WILLIAM & MARY | PUBLIC POLICY

Critical Infrastructure that Inspires Confidence and Delivers Results

Proceedings from a symposium hosted by the W&M Public Policy Program on April 5, 2024 in Williamsburg Virginia

Crim Dell bridge on the campus of William & Mary

Acknowledgements: The W&M Public Policy Program thanks the Office of the Provost and our Public Policy Board of Advisors for financial support that made the symposium possible. In addition, we thank Kurt Klingenberger for sage advice, Sophie Correll who flawlessly managed event logistics, and April Greener for editorial assistance. Finally, we thank the symposium participants, including W&M Public Policy students, who offered their time, energy, and ideas that formed the basis for this report.

Suggested citation: Paul Manna and Owen Williams. 2024. Critical Infrastructure that Inspires Confidence and Delivers Results. Proceedings from a symposium hosted by the William & Mary Public Policy Program, Williamsburg, VA, April 5, 2024.

Table of Contents

Dedication

We dedicate this report to Dorlian Castillo Cabrera, Alejandro Hernández Fuentes, Miguel Angel Luna Gonzalez, José Mynor López, Miguel Luna, and Maynor Yasir Suazo-Sandoval who died tragically while servicing the Francis Scott Key Bridge on March 26, 2024, the week before our symposium. The bridge collapsed after the container ship Dali struck one of its support piers. May the memories of these men continue to inspire the daily vital work of other critical infrastructure professionals in the United States and abroad.

Symposium Overview and Goals

On April 5, 2024, the W&M Public Policy Program convened approximately 30 policy experts from federal, state, and local governments (including people with military or civilian roles), representatives from the private sector and non-profit sector, and academic researchers to discuss critical infrastructure policy in the United States. Those experts also engaged students throughout the day. The conversation was organized around specific discussion prompts and key problems of practice that critical infrastructure professionals regularly face. Given the participants' backgrounds, examples came from local settings in the Richmond to Virginia Beach corridor here in Virginia, as well as examples from other states and the nation.

The symposium aimed to achieve three key goals.

First, it provided participants with opportunities to discuss critical infrastructure challenges and opportunities with leaders who work across governmental and non-governmental sectors at federal, state, and local levels, allowing them to learn from one another in a highly interactive discussion format.

Second, the participants were able to explore specific strategies for addressing difficult problems of practice including critical infrastructure governance, use of federal funds, guarding against both slow- and fast-moving threats, and fostering community trust.

Third, the results of the discussion provided the basis for these published proceedings, which compiles and summarizes ideas that the participants offered throughout the symposium.

We hope this report provides insights and inspiration for others interested in this important policy area. Interested readers with additional questions can contact Prof. Paul Manna (pmanna@wm.edu) for more information about the symposium and this report's conclusions.

Organizations Represented at the Symposium

The ideas and conclusions in this report are the interpretations of the authors and do not necessarily represent the positions of the organizations named here.

City of Richmond, Virginia

City of Newport News, Virginia

Federal Emergency Management Agency

FEWSION, Northern Arizona University

Global Research Institute, William & Mary

Hampton Roads Alliance

Hampton Roads Military and Federal Facilities Alliance

Hampton Roads Sanitation District

James City County, Virginia

National Association of Clean Water Agencies

Office of the Secretary of Defense

Office of the Under Secretary of Defense for Intelligence & Security

North Carolina Department of Transportation, Board of Transportation

State of Washington, Emergency Management Division

Virginia Department of Transportation

Virginia Sea Grant Program

Virginia Institute of Marine Science

U.S. Department of Homeland Security, Cybersecurity & Infrastructure Security Agency

U.S. Army War College

U.S. House of Representatives

U.S. Air Force, Langley AFB

U.S. Army Corps of Engineers

U.S. Navy, Mid-Atlantic

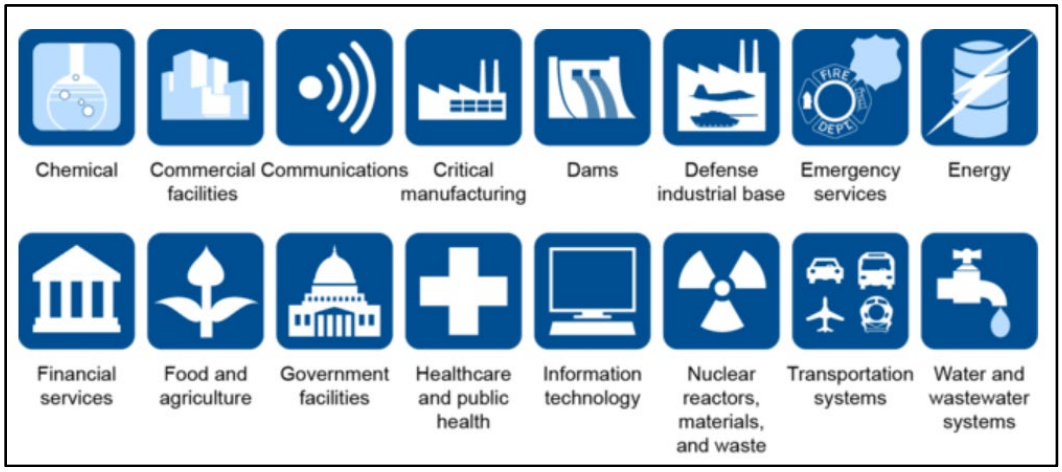
U.S. Coast Guard

W&M Public Policy Program

Definition of Critical Infrastructure

Critical infrastructure is a complex and capacious concept. The Cybersecurity & Infrastructure Security Agency (CISA) within the U.S. Department of Homeland Security has identified 16 sectors that collectively make up the critical infrastructure of the United States. As CISA notes, across these sectors, their "assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[1] Figure 1 lists each sector.

Figure 1. The 16 Critical Infrastructure Sectors



Source: Government Accountability Office. 2023. Critical Infrastructure Protection: Time Frames to Complete DHS Efforts Would Help Sector Risk Management Agencies Implement Statutory Responsibilities (GAO-23-105806). February 7.

[1] Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors.

1. Top-of-Mind Issues

Introduction prompt: What key issue about critical infrastructure is top of mind for you right now? Why is that issue so salient for you?

The symposium began with each participant introducing themselves by describing their daily work and also identifying which aspects of critical infrastructure policy were capturing most of their attention at the moment. Their answers reflected the diverse set of professional backgrounds that they brought to the event and highlighted the multidimensional nature of critical infrastructure policy. The following major themes, summarized in Table 1, emerged in this opening round of discussion.

Table 1. Top-of-mind themes emerging from discussion

Theme	Summary
Communications	Key dimensions include physical critical infrastructure assets that make modern communications possible, and also the processes involved in communicating about critical infrastructure within government, among government and its partners and the broader public, and to the nation's allies and adversaries.
Emerging threats to the homeland	Numerous vulnerabilities are "in play" for adversaries interested in making mischief and doing major harm. Strategies and tactics for confronting emerging threats require complex coordination across government and its partners.
Distribution of federal funding	New funding streams are creating opportunities for infrastructure enhancements, yet varying capacity of subnational governments have produced implementation and equity challenges.
Resilience and aging infrastructure	Environmental changes are outpacing critical infrastructure developments in various sectors. Tensions exist between innovating for the future (inventing new things) and protecting and servicing basic infrastructure assets already in place (maintaining old things).
Building back after disasters	The increasing frequency of severe weather events means that rebuilding is a more regular occurrence. Opportunities exist during rebuilding to assess what resilience strategies and authority structures were effective, and which need revisions.
Interdependencies	The nation's 16 critical infrastructure sectors depend upon one another in various ways. Seeing those connections and their implications for when things might go wrong is important for identifying potential overall weaknesses or vulnerabilities.

Communications. Receiving and transmitting information about critical infrastructure is itself a multidimensional topic. One dimension focuses on the physical aspect of communications, such as broadband technology, cell-phone networks, and military communications networks. These areas all require important investments, maintenance, and

protection. A second dimension focuses on the process of communications, which itself contains internal and external elements. Internal communications are critical within and across government agencies so that public officials can share information as they make plans and respond to fast-moving threats to infrastructure. External communications involve information gathering and sharing with the broader public, and the government's private sector partners. Those channels are vital when danger strikes or when infrastructure systems fail. External communications also involve engaging the nation's allies and also adversaries that might want to do harm to U.S. critical infrastructure. Projecting power that can make adversaries wary of initiating attacks, while simultaneously educating Americans to combat foreign misinformation, which can stoke confusion during fast-moving attacks, are all salient here.

Emerging threats to the homeland. In the increasingly interconnected and complex world, the United States cannot count on its relative geographic isolation from its adversaries for protection. The nation's enemies increasingly see the assets within the nation's boundaries as "in play" and ripe targets for, at best, making mischief and, at worst, inflicting major harm. Given the range of critical infrastructure sectors, federal defense and security agencies and their subnational partners face growing security challenges. For example, a major power outage sparked by a hostile attack, including domestic terrorism, could disrupt the flow of electricity to U.S. military bases, hampering readiness. Managing evolving threats can be tricky because it is not always easy for national government agencies to share intelligence or real-time updates with state and local partners, even though those partners often provide the first line of defense given that all infrastructure failures or disasters begin as local events. As the nation develops and implements its national security strategy, shaping plans that are adaptable and leverage assets across levels of government, not just the U.S. military and security agencies, will remain an ongoing challenge.

Distribution of federal funding. In recent years, the United States has made substantial investments in critical infrastructure, most notably through the passage of the Infrastructure Investment and Jobs Act of 2021.[2] That trillion-dollar act provides tremendous opportunities for bolstering and transforming the nation's critical infrastructure. Nevertheless, taking advantage of the opportunity has been challenging. State and local authorities can be overwhelmed by program complexities and requirements as they attempt to leverage these funds while also spending them on time and in the right ways, consistent with IIJA requirements and other regulatory demands that sometimes are unfunded. Further, capacities of states and localities vary, which risks further exacerbating gaps in infrastructure between high- and low-resourced jurisdictions. Those gaps are most likely to widen when infrastructure funds flow via competitive grant programs.

Resilience and aging infrastructure. In many ways, maintaining, modernizing, and protecting the nation's critical infrastructure involves several different races against time. Keeping ahead of emerging foreign threats is one example, noted above. Another is that changes in the natural environment are moving at a rapid pace and the nation's systems struggle to keep pace. As one symposium participant noted, "Our systems are built for yesterday." Several of those key systems that most people take for granted, such as public works that provide clean

[2] The Brookings Institution is tracking implementation of the IIJA with its Federal Infrastructure Hub resource: https://www.brookings.edu/articles/federal-infrastructure-hub/.

water while removing waste, sometimes do not receive as much attention amidst other efforts to develop next-generation technologies in battery power and telecommunications. Yet very basic elements of those systems, including their pipes and reservoirs and pumping stations, remain vital for the nation's success, even as they depend more on high-tech computer systems for their operation. A further challenge is that professional rewards in the fields of engineering often focus more on the design and construction of new assets, and less on creating viable strategies for maintaining those assets over their lifespans. These challenges have converged with much urgency in the Hampton Roads region in Virginia. The City of Norfolk, for example, a major port and home to Naval Station Norfolk, the largest U.S. naval base in the world, faces substantial challenges due to rising sea levels and also increasing demands for fresh water and electricity from industry and the broader public.

Building back after disasters. The Hampton Roads area of Virginia is no stranger to hurricanes and other powerful storms. Those intense weather events, which nationally are becoming more frequent, create challenges for state and local authorities as they respond to their people's needs. All disasters begin as local events, as the saying goes. They also challenge the federal government given the supportive role it plays in disaster response and simultaneously as it attempts to protect its numerous military assets in the region. Building back after disasters creates a moment where governments and their partners can assess how past development strategies might have mitigated damage. They can use that information to plan future approaches that ensure governments have adequate authority and capabilities to respond and that create good incentives for individuals and businesses to follow practices that can minimize future damage.

Interdependencies: In attempting to maintain and protect infrastructure across the 16 critical sectors that CISA has identified, interdependencies abound. In general, an interdependency exists when the failure of one system creates cascading effects across others. Sometimes these interdependencies are clear for everyone to see, such as a failure of the electrical grid that could undermine other sectors like communications, health care, and public works. Not all interdependencies are obvious, though. For example, state plans for responding to severe weather often assume the availability of state National Guard forces and assets. However, if such an event were to occur simultaneously during a major attack on the nation's infrastructure from a foreign adversary, those assets might be deployed instead to support their federal military missions, leaving states unable to execute their emergency plans. Addressing these complexities requires first recognizing that they exist and then developing defense and response frameworks that can minimize their effects during times of stress or severe danger.

2. Governing Critical Infrastructure within and across Silos

Discussion prompt: How to navigate the challenges that siloed governance creates for critical infrastructure, including during "quiet" times as well as moments before, amidst, and after human or natural disasters?

Policy practitioners everywhere lament the challenges of working in siloed environments that create thorny governance challenges. A major example is the relationship between the military and civilian communities around expectations regarding prioritization and use of infrastructure, especially in times of disaster. More generally, too, within and across the military and civilian sectors, silos can create challenges because government funding comes from numerous sources and interacts with different public and private entities on the ground that actually own the vast majority of the nation's critical infrastructure. Still, the specialization that silos provide can help simplify tasks and make policy implementation more tractable. In discussing this topic, the symposium participants surfaced the themes summarized in Table 2.

Table 2. Governance themes emerging from discussion

Theme	Summary
Benefits of silos	Elected officials and the public often lament agency silos, which sometimes create artificial divisions that fail to reflect the networked conditions existing in the real world. Yet silos also provide division of labor and specialization that can mobilize expertise.
Disaster response	Responding to disasters involves activating siloed organizations so they can operate as high-functioning networks during fast-moving events where lives and physical assets are stressed or in danger.
Foreign threats	Adversaries of the U.S. may exploit vulnerabilities that fall between the cracks of silos involving government and non-governmental actors that manage the nation's critical infrastructure.
Military and civilian sectors	The policy incentives that create "inside the fence" versus "outside the fence" perspectives are strong when it comes to military relationships with local communities. Still, cooperation on critical infrastructure development is possible when leaders prioritize building relationships and embrace creative ways to solve problems.
Funding challenges	Funding streams reinforce silos and create incentives that run against holistic thinking about critical infrastructure maintenance and development. Budget processes and the policy jurisdictions of legislative committees reinforce these tendencies.
Looking ahead	Critical infrastructure professionals see benefits from collaboration across silos but recognize the time constraints and incentives that make these approaches difficult to engineer in practice. Further, emerging technologies may provide opportunities to integrate siloed production of data that are relevant for maintaining and protecting critical infrastructure.

Benefits of silos. Division of labor across government agencies creates operational silos that can exacerbate real-world critical infrastructure problems in ways that complicate policy implementation. The prior discussion about interdependencies, which sometimes cut across different silos, reveals as much. Still, despite these critiques, it is important to remember that silos exist for a reason. Dividing up labor breaks down complicated problems into manageable parts. It also allows governments to mobilize specialized expertise to address particular technical or organizational challenges. Any discussion of reforming how silos operate, then, would benefit from incorporating these ideas, as well, so that critical infrastructure sectors can benefit from these structures while overcoming the weaknesses and blind spots they create.

Disaster response. All critical infrastructure emergencies, whether from natural forces or attacks from an internal or external adversary, are felt most acutely at local levels. During an unfolding disaster and in the immediate aftermath, people in local communities face tremendous interconnected stresses that siloed divisions of labor are challenged to handle. As part of planning for disaster response, then, it is important for critical infrastructure managers to anticipate the personal and professional connections across silos that will be most impactful when danger strikes. That includes thinking about the networks and subnetworks relevant to disaster response, such as key supply chains, the lines of communication and information sharing that they require, and the budgetary processes that allow funds to flow quickly and flexibly to address the most acute needs without becoming ensnared in cross-silo turf battles or unhelpful bureaucratic red tape.

Foreign threats. In the past, a massive nuclear attack was the only scenario where government strategists saw the nation's critical infrastructure as at risk from major non-natural threats. Today, threats are more complex and can involve non-kinetic techniques. Foreign meddling in the operations of the nation's critical infrastructure, such as computer hacking to disrupt major systems or the spread of disinformation campaigns that exploit panic during natural disasters, can pull at the seams between organizational silos. Planning within silos sometimes also makes assumptions about what other silos will do. For example, state or local authorities, via their emergency response plans, may assume the availability of federal assets during a disaster. Their assumptions may be wrong, though, if national authorities simultaneously need to mobilize those same assets to address a foreign adversary that has used the disaster as a window of opportunity to do harm.

Military and civilian sectors. Outside moments when the nation's adversaries may be planning or executing an attack, a common theme that shapes how military and civilian silos interact to manage the nation's critical infrastructure is the notion of concerns that are "inside the fence" of military installations and others "outside the fence." Those distinctions have real policy consequences, but in practice the division is artificial given that transportation, public works, and energy transmission networks within military properties connect to and rely on smooth operations outside those properties, as well.[3] Maintaining robust communication channels between base commanders and their staffs along with local government and private-sector critical infrastructure professionals can enhance daily operations and help solve pressing problems. As an example, the military often prioritizes personnel and tactical concerns over

[3] The brief documentary film *Tidewater* vividly reveals this sort of military and civilian interconnectedness. One can view the film here: https://www.amresproject.org/tidewater-film.

basic needs like keeping public works or energy systems on bases up to date. In contrast, local governments have more robust maintenance and replacement plans for such systems. Creative collaborations can help overcome this disconnect.

Funding challenges. Budget processes often create the silos that exist across the nation's critical infrastructure sectors. Government programs that fund road improvements, support upgrading ports of entry, and defend against cyber or physical attacks all live within specific government agencies that receive funds to support these programs. Those organizational forms are tied to legislative processes baked into committee structures and jurisdictions that elected officials aggressively protect. As such, the resulting funding silos create disincentives for considering holistic concerns across sectors and also across time given that funding cycles imperfectly map onto the timeframes where funds might be needed to seize an opportunity or respond to a pressing need. When those hurdles delay action, scenarios can emerge where a small maintenance issue becomes a pressing need that could require major repairs or renovations.

Looking ahead. Emerging technologies and practices suggest several new options for leveraging the strengths of organizational silos while simultaneously avoiding the many pitfalls documented in this section. Society is becoming increasingly complex, which can accelerate the tendency to divide labor and create more silos. Simultaneously, though, leaders inside and outside government increasingly recognize the impossibility of managing the massive information and data needs that complex systems require. As artificial intelligence (AI) tools become more nuanced and sophisticated, they may be able to mobilize civilian or military agencies more swiftly when disaster strikes a critical infrastructure sector. Additionally, prior to disasters or attacks, sophisticated mapping and network analysis tools, such as those at the FEWSION project of Northern Arizona University,[4] are providing ways for leaders to obtain cross-sector perspectives on their work. That can help them identify relevant partners, including ones that had not occurred to them, and build communication channels that can overcome persistent bottlenecks.

[4] See https://fewsion.us/ for more information.

3. Leveraging Federal Investments for Critical Infrastructure

Discussion prompt: What strategies have federal agencies and governments across states and localities developed to make best use of these funds to support critical infrastructure? Which strategies have been best for avoiding bottlenecks or other administrative problems during implementation?

Federal funding streams amounting to more than one trillion dollars to support critical infrastructure development, maintenance, and protection are flowing from the Infrastructure Investment and Jobs Act of 2021, the Inflation Reduction Act of 2022, and other federal sources, including military budgets. Symposium participants discussed the tremendous potential that comes with these new resources as well as the hurdles that critical infrastructure professionals will need to navigate to spend these dollars well. The key themes from this discussion thread appear below in Table 3.

Table 3. Federal investment themes emerging from discussion

Theme	Summary
Complexity and unintended outcomes	Federal investments in critical infrastructure represent a double-edged sword. On the one hand they provide valuable and needed resources. On the other hand, they increase complexity during policy development and implementation due to foreseen and unforeseen circumstances.
Congressional processes	Congressional budgeting and oversight processes create certain expectations for state and local managers of critical infrastructure, which sometimes are at odds with local conditions or needs. Subnational communication to national elected officials and agency staff can help break through these patterns to foster productive change.
Capacity challenges	Federal funding opportunities do not always become realized on the ground. A big factor contributing to this outcome is the weak capacity that many state and local governments have in competing for funds and in providing matching dollars that some federal grants require.
Sharing lessons	Much untapped potential exists for grant recipients to share knowledge about their experiences working with grants, especially to those with less experience managing large and complex projects. Grant processes with competitive dimensions can limit incentives for this sort of sharing.
Stakeholder and public engagement	Federal funders are increasingly expecting states and localities to incorporate public and other stakeholder input into their grant applications. This requires advance planning and intentionally designed processes to incorporate actual rather than skewed perspectives from the most active groups that might not necessarily be experiencing the greatest needs.

Complexity and unintended outcomes. Securing adequate funds for regular maintenance, substantial upgrades, and new innovations are major issues confronting all of the nation's critical infrastructure sectors. Massive new federal funding streams create opportunities

to address those challenges, but even generous federal funding creates complexities of its own. As noted earlier, state and local governments must have pre-existing capacities to apply for and successfully compete for federal funds. Those realities hit hard, for example, when federal dollars earmarked for rural areas sit unused because those governments lack the systems to apply for them. They also intersect with other constraints, as when spending federal money requires subnational jurisdictions to demonstrate assurances that their critical infrastructure projects uphold environmental or historic preservation goals. Such complexity means that funds meant to accomplish multiple goals, such as the IIJA's push to improve infrastructure and put people back to work, may not reach their full potential due to delays in accessing and spending funds. The sense of urgency around these matters is palpable. As one member of the symposium commented, "federal funding has become a matter of survival, it is no longer just supplemental."

Congressional processes. Legislative processes in the U.S. Congress powerfully shape the use of federal investments in critical infrastructure. Sometimes those processes limit possibilities. The IIJA's restriction that federal military agencies were ineligible for its funds reinforced the "inside the fence" versus "outside the fence" idea referenced earlier. Committee jurisdictions also reinforce the silos problem, and sometimes mean that different silos (i.e., transportation versus electrical grid maintenance) compete against one another. How to address these challenges? Skilled agency administrators at state and local levels recognize that leeway does often exist in federal laws and regulations, but it takes a trained eye to see it. Further, when constituents within a state or congressional district strategize and mobilize their advocacy they increase the chances that their elected representatives will hear their pleas and act in their interests. Crafting compelling, cohesive narratives involving local voices will play to the primary concern of all legislators, namely, how to rack up the most votes in the next election.

Capacity challenges. "Money chases money." That's how one symposium participant summed up the relationship between federal agencies poised to offer critical infrastructure funds to states and localities and those state and local jurisdictions hoping to receive support. Without adequate funding to support grant acquisition and management, subnational government officials will struggle to receive what they believe is their fair share of the pie. Paying grant writers to go after grants makes good sense in theory. It can be difficult to execute in practice, though, if funds do not exist to hire those experts with the pen. As a result, a tendency towards risk aversion can find its way into the thinking of those officials. One other symposium participant echoed this idea in noting how there is "no bigger source of institutional embarrassment" than receiving a grant that you cannot execute.

Sharing lessons. As anyone or any organization that has ever applied for a grant will attest, the processes of applying for, receiving, spending, and closing out a grant produce numerous "ah ha" moments of learning. Some of those moments produce great insights about processes that could provide additional benefits if repeated in the future. Others cut the opposite way when delays, frustrations, and failures manifest. Given these realities, opportunities for grantees to learn from one another is a major gap in the federal grants process. Most collaborative learning opportunities are front-loaded, as when federal agencies host meetings or webinars to explain how to apply for recently announced grants. Those moments are helpful, but perhaps even more so would be additional proactive and real-time sharing among grant recipients across the arc of a grant's life. That could help save time, resources, and human effort

since grant recipients often encounter similar problems but struggle alone to come up with answers. A parallel dynamic exists when grant funds flow via competitions. In those moments, when funds are limited and governments either win or lose, recipients literally are working against one another as they develop their applications. Crafting institutions to facilitate sharing in these contexts, or perhaps creating more grant projects where applicants co-apply with others (i.e., multiple localities or multiple states submitting single proposals) are two ways to leverage sharing of valuable knowledge.

Stakeholder and public engagement. Contemporary federal funding processes for critical infrastructure are increasingly encouraging or requiring local jurisdictions to engage residents and other stakeholders as they craft their proposals. A key goal here is to increase the chances that projects are not simply serving powerful, entrenched interests or overlooking historically underserved or marginalized communities. That will help ensure that past blemishes on critical infrastructure initiatives—as in policies of redlining that shaped urban development and either under-invested in or literally wiped out vibrant Black and immigrant neighborhoods[5]—do not repeat themselves. Broad engagement also recognizes the idea from disaster management that all emergencies start and end locally. Hearing from people not only when their needs are most acute but also during planning to respond to those times of crisis can unearth valuable information and produce more relevant critical infrastructure projects worthy of financial support. Such engagement, if it is to be inclusive, needs to be an ongoing process, then, and not simply timed to the announcement or anticipated announcement of new federal funding streams. An added bonus of regular engagement is that it gives state and local governments and their partners more opportunities to combat misinformation, especially when their outreach strategies involve trusted members of subgroups within their larger communities.

[5] See the Mapping Inequality project at the University of Richmond for more details of these processes and their results: https://dsl.richmond.edu/panorama/redlining/.

4. How Critical Infrastructure Policy Can Bolster or Undermine Trust

Discussion prompt: How do critical infrastructure failures undermine trust? And what can creative leaders do about it?

A compelling challenge confronting public officials at all levels is the declining public trust in government institutions. Strained power grids, flooded streets, and attacks on the nation's critical infrastructure contribute to this problem and cultivate doubts about the government's ability to "deliver" for the American people. This concern becomes especially salient when equity concerns arise and some communities see their needs failing to register on government agendas for infrastructure maintenance or protection. However, leaders who maintain and protect critical infrastructure can use their work to create new wellsprings of trust inside and outside their organizations. Table 4 summarizes key themes from this discussion thread.

Table 4. Infrastructure and trust themes emerging from discussion

Theme	Summary
Communication strategies	Communication about critical infrastructure to partners, constituents, and overseers requires a multifaceted strategy. Otherwise, allowing media or other narratives to drive discussions can foster confusion, mistrust, and, in worst case scenarios, the spread of misinformation.
Over- and under-reactions	Fast-moving events coupled with the speed of modern communications (and the willingness of our adversaries to exploit them) can prompt people to overreact to perceived events that appear to stress or threaten critical infrastructure. Those overreactions have cascading effects, so proactive and swift communication to minimize their effects are key. In contrast, other moments requiring greater concern—as with the mundane but vitally important steps in preparing for storm season or practicing safe computing—receive less attention than they should.
Private sector leadership	Governments supply funds for much of the nation's critical infrastructure while simultaneously, the private sector actually owns many of the assets within the 16 critical sectors. Trust between government and private industry is important for conveying clearly to people how those joint-responsibilities shape people's lived experiences.
Equity	Government priorities often focus on the loudest or most organized communities, which can represent narrow slices of local, state, and national populations. Communication strategies that include all voices, especially those with less power, are important for ensuring that all people, regardless of their societal position, trust that critical infrastructure professionals are looking after their interests.
Local government connections	Fostering trust begins with recognizing who is trusted within various communities. Identifying those leaders and engaging them in conversations about critical infrastructure policy can help enhance the government's reputation and foster co-production around preparedness and disaster response.

Communication strategies. A compelling insight from the symposium participants is that the vast majority of critical infrastructure challenges are not due to a lack of technical knowledge or expertise about how to build a more efficient electrical grid, more efficient system of public works, or more resilient cyber networks. Instead, the most challenging issues involve the human dynamics that govern and oversee critical infrastructure. Chief among them are all of the elements associated with communicating with the broader public. Choosing the proper communication channels for various audiences to ensure that people understand their own personal responsibilities for disaster preparedness or response is one example. Some audiences would prefer modern message forms via social media and text messaging, while legacy systems like making phone calls or old-fashioned mailers to home addresses will be more effective in reaching others. Developing these communication channels is hugely important during crisis moments. However, one should not overlook the value of communication during more "normal" times, too. It can call attention to critical infrastructure success stories and put a human face on work that many people take for granted, while simultaneously building trust between the people and agencies responsible for critical infrastructure.[6] Such trust can help deflect the impacts of misinformation campaigns when disasters do strike, such as when the nation's enemies tried to stoke confusion and mistrust during the tragic East Palestine, Ohio train derailment.[7]

Over- and under-reactions. Every day, the general public's attention is pulled in several directions simultaneously. When people trust critical infrastructure professionals inside and outside government they increase the chances that people will calibrate their reactions to news about critical infrastructure in ways that prevent problems from becoming worse. The East Palestine train derailment, noted above, is one example. The tragedy itself was bad enough, but when the nation's enemies layer misinformation onto those situations, which shapes public opinion, it can dial up fear or mistrust. Whereas that sort of panic can cascade quickly and undermine future cooperation between government and the people, the need to prompt action in more mundane times poses its own challenges. As one symposium participant observed, people nowadays seem to take less personal responsibility for their own preparedness than they did in previous eras (i.e., compare public participation in civil defense during the Cold War compared to hurricane preparedness today). Those under-reactions can be just as devastating as over-reactions to less significant threats. Regular communication from critical infrastructure professionals that foster trust can help calibrate those reactions to meet actual conditions.

Private sector leadership. Reading between the lines of Figure 1, which appeared earlier in this report and summarized the nation's 16 critical infrastructure sectors, one will recognize an important paradox. Although government policy and funding powerfully shape critical infrastructure in the United States, huge swaths of it are owned by the private sector. In addition, technological advancements, such as the development of massive data centers that power cloud computing and AI applications for governments and citizens alike place heavy burdens on the nation's critical infrastructure given their demands for water and electricity. These realities mean that even as the actions of government officials can shape public trust, so too can private sector leadership, especially during times of crisis. The 2021 example of the Colonial Pipeline

[6] An iconic example is the social media work of the Northeast Ohio Regional Sewer District, available at https://x.com/neorsd.

[7] Associated Press. 2023. "Pro-Moscow Voices Tried to Steer Ohio Train Disaster Debate." Voice of America, March 18. https://www.voanews.com/a/pro-moscow-voices-tried-to-steer-ohio-train-disaster-debate-/7011413.html.

Company ransomware attack is an excellent demonstration of how such private sector decision making can influence public trust.[8] The actual attack itself hit the business infrastructure of the company, not the pipeline itself. Still, company leaders decided to shut down the pipeline worrying that it might have suffered a subsequent attack. The crisis only lasted a few days but the panic that rippled across several states in the south and southeast drove up fuel prices and inconvenienced travelers. There was no evidence that the pipeline itself was at risk, but that detail was buried in the flurry of information about the incident. When such systems go down, though, people can be quick to blame the government, which further erodes trust. As such, how governments and private sector leaders cooperate to manage the nation's critical infrastructure is another vital component that can contribute to public confidence in these systems.

Equity. A cross-cutting theme in all the symposium's discussions was how to ensure that the benefits of investing in critical infrastructure do not skew toward the most well-off segments of society while leaving others behind. An important element for avoiding the sordid past of redlining and disasters such as the Flint, Michigan water crisis, for example, involves working extra hard to ensure that government serves all communities well. That means not only holding open meetings and listening sessions where people come to government or other community forums. It also requires critical infrastructure professionals to identify leaders within communities that are chronically underserved and then meet them on their own turf to better understand their priorities and visions of pressing problems or future opportunities. That sort of pro-active engagement will not only increase the chances that investments from the IIJA and other government programs benefit as many people as possible, it will also help governments respond to emergencies when natural disasters or attacks from the nation's enemies occur.

Local government connections. Compelling evidence demonstrates that face-to-face interactions can foster empathy between discussion partners and produce deeper understanding and more effective problem-solving.[9] Local leaders lived these lessons first-hand, as one symposium participant recalled, during the COVID-19 pandemic. When city and county governments set up drive-in clinics to administer testing for the virus, they initially had little luck getting residents to participate. When they pivoted their strategy to include aggressive engagement with key community members, such as religious leaders, and then worked with them as partners the clinics became much more successful. Those same processes of local face-to-face engagement have applications in critical infrastructure policy, as well, given that public opinion polls consistently show that people are more likely to trust local governments than those that are more distant from their lives. Critical infrastructure projects serve as potential sites for rebuilding and reinforcing trust more generally, between ordinary people and the governments that serve them. Those results will not emerge without intentional persistent efforts from local officials, though, as the COVID-19 example here illustrates.

---

[8] U.S. Government Accountability Office. 2021. Colonial Pipeline Cyberattack Highlights Need for Better Federal and Private-Sector Preparedness." May 18. https://www.gao.gov/blog/colonial-pipeline-cyberattack-highlights-need-better-federal-and-private-sector-preparedness-infographic.

[9] Marco Iacoboni. 2009. *Mirroring People: The Science of Empathy and How We Connect with Others*. New York: Picador.

5. Synthesis of key lessons learned and next steps

Discussion prompt: What main ideas from today's discussion resonate most with you? What key question or questions still remain that merit further attention?

The symposium concluded with participants reflecting on the numerous issues across the day's discussion threads. This exchange also included students who attended the event and observed the previous rounds of conversation. As in any symposium where numerous complex issues are on the table, the participants concluded the day with both insights and additional questions. The list in this concluding section reports these ideas in no particular order.

An overarching theme of the day seemed to be "meeting people where they are." Asking questions and then listening to the answers people offer is key. Sometimes information deficiencies can be as simple as not knowing something or not having asked.

"Resources and relationships" appear to be two issues that go hand in hand. When resources appear to serve all people well, and they understand government use of resources and see that they are serving valuable ends, then connections between government and the people are stronger.

Thinking about hierarchies and networks, and how both bear on critical infrastructure maintenance and protection, can provide insights for future policy.

Much evidence documents that people do not trust government. A key priority for critical infrastructure professionals should be to consider *why* that is and what they can do about it through their own policies, initiatives, and communication.

Differences in equity can be apparent even on different sides of the same city. How do local residents perceive these inequalities and how does it affect their interactions with the government? Those who engage are more likely to be listened to, so prompting broad engagement gives government officials the best chance to understand the views of the people they serve.

At what point does hardening infrastructure in some areas become maladaptive to our society? When would disinvestment make sense? Sometimes retreat may be more effective, but it is a challenging message to convey to people who have strong ties to a particular geographic locale.

Sometimes communication only seems necessary in times of crisis but communicating during "quiet times" can actually make it easier, then, for more difficult moments. Stakeholders may not be able to grasp the bigger picture that only governments may be able to see. How does government create forums for proactive, honest discussions?

Misaligned incentives between the public and private sectors can hinder making the best investments or innovations in critical infrastructure. Both sectors value secrecy when

government protects national security information and the private sector deploys proprietary technologies as it seeks profit. But because transparency can be valuable, such as when it allows for swift responses to emergencies, processes that facilitate information sharing are worth pursuing when possible. That sort of problem solving requires difficult and honest conversations.

Re-emphasizing the differences between hierarchy and networks may not be as incompatible as was previously stated. Hierarchies are, after all, simply a specific network form. Can hierarchies be beneficial? Many organizations embrace those forms. They also have shown evidence of adapting toward more democratic forms.

Adversaries can be reinforcing structural issues they see in our democratic systems as a way to turn our institutional structures and governing processes against us.

One strategy for fostering network cooperation is to incentivize critical infrastructure professionals to have regular conversations with external partners a couple of steps removed from their immediate surroundings. That will help deepen everyone's understanding of the complex connections within and across these sectors. Instead of having critical infrastructure professionals see things as "I am responsible" for operations of X, Y, and Z systems, one could reconfigure that understanding so that people think "myself, along with one degree of separation on my network are responsible" for those systems.

In addition to fostering trust between governments and their non-governmental partners, building trust among private partners themselves, who can sometimes be competing against one another for profits and market share, will be essential in some ways to bolster the nation's critical infrastructure.

Policy designs that foster cooperation among governments, as with jointly submitted grant proposals, are rare. Creating more opportunities for joint project submissions could strengthen valuable ties and produce more innovation.

An enduring challenge across critical infrastructure sectors is tracking long-term benefits of programs. How to know when critical infrastructure investments have a good return-on-investment? Outcomes can be complex and difficult to measure, especially when non-events (i.e., cyber attacks are deterred or prevented) count as successes.

In considering government capacity, one can ask what effect does outsourcing government work have on the public's trust in government? What is the level of reliability of the organizations receiving this outsourced work?

Appendix

This appendix contains materials that informed the discussion at the symposium. The participants received these background items in advance of the discussion. The materials appear here in the following order.

Welcome and introduction letter

Symposium agenda

Discussion #1 Background Memo: Governing Critical Infrastructure within and across Silos

Discussion #2 Background Memo: Leveraging Federal Investments for Critical Infrastructure

Discussion #3 Background Memo: How Critical Infrastructure Policy Can Bolster or Undermine Trust in Government