure on outputs:

The 2024 ransomware attack on Change Healthcare, a subsidiary of UnitedHealth Group, represents one of the most severe cyber incidents in the U.S. healthcare sector. The attack exposed the sensitive health information of over 100 million individuals, nearly one-third of the American population. The breach was facilitated by a critical failure to implement multi-factor authentication on a key server, compounded by inadequate network segmentation and privileged account management practices. The ramifications were

extensive, disrupting healthcare operations nationwide. Providers faced significant challenges in processing claims and payments, leading to cash flow issues that threatened the viability of smaller practices, particularly in rural areas. Patients, too, were directly impacted, with difficulties in accessing medications and care due to system outages. The financial burden of the attack is estimated to reach between $2.3 billion and $2.45 billion, reflecting both the immediate response costs and ongoing operational disruptions. Moreover, the incident raised serious concerns about the concentration risks inherent in the consolidation of healthcare data processing under a few large entities, underscoring the urgent need for stronger cybersecurity measures across the healthcare industry.

3.2. Considerations and Lessons from Key Perspectives

3.2.1. Public and private sector collaboration

Public-private partnerships (P3) have been used across sectors and have ranged in scope from $50 million projects to ones over $5 billion, attracting private sector capital from diverse sources, including pension funds, insurance companies, and sovereign wealth funds. These partnerships provide private capital to help finance projects, engaging the private sector often in aspects of design, construction, and performance management, while maintaining public asset control. Although not suitable for every type of project or objective, P3s can increase efficiency and scale of project delivery, provided the scope and accountabilities are clear.

The Federal government is responsible for promoting the health of the nation's infrastructure. A corollary of that ultimate responsibility is how resources can most effectively be marshaled, deployed, and coordinated under Federal purview to achieve prioritized objectives in meaningful timeframes. The beneficial impacts of the private sector partnerships with the public sector represent a compelling opportunity but also presuppose thoughtful management of crucial decision points with respect to role clarity:

1) What roles can each sector play in the new development or upgrade and maintenance of a given asset: owner, regulator, or operator?
2) Besides the role of regulator outside of governmental mandate, what are the most constructive outcomes that would favor entrusting the private sector with participating in or even fully enacting any of the other roles?
3) How can the Federal government's role in supporting private investment in critical infrastructure preparedness be reconciled with SLTT authorities to align with national standards and overarching priorities?

In addressing the above questions, it is important to maintain clarity on P3's purpose and form. Successful P3s enable appropriate transfer or sharing of risk in alignment with each party's strengths in infrastructure delivery. In the final analysis of high performing collaborations, it comes down to positioning the risk management accountability and consequent reward proposition where (or with whom) it can most effectively be managed. If structured properly, the public sector engages with private capital and capability to yield essential and positively force-multiplying effects, including the following: operational efficiency, agility in innovation, magnified socioeconomic impacts, incentive alignment for asset longevity, and a focus on essential outputs rather than artifactually constrained inputs to partnership. Thus, an effective P3 investment involves more than managing capital expenditures or even building processes. It involves aligning the interests of the community of need with governmental authorities and private sector partners around the full lifecycle of an asset. The P3's form is constituted by clear and definitive contractual obligations to investment, delivery, service, and timeliness, as well as a strong relationship between fulfilling

these obligations and having a reasonable magnitude and stability of returns on investment. In many countries, including the United Kingdom and Australia, where the private sector operates infrastructure assets, the private sector is permitted to own such assets (e.g., airports, water systems) within guardrails that protect the public sector's vital interests and broader accountabilities while still more deeply aligning performance incentives. In the United States, many infrastructure assets in certain sectors such as transportation and water are principally owned by government (important exceptions being the power sector as well as commercial port operations), and yet that would seem to subvert the very aim, if not even the fact, of earnest partnership between the parties to a P3. This said, it is important to consider additional reasons for suboptimized P3 opportunities based on unintended but nonetheless real disharmony between various levels of government and regulatory authorities.

Despite the clear benefits of P3s, several barriers hinder their effective deployment in the United States. One significant challenge is varying legislation across states, and even within states according to regulatory agency. These variations manifest in the mechanisms employed to generate funding for projects, to regulate processes, and to prioritize projects. As private sectors adapt to the nuanced differences between each state, these inconsistencies create challenges, particularly in sectors where the scale of investment is large and the time horizon for performance is long. The absence of uniform performance standards and regulatory frameworks can deter private financing, as these conditions exacerbate potential risks and threaten the stability of returns on investment.

Inconsistency of senior public sector sponsorship, often influenced by election cycles, further complicates the landscape, as does the structural rigidity of Federal contracts and long-term payment obligations. The inconsistency in public sector sponsorship and regulatory support is particularly noteworthy. While regulatory frameworks can create the ideal financial incentives for private investors, especially in emerging technologies or innovative projects, the lack of consistency in these regulations poses a significant risk. Investors are often hesitant to commit to projects where regulatory guidelines may shift unpredictably, as this uncertainty can undermine the stability of their returns. In such environments, investors might demand higher returns to compensate for the added risk, which can make projects less viable.

3.2.2. Data management and analytical capabilities

To effectively address the complexities of promoting infrastructural health, it is imperative to consider the interconnectedness of various sectors that form the backbone of public infrastructure. In many ways, insights into and understanding of these interdependencies have been underserved by deficiencies in clarity, consistency, and reliability of data management and derivative analytics. These may be poised for step-function improvement considering the impressive advances being made in the generative augmented/artificial intelligence (AI) space. However, before delving into the promise of AI, a few caveats are noteworthy:

1) AI tools can be particularly well-suited to crucial insight sharing across sectors, and machine learning (ML) derivative capabilities can be trained to formulate predictive models that permit threat assessment and risk mitigation on a prospective, customized basis. However, the accuracy, scale, efficiency, and benefit of these capabilities is crucially dependent on standardized knowledge-based definition and data management governance.
2) A foundational application of this approach would be illustrated by uniform date and time stamp conventions for data intake and management across all critical infrastructure sectors; however, none presently exists. Such a convention would contribute greatly to fostering verified and validated

data, combining multiple data sources into a central repository, and enabling subject matter experts within and across sectors to access these through interface standards known as universal data connectors.

3) The intended effect of the above is cross-sector application of AI tools producing clean insights that can be extracted from unstructured data pools and then transformed and loaded for more reliable analysis in service of accurate and efficiently scalable impact. Examples of this effect in action illustrate efficiency and sustainability of infrastructure assets and services:
    a. In the context of P3s, more reliable predictive modeling of asset vulnerability could rationalize the long-term cost structure for operations and maintenance as well as related insurance premium expenses over the lifespan of an asset.
    b. In the context of healthcare costs of employees and their dependents for self-funded employers, more reliable population health management interventions bolstered by enhanced clinical, behavioral, and social risk stratification could provide assurance of a rationalized expense trend and thereby direct care to more effective and efficient providers.

Despite these caveats, it remains clear that in the rapidly evolving landscape of public sector infrastructure, the integration of AI-driven predictive analytics is emerging as a crucial strategy for bolstering preparedness and resilience. The adoption of AI in public sector infrastructure is increasingly focused on proactively identifying and managing potential risks. AI-driven predictive analytics, such as those utilized by the Federal Emergency Management Agency' s (FEMA) Resilience Analysis and Planning Tool, enable agencies to analyze vast amounts of data to forecast vulnerabilities and identify areas most at risk from natural disasters and other crises. Integrating AI into these tools allows for more precise and timely predictions, enhancing the ability to implement preemptive measures that protect critical infrastructure.

Moreover, the Department of Homeland Security's (DHS) Public-Private Analytics Exchange Program highlights the value of collaborating between public and private sectors in harnessing AI for infrastructure security.[2] Through responsible AI practices, this program facilitates the sharing of insights and analytics that are crucial for identifying and mitigating potential risks and threats, thereby strengthening the overall resilience of public sector infrastructure.

AI's role in predictive analytics is further amplified by its ability to perform common cause failure analysis. This approach, which is crucial in threat modeling, involves using AI to analyze interdependencies within infrastructure systems, identifying potential failure points that could trigger cascading effects across sectors. By predicting these vulnerabilities, AI-driven analytics support the design of more resilient infrastructures that are capable of withstanding and quickly recovering from disruptions.

As the use of AI in public sector infrastructure expands, so does the importance of managing the risks associated with AI technologies. The Cybersecurity and Infrastructure Security Agency (CISA) emphasizes the need for responsible AI practices, particularly in the context of infrastructure security. This includes ensuring that AI systems are transparent, secure, and ethical, with built-in safeguards to prevent misuse or unintended consequences.

The CISA Roadmap for Artificial Intelligence outlines a comprehensive approach to managing AI risks, which includes rigorous testing, continuous monitoring, and regular updates to AI systems. This roadmap serves as

[2] See also: Clinton, Larry. 2023. *Fixing American Cybersecurity*. Georgetown University Press.

a guide for public sector entities to develop and implement AI technologies that are effective and aligned with broader ethical and security standards.

In addition to enhancing security, AI also presents opportunities to address the energy challenges associated with data centers that power AI capabilities. AI can be leveraged to optimize energy consumption in these centers, thereby reducing their environmental impact. AI systems can be designed to monitor and adjust energy usage dynamically, ensuring data centers operate efficiently while minimizing their carbon footprint. AI applications in smart buildings, power stations, and other infrastructure components are already demonstrating significant energy savings. AI-driven systems in smart buildings can predict and manage energy needs based on real-time data, adjusting heating, cooling, and lighting to match occupancy patterns and external conditions. When ML supported by AI is introduced into power system operations, grid operators can use advance simulation to plan and operate the system to increase its efficiency in all circumstances and its resiliency against unlikely but severe natural and technology-induced disasters.

The integration of AI-driven predictive analytics into public sector infrastructure is not just a technological advancement but a strategic imperative. By effectively managing AI risks and leveraging AI for energy optimization, public sector entities can significantly enhance the resilience and sustainability of infrastructure. As AI continues to evolve, its role in safeguarding and optimizing infrastructure will only become more central, underscoring the need for ongoing investment in responsible AI technologies and practices.

3.2.3. Cross-sector considerations

In addressing the complexities of promoting infrastructure health, it is imperative to consider the interconnectedness of various sectors that form the backbone of public infrastructure. Experts from multiple critical infrastructure sectors have highlighted several barriers that impede enhanced preparedness. These insights, drawn from authoritative private sector sources as well as Federal agencies including CISA, the U.S. Department of Energy (DOE), and the U.S. Department of Health and Human Services (HHS), underscore the need for a harmonized approach to infrastructure preparedness. This section delves into these barriers, emphasizing opportunities to improve in cross-sector collaboration, scenario-driven training, and standardized performance metrics to bolster infrastructure preparedness.

Comprehension of Interdependence Across Sectors:

One of the most significant barriers to enhanced preparedness is poor understanding of the extreme interdependence between critical infrastructure sectors. This interdependence is not only crucial for organizing an effective crisis response but also for coordinating improvements in preparedness. Failing to recognize how sectors such as energy, water and wastewater, healthcare, communications, and transportation intertwine can lead to gaps in response capabilities and vulnerabilities in infrastructure security. For instance, a disruption in the power grid can have cascading primary effects as well as amplifying secondary effects on healthcare facilities, water provision or disposal, transportation networks, and communication systems. It is common to consider anticipated effects within sectors that are in close adjacency during routine operations; however, incursions or breaches often exert amplification of initial patterns of disruption via more indirectly related sectors, which are unanticipated unless care has been taken to understand all potential inter-sector feedback loops. **Figure 1** illustrates the extent to which an incursion or breach in one sector and its adjacencies can impose direct repercussions on another cluster of more closely associated sectors. This indirectly related grouping of sectors, in turn, can generate

reverberating adverse effects that magnify the overall scope of incapacitation and potentially set in motion a vicious cycle of damage that becomes more difficult to contain and recover from.

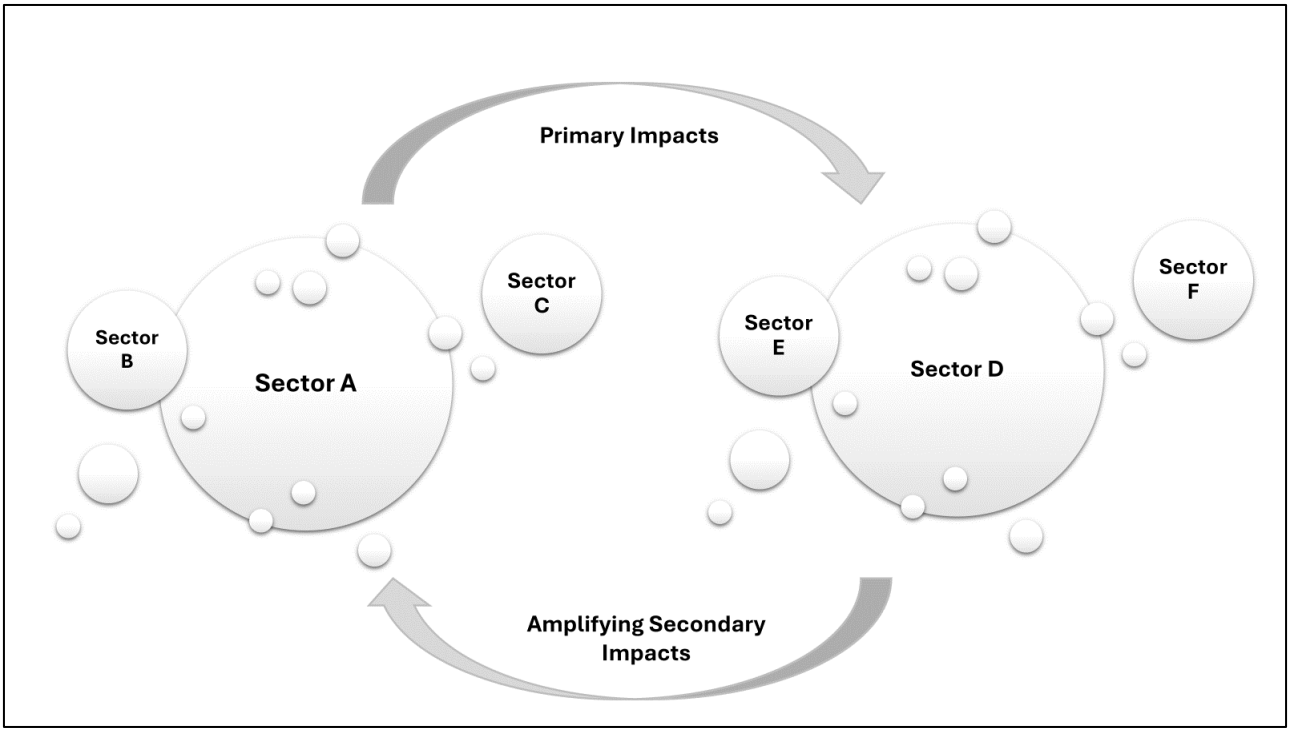

Figure 1: Sector breach and impact

Therefore, comprehensive understanding and anticipation of these interdependencies is essential for developing robust preparedness strategies that foster capabilities to withstand or quickly recover potential crises.

Structured and Iterative Training:

Inadequate emphasis on structured and iterative training across sectors further exacerbates the challenges to preparedness. To address this, a formalized approach to inventory-taking is necessary, identifying both intra-sector imperatives and interdependencies with other sectors. This approach should focus on proactively identifying vulnerabilities and enhancing preparedness for threats to infrastructure functionality and integrity (i.e., threats to the health of infrastructure).

Moreover, there is a pressing need for formalized training exercises that simulate crises based on threat models, capabilities inventories, targeted human talent/skill development, and inferred risk assessments. Such exercises, like the Federal Aviation Administration's airline industry collaborative, involve scenario-driven, systems-level crisis simulations that are crucial for evaluating readiness as well as response-related capabilities and actions in real-time. These simulations not only test the preparedness of individual sectors but also highlight areas where cross-sector collaboration is critical. Iterative improvements in people, processes, and technology deployments can then be made to counteract potential incursions on infrastructure integrity from various sources.

Information Sharing Across Sectors:

Timely, transparent, and liability-protected sharing of information across sectors is another critical area where barriers exist. The complexity of modern infrastructure systems requires seamless communication between sectors, particularly concerning interdependencies or contingencies that might arise during a crisis. Beyond the data management disciplines and analytical capability enhancements described in the previous section, human factors that support effective communication strategies are crucial success elements and require intentional design and deliberate testing.

Infrastructure sector-based Information Sharing and Analysis Centers (ISAC) have been established by infrastructure owners and operators as not-for-profit entities which seek to maintain sector-specific situational awareness and to partner with governmental agencies in responding to and sharing relevant information on physical and cyber threats or incursions. Moreover, a National Council of ISACs was formed in 2003 and now encompasses 27 such entities. However, ISACs vary significantly in terms of effective, timely, and complete threat warning, incident reporting and response coordinating within sectors along lines of associated primary effects, as well as across sectors in reference to collateral impacts. For example, the electricity sector focused E-ISAC sponsors GridEx, the largest grid security exercise in North America, and offers it with regular cadence to member and partner organizations as a forum for practicing how they might better model threats and craft responses to coordinated cyber and physical security incursions. As referenced in the section above, the ISAC serving the aviation sector maintains a similarly rigorous insight and skill building regimen. By contrast, the healthcare ISAC has struggled to improve the quality of information transfer in the face of evolving crises and lacks broad coordination of threat modeling and capabilities assessments within its own sector. To little surprise, the healthcare ISAC also struggles to enhance integration of efforts with other sector-specific ISACs sharing interdependencies with it. Reducing the variation in what ISACs are not only charged with but also capable of doing and accountable to do is indispensable to rendering the National Council of ISACs more contributory to holistic preparedness enhancing efforts. While this must involve mechanisms for limiting the liability, which might otherwise be incurred or anticipated in association with real-time, substantive information sharing (which does currently constitute a disincentive for prompt transparency), it also crucially depends upon structured approaches to continually practicing and iteratively refining the paradigm of in-sector and cross-sector stakeholder engagement. Training exercises must incorporate clear mechanisms for such insight sharing, ensuring that key performance indicators reflect the proper form, content, and cadence of communication channels. Establishing robust protocols and interoperable data management technologies for information sharing can significantly enhance the collective preparedness to mitigate and confront infrastructure vulnerabilities, reducing the risk of cascading failures across sectors.

Federal Standards and Performance Metrics:

Federally mandated outcomes-based standards, accompanied by related performance metrics, are generally lacking and would bolster resilience of public infrastructure. These standards should be derived from evidence-based guidelines for best practices and should enforce requirements on what needs to be in place to mitigate risks to both physical security and cybersecurity. However, it is crucial to allow private sector providers, contractors, and investors the flexibility to determine how to meet these standards within appropriate guardrails.

As was indicated in a prior section, the challenge may be most acutely felt in the finance arena as a function of the tremendous heterogeneity in regulatory policies for sectors that are generally regulated at the state level. It is difficult to arrive at a consistent business model for private sector entities that seek to partner

with the public sector to co-fund projects. What makes financial sense in one state may not in another. From an efficiency perspective, being able to replicate structure approaches across multiple projects attracts investors that wish to deploy large amounts of capital in a manner that does not require undue amounts of local customization. Moreover, consistency of practices, technologies, equipment selection, and the like enables higher levels of reliability and provides for improved economies of scale. Finally, in relation to regulatory consistency under Federal guidance, as vulnerabilities materialize during the life of a P3 project and increased requirements develop to address those concerns, regulatory allowances for operation and maintenance needs must support the additional investment and facilitate the interventions required to respond adequately and promptly. In this way, care must be taken to extend the serviceable life of assets and to maintain the designed returns for the private sector investor, thus supporting the proper incremental adaptations of infrastructure maintenance in response to originally unforeseen needs – needs that, if unattended, would result in disruptions in functionality and ultimately greatly increase costs.

From the perspective of tactical preparedness in infrastructure asset stewardship, it is essential to identify and refine what constitutes a minimum viable operation (MVO) within and across sectors. The more shared baselines of infrastructure conditions are understood, the greater the likelihood of achieving and maintaining a level of preparedness that avoids crisis expansion and blunts the required intensity of response and recovery burdens. In keeping with the theme addressed in the prior section, formalized, iterative training exercises designed to target these MVOs are not uniformly adopted, leaving open important questions about whether sectors can maintain critical functions during a crisis. Compliance with standards, when they do exist in the proper form, are not consistently linked to Federal funding for SLTT governments, as well as cross-linked entities such as P3s; they therefore lack incentive alignment to promote de facto enforcement.

Infrastructure Security and Preparedness "Poverty Lines:"

A significant challenge in promoting infrastructure health is the existence of infrastructure security and preparedness “poverty lines.” Small systems servicing basic infrastructure needs of geographically isolated or low affluence communities often lack the financial resources necessary to upgrade antiquated physical infrastructure or outdated technology. Without targeted assistance, these entities are at risk of staying or falling behind in preparedness efforts, potentially becoming weak links in the broader infrastructure network chain. Recognizing this disparity is crucial, and efforts must be made to provide focused support to these vulnerable entities and the communities they serve, ensuring that all parts of the infrastructure network can contribute to and benefit from enhanced preparedness initiatives. This arena represents an especially aggrieved casualty of underpowered application of the P3 paradigm, which could otherwise play the crucial role in closing resourcing gaps and accelerating the renewal or development of infrastructure assets and supporting technologies. This especially applies to small utilities (especially in the water/wastewater sector) and stand-alone, safety net health facilities that lack substantive connection to larger support systems or access portals to broader networks. They also often lack the financial means to upgrade and secure plant, tools, and technologies to withstand threats or harm to their physical and digital assets. A more robust application of the P3 model could provide these entities with access to needed capital and expertise, fostering innovation and resilience in sub-sectors that are all too often overlooked. By leveraging private investment in conjunction with public resources, the P3s could be especially helpful in bridging the gap between current infrastructure capabilities and the demands of a rapidly changing threat landscape.

3.2.4. Synthesis of research findings and the approach to solution-building

This Subcommittee's subject matter expert briefings and adjunctive research yielded insights that paralleled very closely to many of the findings articulated in recent NIAC reports on barriers to cross-sector collaboration, on water management challenges, and on assuring the reliability of our national electrical grid (see references below). The inputs to those examinations and the ones reported here concord on issues that apply broadly as sources of inertia or friction along the path to more prudent infrastructure asset development and stewardship. These include:

- Suboptimal prospective (rather than only retrospective) insight generation
- Lack of standardization on meaningful performance metrics
- Regulatory inconsistencies
- Incentive misalignments
- Inattention by policy makers and enforcers at multiple levels to prioritize prevention investments as a more effective and efficient means of conserving resources while reducing risk, vulnerability, and the burden on crisis response and recovery capacities

The latter consideration is the one that most inspires applying the holistic paradigm of health to infrastructure, insofar as approaching the enhancement of our national infrastructure's preparedness to withstand threats and vulnerabilities is akin to confronting the well-being of patients by emphasizing preventive care strategies. In both contexts, readiness emerges most effectively from anticipating threats and building buffering capabilities to mitigate the risk profile of a dynamic system of systems.

Promoting infrastructural health requires a proactive approach that harnesses the opportunity to incentivize and support stronger private sector engagement; addresses the complex interdependencies between sectors; emphasizes structured training and highly reliable insight sharing; and implements Federally mandated, rigorous standards and performance metrics. The approach to solution-building for these challenges contains the following five interwoven initiative categories that also reflect points of cross-linkage and continuity with other NIAC reports submitted in 2023 and 2024:

1) *Enhancing insights* into threats, risks and capabilities in relation to preparedness
2) *Establishing insight-driven standards of performance* within and across sectors
3) *Training formally and regularly* on insight-driven standards and refining targeting of baseline cross-sector functionalities
4) *Asserting Federal governmental direction* consistent with standards, harmonizing with SLTT entities
5) *Realigning incentives for private sector investments* of capital and capabilities

These initiative groupings do not express a unidirectional, linear process that, once launched, runs to some point of completion and awaits future reactivation of the same sequence after a period of inactivity. Instead, they constitute elements of an ongoing, virtuous cycle of continuous learning and adaptation fueled by feedback loops between each element and every other. The specific recommendations that are presented in the next section of this report are intended to be read in this spirit and in accordance with **Figure 2**.

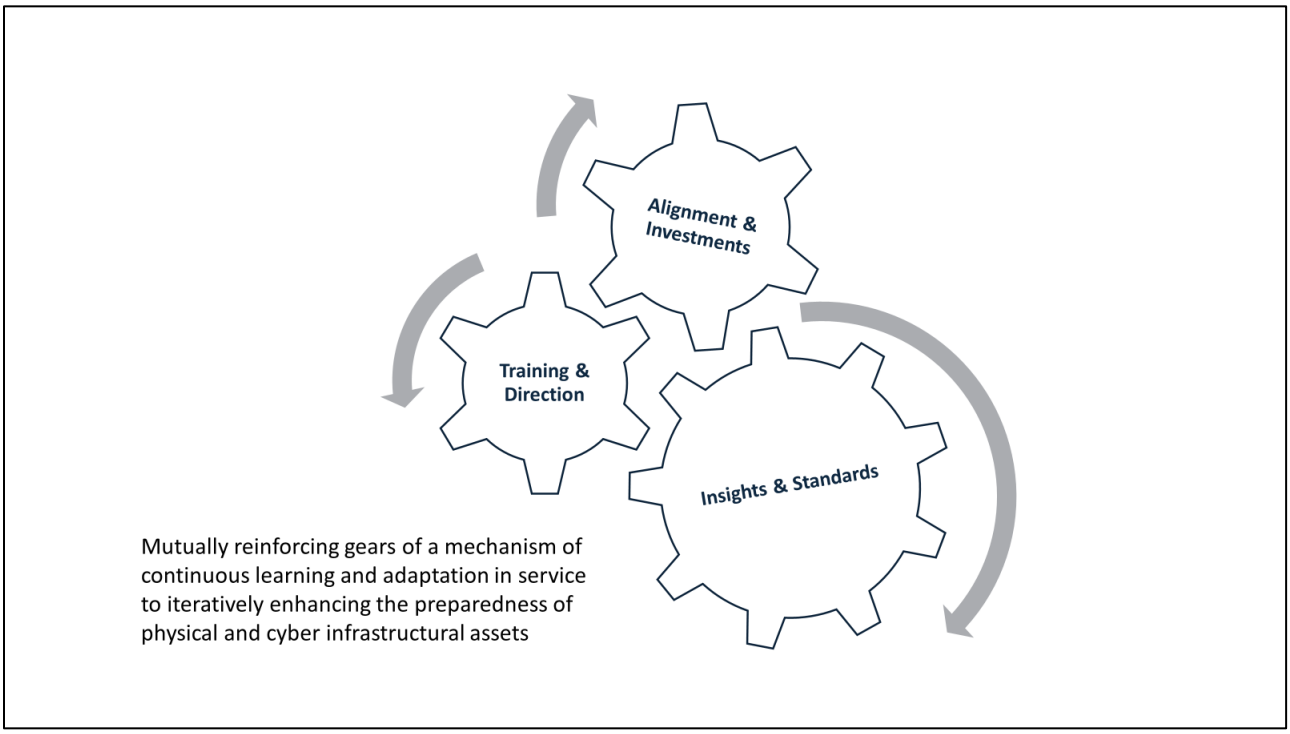

Figure 2: Reinforcing gears of a continuous learning mechanism

4. Recommendations

4.1. Enhance the Quality of Insights into Threats, Risks, and Capabilities in relation to Preparedness.

4.1.1. Bolster data management integrity and knowledge base governance.

Adopt a uniform date and time stamp convention for data intake and management across all infrastructure sectors.

Incorporate requirements for information system architecture and processes that assure verified and validated data inputs to essential infrastructure health promotion workstreams directed by Federal authority.

Integrate multiple data sources into a central repository dedicated to infrastructure health promotion and ensure accountability for this database management system to operate data transactions according to the principles of atomicity, consistency, isolation, and durability (ACID).

Enable subject matter experts within and across sectors (e.g., ISAC participants) to access validated and verified data managed according to ACID principles through universal interface standards (common data connector functionalities).

4.1.2. Build data profiles for capabilities inventories and risk assessments.

Create a dedicated task force to comprehensively analyze and model interdependencies between infrastructure sectors.

The task force should include representatives from key agencies (CISA, FEMA, DOE, HHS, etc.), industry experts, ISACs, and academic institutions.

The task force should oversee the application of AI capabilities to feed curated data into ML algorithms through which to build and refine predictive analytics to anticipate and quantify threats as well as to expose and characterize vulnerabilities.

4.2. Commit to Insight-driven Standards of Performance within and across Sectors.

4.2.1. Structure simulation-based threat modeling.

Expand Federally funded training programs that emphasize iterative and structured scenario-based exercises, like GridEx. These exercises should involve multiple interrelated sectors as well as regulatory, industry, and research and development stakeholders (consider also, in the latter category, representatives of Federally funded research and development centers). The focus must be on realistic threat simulations.

Develop a national database to track training participation, lessons learned, and identified vulnerabilities, which should inform future iterations of training exercises.

Build objectives for successful training around predictive modeling of potential (anticipated and unanticipated) vulnerabilities and not just retrospective failure analysis.

4.2.2. Set Minimum Viable Operations (MVO) Standards.

Develop an MVO certification for infrastructure sectors that outlines the minimum requirements for maintaining readiness to enact essential functions during a crisis. This certification should include benchmarks for physical infrastructure, cybersecurity, and personnel training.

Encourage state and local governments to adopt MVO standards within their infrastructure planning and management frameworks, ensuring a consistent baseline of preparedness across jurisdictions.

4.3. Train Formally on Insight-driven Standards and Iteratively Refine Targeting of Baseline Cross-sector Functionalities.

4.3.1. Build on best practice ISAC models to develop training disciplines.

Task and support the National Council of ISACs to undertake a comprehensive assessment of variability in effectiveness of all ISACs and to establish and sponsor coordinated best practice-driven training exercises, educational opportunities, and sharing of actionable insights.

These initiatives should be modeled on the simulation-based exercises already being enacted in a rigorous fashion under sponsorships of the electricity and aviation ISACs for their respective stakeholders.

4.3.2. Target cross-sector learning.

Apply threat modeling and risk assessments to training exercises that map out primary and secondary effects of disruptions, using simulations to understand how cascading failures propagate across sectors.

4.4. Assert Federal Governmental Direction Consistent with Insight-driven Standards, Coordinating with SLTT Authorities

4.4.1. Mandate training through key certification requirements.

Integrate data quality management practices, intra- and cross-sector training, and MVO certifications into regulatory requirements and Federal grant eligibility criteria.

To the maximal extent possible, these certifications should be based on the demonstrable ability to reliably fulfill outcomes metrics rather than process-oriented objectives.

4.4.2. Connect adoption of basic standards to Federal funding and provide incentives to adhere to standards.

Mandate participation in structured, MVO standards-driven training for entities receiving Federal infrastructure funding or grants, including SLTT governments, to ensure consistency in preparedness across the country.

Entities, including P3s, that meet or exceed MVO standards should be granted preferential access to Federal grants, special contracting provisions, or special procurement opportunities. [3]

[3] Note: A recent example of this kind of approach is the National Telecommunications and Information Administration's Broadband Equity, Access, and Deployment program that ties Federal funding to the adoption of basic standards for broadband speed, reliability, and affordability.

4.5. (Re)align Incentives to Strengthen Sustainable Private Sector Investments of Capital and Capabilities.

4.5.1. Incentivize the adoption of P3 legislation.

Support states that establish P3s as a potential delivery model for infrastructure projects across states. While cities and states will then have the discretion to pursue traditional procurement models or P3s, having enabling legislation will allow local authorities the option to increase private investment.

To ensure the effectiveness of this approach, condition eligibility for certain Federal discretionary funding on states having P3-enabling legislation in place.

Allocate discretionary funding to support states, planning agencies, and municipalities in conducting thorough project screenings and Value for Money analyses. These assessments would help identify opportunities where private financing could accelerate project delivery and improve outcomes.

4.5.2. Streamline environmental reviews and related permitting.

Focus on modernizing the environmental review process for infrastructure projects. The current system often acts as a deterrent to private investment due to its complexity and unpredictability. By implementing a streamlined and coordinated approach among Federal agencies, the government can significantly reduce approval timelines while maintaining rigorous environmental standards. Progress here would be advanced by governmental alignment in setting cross-agency agendas on the highest national priorities to move related processes more quickly, avoiding the inertia associated with each agency furthering its work according only to its individual line of priorities.

Incorporate innovative approaches that transform environmental reviews from potential obstacles into tools for achieving better project outcomes.

Establish clear protocols for integrating private sector technical expertise and risk assessment during the early planning stages, ensuring that potential issues are identified and addressed proactively.

4.5.3. Reform Federal budget scoring rules.

Revise budget scoring rules to better reflect the long-term nature of infrastructure investments and the unique characteristics of alternative project delivery methods that incorporate private financing.

Implement capital investment protocols that allow certain categories of public infrastructure investment to be classified as operating leases, particularly for facilities such as Veterans Affairs hospitals, Army Corps of Engineers projects, and Federal agency buildings.

Align reforms with existing rulings to support lifecycle procurement approaches in P3 projects.

4.5.4. Expand opportunities to utilize private activity bonds.

Address limitations in Private Activity Bond (PAB) programs. This includes raising volume caps on surface transportation PABs and eliminating the Alternative Minimum Tax penalty that currently diminishes their attractiveness to investors.

PAB eligibility should be broadened beyond transportation to encompass environmental projects, public facilities, and other critical infrastructure sectors, thereby expanding the pool of potential P3 projects.

4.5.5. Increase funding for existing blended financing tools.

Federal funding and loan programs such as the Transportation Infrastructure Finance and Innovation Act and the Water Infrastructure Finance and Innovation Act should receive stable and growing funding allocations, with a renewed emphasis on linking program participation to private capital involvement.

Address the long-term solvency of the Highway Trust Fund by stabilizing current revenue streams and identifying new funding sources. This commitment to sustainable funding will provide the certainty needed to attract private investment in transportation infrastructure. [4]

[4] Note: an additional case in point with regard to stable and sustained funding commitments of this general type is the Maritime Security Trust Fund that the Kelly-Waltz bill (Ships for America) envisions.

5. Call to Action

Promoting infrastructure health is about fostering a culture of preparedness that permeates every aspect of public infrastructure management. It is therefore much more than building stronger bridges, more robust power systems, or more incisive predictive analytics tools. It is critically dependent on responsibly and effectively harnessing the power of P3s along lines that permit each party in the relationship to help each other to address our many challenges with due pace, focus, and quality of design and delivery. This overarching approach can, in turn, foster, complement, and empower parallel investments in early detection, preventive intervention, and continuous training in service to results-oriented performance standards that support public sector infrastructure capable of withstanding and more rapidly recovering from a wide range of threats.

This health-inspired paradigm of preparedness enhancement allows policymakers, industry leaders, and the public to conceptualize infrastructure not merely as a static collection of physical assets but as dynamic systems that require ongoing care and attention to maintain their vitality and functionality in service to communities' best opportunities to thrive. As such, it aims not only to reduce the likelihood or frequency of disruptions but also to ensure that when challenges do arise (and they inevitably will), our response capabilities will be set up for optimal effectiveness and efficiency.

By implementing this report's recommendations, the Federal government can create a more favorable environment for accelerating the development of critical projects and ensuring that infrastructure investments in preparedness reflect the highest standards of American ingenuity, performance, and durability. In so doing, the United States can build the robust, modern infrastructure necessary to close current resiliency gaps while maximizing the value of taxpayer dollars as well as human and material resources.

Appendix A: Acknowledgements

Subcommittee Members

Conrad M. Vial, Senior Vice President of Sutter Health and Sutter Health Network President, Sutter Health

Alan S. Armstrong, President and CEO, Williams Inc.

Bilal Ayyub, Professor and Director, Center for Technologies and Systems Management, Department of Civil and Environmental Engineering, University of Maryland, College Park

Deneen DeFiore, Vice President and CISO, United Airlines

David L. Gadis, CEO and General Manager, DC Water

David Grain, CEO and Founder, Grain Management, LLC

Beth Keolanui, Executive, Healthcare Products and Services, Sutter Health

Eva Lerner-Lam, President, Palisades Consulting Group

Jonathan Ma, Vice President, Strategic Finance and Treasurer, Sutter Health

Norma Jean Mattei, Professor, University of New Orleans

Ricardo Medina, Project Director, Simpson Gumpertz & Herger

Jacki Monson, Senior Vice President, Chief Integration Officer, Sutter Health

Amir Nayeri, Deputy Global Director of Business Development, Meridiam

Adebayo O. Ogunlesi, CEO, Global Infrastructure Partners

Jorge Ramirez, Managing Director, GCM Grosvenor

Pasquale Romano, CEO, Redoxblox

Anthony W. Thomas, President and CEO, Shinall Advisors LLC

David Totman, Infrastructure Industry Strategist

Sadek Wahba, Chairman and Managing Partner, I Squared Capital

Christopher J. Wiernicki, Chairman and CEO, American Bureau of Shipping

Audrey A. Zibelman, Senior Advisor and Board Member

Subcommittee Briefers

Manny Cancel, Chief Executive Officer, E-ISAC

CDR Thomas Christl, Director, Office of Critical Infrastructure Protection

Josh Corman, Founder, I Am The Calvary

Deneen DeFiore, Vice President and CISO, United Airlines

Ben Djiounas, Managing Director, J.P. Morgan

Lisa Einstein, Chief Artificial Intelligence Officer, CISA

Philip Hinson, P.E., M.ASCE

Eva Lerner-Lam, President, Palisades Consulting Group

Brian Mazanec, Deputy Director, ASPR Center for Preparedness

Jacki Monson, Senior Vice President and Chief Integration Officer, Sutter Health

Tyler Reeder, Managing Partner, Energy Capital Partners

Eric Rollison, Assistant Director for Risk Analysis, Resilience and Recovery, Department of Energy

Jeffrey Thompson, CEO, DC Water

David Totman, Infrastructure Industry Strategist

Appendix B: Definitions

Term	Common Definition
GridEx	Provides the electricity industry, government agencies, and other relevant organizations the opportunity to exercise emergency response and recovery plans in response to simulated cyber and physical security attacks and other contingencies affecting North America's electricity system.
MVO	MVO is the bare minimum an organization needs to function. In a crisis, MVO-based functions must continue to perform.

Appendix C: Acronyms and Abbreviations

Acronym/ Abbreviation	Definition
ACID	Atomicity Consistency Isolation Durability
AI	Artificial Intelligence
ASCE	American Society of Civil Engineers
ASPR	Administration for Strategic Preparedness and Response
BEAD	Broadband Equity Access Deployment
CISA	Cybersecurity and Infrastructure Security Agency
DHS	Department of Homeland Security
DOE	Department of Energy
E-ISAC	Electricity Information Sharing and Analysis Center
FEMA	Federal Emergency Management Agency
HHS	Health and Human Services
ISAC	Information Sharing and Analysis Center
ML	Machine Learning
MVO	Minimum Viable Operations
NIAC	National Infrastructure Advisory Council
NTIA	National Telecommunications and Information Administration
P3	Public-Private Partnership
PAB	Private Activity Bond
RAPT	Resilience Analysis and Planning Tool
SLTT	State Local Tribal and Territorial
TIFIA	Transportation Infrastructure Finance and Innovation Act
WIFIA	Water Infrastructure Finance and Innovation Act

Appendix D: References

Alder, Steve. 2024. "UHG: Substantial Proportion of US Population May Be Affected by Change Healthcare Cyberattack." HIPAA Journal. April 23, 2024. https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/.

"ASCE NOAA Taskforce." 2024. Asce.org. 2024. https://www.asce.org/communities/institutes-and-technical groups/sustainability/asce-noaa-taskforce.

Change Healthcare. n.d. "Change Healthcare Cyberattack Support." https://www.unitedhealthgroup.com/ns/health-data-breach.html.

CISA. 2023. "Roadmap for AI." November 7, 2023. https://www.cisa.gov/resources-tools/resources/roadmap-ai

CISA. n.d. "Artificial Intelligence." https://www.cisa.gov/ai.

CISA. n.d. "The President's NIAC Reports and Recommendations." https://www.cisa.gov/resources-tools/groups/presidents-national-infrastructure-advisory-council/niac-reports-and-recommendations.

Clinton, Larry. 2023. *Fixing American Cybersecurity*. Georgetown University Press.

E-ISAC. 2024. "GridEx XIII." 2024. https://www.eisac.com/s/gridex.

EPA. 2015. "Water Infrastructure Finance and Innovation Act (WIFIA)." US EPA. August 10, 2015. https://www.epa.gov/wifia.

Federal Aviation Administration. 2023. "Connect and Collaborate | Federal Aviation Administration." https://www.faa.gov/data/collaborate.

FEMA. 2023. "Resilience Analysis and Planning Tool (RAPT) | FEMA.gov." June 9, 2023. https://www.fema.gov/about/reports-and-data/resilience-analysis-planning-tool.

National Council of ISACs. 2015. "MEMBER ISACS." https://www.nationalisacs.org/members.

Schwartz, Mark W. "Rethinking Risk and Responsibility in the Western Wildfire Crisis." *Stanford Social Innovation Review*, 2022. https://doi.org/10.48558/BXNS-K043.

Stephens, Scott L, Daniel E Foster, John J Battles, Alexis A Bernal, Brandon M Collins, Rachelle Hedges, Jason J Moghaddas, Ariel T Roughton, and Robert A York. 2023. "Forest Restoration and Fuels Reduction Work: Different Pathways for Achieving Success in the Sierra Nevada." *Ecological Applications* 34, 2 (2932). https://doi.org/10.1002/eap.2932.

U.S. Department of Homeland Security. n.d. "AEP Overview and Documents | Homeland Security." https://www.dhs.gov/publication/aep-overview-and-documents.

U.S. Department of Transportation. 2019. "Status of the Highway Trust Fund | Federal Highway Administration." https://www.fhwa.dot.gov/highwaytrustfund/.