NIAC The President's National Infrastructure Advisory Council

Cross-Sector Collaboration to Protect Critical Infrastructure:

Barriers and Recommendations for Improvement

March 2023

Table of Contents

About the NIAC

The President's National Infrastructure Advisory Council (NIAC) 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

Executive Summary

The security and resilience of our critical infrastructure depends on collaboration across sectors. Significant barriers block effective collaboration. This report analyzes those barriers and presents recommendations to address them.

The NIAC's **recommendations** include the following:

1. Form a convening group to develop cross sector drills to enhance coordinated responses to physical or cyber-attacks on critical infrastructure
2. Harmonize standards that govern common activities of the private sector
3. Enhance coordination among local, state, tribal and federal government entities
4. Engage vulnerable communities in planning and restoration efforts
5. Enhance the timeliness and transparency of threat information
6. Undertake a common cause failure analysis for critical infrastructure supply chains and services
7. Prioritize standard setting in the areas of threat modeling, network segmentation, access provisioning and privileged account management
8. Pilot-test the benefits that additional third-party certifications can provide to sector and cross-sector stakeholders
9. Develop methods to ensure timely delivery of infrastructure support provided by the Infrastructure Investment and Jobs Act and the Inflation Reduction Act
10. Ensure consistency in international trade requirements and "Buy America" mandates in federal, state and local contracts
11. Examine development of additional mechanisms and forums to enhance opportunities for cross-sector collaboration

The NIAC concludes that standards governing the security and resilience of critical infrastructure assets should be mandatory. The NIAC acknowledges that standards need to be developed with industry input, but standards should ultimately be mandatory when they deal with security vulnerabilities that could impact the provision of critical infrastructure across sectors. This report also explains why such standards should be outcome-based. Outcome-based standards identify *what* needs to be addressed to ensure cross-sector physical and cyber security while leaving the *how* (i.e., the specifics of how each provider adjusts its business practices to meet that standard) to the providers themselves.

Introduction

On December 27, 2022, The National Security Council (NSC) tasked the NIAC to examine cross-cutting infrastructure policy challenges. The Cross-Cutting Infrastructure Policy Challenges Subcommittee, which was comprised of 13 Subcommittee members, was formed to draft a report to address the tasking on behalf of the broader NIAC. The Subcommittee members examined the means to improve cross-sector collaboration both within the private sector and between the private and the public sectors.

As a result of its deliberations, the NIAC:

- Identified nine barriers to cross-sector collaboration;
- Provided eleven specific recommendations; and
- Provided its input on whether standards governing critical infrastructure should be mandatory or voluntary.

1. The NIAC's Charge

The NSC tasked the NIAC with the following:

> *Short-term Study*
>
> *The confluence of significant changes in the threat environment, increasing reliance on new technologies, and major infrastructure investments present an opportunity to develop consensus recommendations regarding several urgent, cross-cutting infrastructure policy challenges.*
>
> *For report-out at the March 2023 Quarterly Business Meeting, the NIAC will assess and develop recommendations to improve U.S. infrastructure resilience and security (with specific emphasis on cybersecurity and physical attacks; climate change and natural disasters; labor; and supply chain fragility) regarding the following:*
>
> - *What are the primary barriers to cross-sector collaboration (e.g., planning, regulation, data, standards, risk-equivalency, intelligence, etc.) and how can government and the private sector work together to break down the siloes?*
> - *What are the NIAC's views on voluntary versus mandatory standards for addressing the risks noted above to U.S. infrastructure resilience and security?*
> - *What role should private sector owner/operators have in reducing the potential risks of cross-sector interdependencies?*

To undertake its work and with input from NSC staff, the Subcommittee defined the scope of cross-sector collaboration as encompassing:

- Collaboration on infrastructure resilience and security among sectors within the private sector;
- Collaboration of those sectors with federal, state and local governments; and
- Collaboration between government, the private sector and academic institutions.

2. Subcommittee Activities

The Subcommittee held the following meetings and received the following briefings from key Cybersecurity and Infrastructure Security Agency (CISA) and NSC officials:

January 23, 2023 – Kickoff meeting for the Subcommittee.

January 30, 2023 – Subcommittee meeting with briefing from Jennifer Pedersen, Deputy Assistant Director (Acting) National Risk Management Center (NRMC), CISA, who spoke about the NRMC's current work followed by a question-and-answer session.

February 6, 2023 – Subcommittee meeting focusing on Subcommittee Member discussion around the three short-term study topic questions. Chair Manu Asthana sought written submittals from the Subcommittee members on the following three areas below and using three scenarios as a general guide: a global pandemic, a natural disaster and a broad based cyberattack on U.S. critical infrastructure:

- *Identify the top two to three areas where the Subcommittee member's sector needs to collaborate with another sector or the government, and where it is believed that the needed collaboration is unlikely to occur adequately.*
- *Identify from each Subcommittee member their views as to what needs to change for this collaboration to occur when needed in a crisis.*
- *Identify if this change should be mandated or voluntary, and why*.

February 9, 2023 – Subcommittee briefing from Anne Neuberger, Deputy National Security Advisor for Cyber and Emerging Technologies, who spoke about the Biden Administration's efforts to secure critical infrastructure, with a focus on the sector-by-sector interdependencies approach to establish minimum cybersecurity requirements, followed by a question-and-answer session.

February 16, 2023 – Subcommittee meeting focusing on discussion of the initial draft report for the Short-Term Study Topic.

February 23, 2023 – Subcommittee meeting, with comments provided by invited NIAC members on the draft report.

February 27, 2023 – Subcommittee meeting focusing on final discussion and comments from Subcommittee members.

3. Organization of this Report

This report is organized as follows:

1. Barriers to Cross-Sector Collaboration across the Sectors details the Subcommittee's identification of barriers to needed cross-sector collaboration designed to improve United States (U.S.) infrastructure resilience and security.
2. Recommendations provides specific recommendations on improving cross-sector collaboration both among private sector providers of critical infrastructure and between such providers and the public sector.
3. Voluntary or Mandatory Critical Infrastructure Standards provides the Subcommittee's views on whether standards coming out of this process should be mandatory or voluntary.

Barriers to Cross-Sector Collaboration across the Sectors

The NIAC identified the following common themes as overarching potential barriers to cross-sector collaboration.

1. Lack of Clarity in Decision-Making and Command

In addressing events such as a pandemic, cyberattack or physical disaster, our complex governance structure of potentially overlapping national, state and local authorities (and the lack of clear decision-making authority among them) can hinder proactive planning and organized responses. For example, during national infrastructure disasters, layers of government must negotiate their respective responsibilities in responding to the disaster at hand. Moreover, within the federal family of agencies, notwithstanding existing lead agency protocols, there can be a lack of clear authority leading to disparate answers to industry or delays in times when swift decision-making is needed. As different sectors of the economy work with and report to a panoply of federal, state or local agencies, this decision-making complexity can inhibit cross-sector collaboration with the private sector. These kinds of barriers have been witnessed in such events as the response to Hurricane Katrina, the provision of personal protective equipment (PPE) during the early days of the pandemic, and responses to natural and man-made attacks on critical infrastructure.

The need for **clear proactive decision-making and command** is not limited to the public sector. In the private sector, resources are not always harnessed across sectors effectively during incidents to ensure a comprehensive response. For example, local marine resources can be extremely valuable in disaster response to assist with evacuations, flow of disaster-response supplies, and restoration of critical cargo flows. Yet to be effective, local and regional entities must coordinate responses to ensure quick access to and direction for deployment of maritime assets during natural disasters. More proactive planning and clarity of decision-making processes would allow for this enhanced level of cross-sector collaboration.

2. Risk Equivalency

Critical infrastructure sectors may have **different risk tolerance levels** based on how a particular risk impacts their operations and their legal and fiduciary duties. However, increased mutual interdependencies create challenges when managing various risk equivalencies across sectors. For example, if a disruption in the electric sector denies power to the communications sector for a prolonged period of time, then the communications sector may be unable to provide services to the electric sector. Identifying these critical time-sensitive interdependencies can help to prioritize restoration efforts.

3. Lack of Outcome-Based Goals to Secure Critical Infrastructure

In setting clearly defined common goals to secure critical infrastructure, there should be a focus on *shared outcomes* that participating sectors and government partners seek to achieve collective action. More work both across the sectors and between the public and private sector is sorely needed to identify more **outcome-based common goals**. Making the goals outcome-based is key because industries in different sectors (and even within sectors) will have different ways of reaching the same outcomes.

4. Inflexibility of Legal Requirements that Can Hinder Rapid Responses

The public sector is often expected to be nimble when responding to physical or cyber threats to critical infrastructure. Yet public sector officials face many laws and regulations that require **extensive legal processes** to be followed in the course of such a response. Government agencies can find themselves bound by statutes that govern their actions and which may not allow them to modify or depart from those procedures in emergencies. Congress has begun to address these issues by enacting the Fixing America's Surface Transportation (FAST) Act, which provides new authority to the executive branch to address cybersecurity incidents more quickly. Yet laws in other areas, ranging from antitrust laws to environmental laws, often lack this flexibility to respond to emergency situations, short of the President declaring a national emergency under the Stafford Act.

5. Cross-Sector Supply Chain Physical and Cybersecurity Challenges

As our nation's industries have become more dependent upon one another, information sharing and cross-sector collaboration concerning **commonly used hardware and software inputs** grows in importance. This need exists both for physical dependencies but is even more pronounced in addressing cybersecurity concerns with products received from others in the supply chain. The NIAC identified three examples: 1) the growing need for increased coordination between the electricity and natural gas sectors; 2) the healthcare sector's challenge in managing different proprietary platforms to access medical records; and 3) issues faced by shipping companies versus port facilities in reconciling separate protocols and information systems. In short, if various industries in the supply chain are not communicating and developing workarounds for damaged or compromised hardware and software inputs, the entire supply chain can face crippling interruptions.

6. Cross-Sector Skills Training and Workforce Development

To maintain a strong economy, critical infrastructure sectors will need to continually **attract new talent** both in the public and private sectors, **retain trained workers** and **develop a skilled workforce** that can support highly integrated and co-dependent industries. Similarly, the public sector is facing significant retirements of experienced employees while we need qualified government workers supporting the public sector.[1]

The NIAC also noted that the ability to attract talent in the information technology (IT) sector varies significantly between industries. Specifically, it is easier for industries where IT is part of their core business to attract highly skilled talent as compared to industries where it is a necessary component but not the core function of the business. This can leave these latter industries hard pressed to find talent to meet their cybersecurity needs. This problem is exacerbated for the public sector which must compete for talent with the private sector in the IT field. The NIAC noted the need for talent in the private sector to be available to provide education and support to the public sector given the inherent lack of symmetry in the public sector's ability to attract and retain highly skilled talent in the IT area.

[1] A good example of a national collaborative effort to develop a skilled labor force can be found in the *'Be Pro Be Proud'* initiative which is designed to reach young Americans to stimulate their interest in these needed technical jobs of the future. See www.beprobeproud.org

7. Need for Common Standards to Protect Critical Infrastructure

Our critical national infrastructure is becoming increasingly cross-sector dependent. This was illustrated dramatically by the impact of supply chain issues during the pandemic. Those issues affected a host of industries that depend on the timely delivery of key components ranging from steel to electric transformers to PPE. In addition, given our increased cross-sector dependence on information technology, cybersecurity is increasingly becoming a critical cross-sector area of concern. The **lack of baseline cybersecurity standards** allows for different levels of rigor toward employing good cybersecurity hygiene across industries. The lack of basic standards can also result in a diminished focus and unintentionally encourage **relaxed approaches to security** as businesses weigh the cost of enhancing their cyber and physical security with maintaining their competitive position in the market.

The lack of common standards affecting critical infrastructure encompasses more than cybersecurity. Industries that operate in multiple jurisdictions can face a panoply of local risk assessments and inconsistent required mitigation actions during an emergency. For instance, during the COVID-19 pandemic, the marine transportation industry was often shut down in one locale yet permitted to operate with mitigation in another. The electronic vehicles (EV) charging industry is another industry that increasingly needs a common set of standards since it requires a degree of consistency across state and local jurisdictions to provide a safe and secure infrastructure for use by the traveling public. By the same token, the electric industry is attempting every day to manage a product that travels at the speed of light and does not respect state borders yet faces a host of different regulatory regimes at the state and federal level.

8. Need for More Intelligence Sharing from the Government

The threat landscape around cybersecurity grows each day. Timely sharing of sensitive intelligence related to cyber activity is critical both before and during broad cyberattacks involving one or more critical infrastructure industries. Moreover, for smaller organizations with facilities that are critical for national security, the federal government may need to consider subsidizing the buildout of collaborative capabilities to receive and process the intelligence information they may receive.

The NIAC recognizes the sensitivities around sharing of intelligence information. However, the NIAC believes there is a difference between sharing the ***source of the threat,*** which the private sector does not necessarily need to know, versus more specifics on the ***nature of the threat*** so the private sector can take self-help steps to mitigate.

9. Need for Private Sector Information Sharing Regarding Vulnerabilities

Developers of systems and assets are naturally cautious about providing information about potential vulnerabilities in the systems they provide to their downstream customers. In addition to the competitive sensitivity of such information, antitrust laws can serve as a block to sharing such information both vertically within the supply chain and horizontally among common businesses.

Similar barriers exist in ensuring that a provider of cyber software or hardware identifies the key interfaces with stakeholders that use the product and may be affected by any vulnerabilities. For example, from both cyber and commerce perspectives, there is inadequate understanding of the private versus public inter-workings of ports and the marine transportation system's interaction with other surface transportation modes.

Many private industries as well as government share a **lack of recognition and consistent proactive communication** of cross-sector dependencies for cyber and physical attack prevention and restoration. To illustrate, the electricity sector is becoming increasingly dependent on the natural gas sector, yet the physical and cybersecurity regulatory requirements for each industry are different. The NIAC identified the need for common approaches to maintenance and security upgrades to critical infrastructure such as dams, levees, pipelines and related physical infrastructure that can affect public safety.

Recommendations

Subcommittee members proposed a range of recommendations as solutions to the barriers identified above. Some recommendations were very specific to industries while others cut across multiple sectors. Although Subcommittee members proposed many industry-specific recommendations, for purposes of this report, the NIAC wishes to flag the following cross-sector proposed recommendations[2]:

1. Form a Convening Group to Develop Cross-sector Drills to Enhance Coordinated Responses to Physical or Cyberattacks on Critical Infrastructure

Although the federal government has established a series of sector-specific collaboratives, (such as the Electricity Subsector Coordinating Council), the NIAC recommends additional coordination *across* those sectors that could be most affected by a physical or cyberattack on critical infrastructure. For example, through the GridEx[3] exercise, the electric sector across the U.S. undertakes drills in response to scenarios that simulate cyber and physical attacks. Cross-sector collaboration is needed to undertake similar drills, which will identify potential impacts across sectors and enhance coordination on restoration. Timely restoration of critical infrastructure is growing in importance as the severity and frequency of events increases. Such cross-sector drilling would also help to identify potential proactive, pre-disaster steps that sectors could undertake to help plan for and mitigate the impact of a given attack. **The NIAC recommends that the NSC gather and analyze informal activities that have been undertaken in this area in the past and use that information to help inform the development of the drills and the scenarios chosen.**

One possible targeted exercise scenario could posit a coordinated cyberattack on major national or regional electrical transmission and distribution systems with resulting long-duration power disruption to cargo and passenger terminals, waterway infrastructure (navigation systems, bridges, etc.), shore power systems for vessels, and electrified cargo handling/lifting equipment as well as electrified vessels/vehicles (tugs, ferries and drayage trucks, etc.).

The exercise could assess how enhanced cross-sector coordination, including a dedicated cross-sector coordination function facilitated by CISA during an event, could help:

1. Isolate the spread of the attack from the grid into the transportation systems;
2. Mitigate the impacts on critical supply chains flowing through the port; and

[2] The ordering of the recommendations in this report is not intended to connote a NIAC statement on the relative priority of each of these recommendations as the priorities may well differ among the diverse industries represented in the NIAC.

[3] GridEx is the largest grid security exercise in North America. GridEx gives Electricity Information Sharing and Analysis Center (E-ISAC) member and partner organizations a forum to practice how they would respond to and recover from coordinated cyber and physical security threats and incidents.

3. Facilitate trade resumption (or shifting certain trade to other ports) as quickly as possible.

The primary goal would be to demonstrate the value of a cross-sector coordination function during such attacks and determine how this function could best support existing incident command structures and sector-specific agencies/sector-coordinating councils.

2. Harmonize Standards that Govern Common Activities of the Private Sector

The NIAC recommends that the federal government consider establishing streamlined processes and best practice standards for common activities such as employee background verification and supply chain security authorization. Such standards and best practices could then be subject to a third-party audit to guarantee that weaknesses in one part of the supply chain do not provide a springboard opportunity for bad actors to attack adjacent co-dependent services.

In the utility sector, the Federal Energy Regulatory Commission, which is charged with ensuring bulk electric system reliability, needs additional coordination with federal and state air-permitting bodies. For example, due to local air permitting requirements, gas transmission operators have had to switch from gas-fired to electric-driven compression, which is dependent on purchasing power from the grid. As a result of a siloed approach between the reliability and the environmental regulator these two critical infrastructure systems have become newly interdependent. This then inadvertently creates a new cross-sector vulnerability and the potential to exacerbate a single point of failure. Government agencies and critical infrastructure owners must improve coordination of regulatory requirements and standards to avoid creating new cross-sector vulnerabilities.

3. Enhance Coordination Among Local, State, Tribal and Federal Government Entities

The NIAC recommends developing and drilling a common playbook that would ensure greater coordination among local governments and among local, state, tribal and federal government entities. The playbook can start with documented takeaways from past events and include specified timelines for developing or revising practices and then drilling for them. Financial incentives for cooperation among these layers of local, state, tribal and federal government would help to maximize their coordination and cooperation.

As noted in the discussion of Barrier 1, the NIAC recognizes existing protocols establishing a lead federal agency with jurisdiction over critical infrastructure. The NIAC believes that further strengthening the lead agency concept would help to ensure more consistent and timely responses across federal agencies. The NIAC believes that a positive step in this area would be to undertake a desktop study of past collaborations within the federal family of agencies that have worked well, and contrast these with past efforts that have failed in this regard.

4. Engage Vulnerable Communities in Planning and Restoration Efforts

The NIAC notes that planning for and exercising restoration efforts should not be limited to industry providers. A successful restoration effort needs to create public trust from the outset. This is particularly important in vulnerable communities that often can be the most affected yet the hardest to reach during such events. **The NIAC recommends including vulnerable communities in planning and restoration efforts.**

This includes low-income communities, tribal communities and organized labor, each of which are critical to planning for and executing a successful restoration effort.

5. Enhance the Timeliness and Transparency of Threat Information

Virtually every sector represented in the NIAC noted the need to receive timely and transparent threat information. For instance, without transparent information, maritime operations that can support disaster response and provide flow of needed cargo cannot continue. **The NIAC recommends sharing early assessment, communication of a threat and its impact on critical infrastructure as early as possible.** NIAC members noted that even if the information is uncertain or imprecise, the dissemination of preliminary warning information to critical infrastructure providers is essential so that early-stage assessments and mitigation efforts can begin to isolate the impact of any potential attacks.

6. Undertake a Common Cause Failure Analysis for Critical Infrastructure Supply Chains and Services

For critical hardware and software components of critical infrastructure, there is a greater risk of unrecognized common cause failures that can simultaneously defeat multiple safeguards. Common cause failure occurs when multiple components of a system fail due to a single common cause. Major natural disasters, intentional acts, and even global pandemics have the potential to drive common cause failures that defeat multiple levels of individual safeguards. These common cause failures can result from a physical incident (e.g., widespread flooding in a region), cyberattacks (e.g., attacks that disable common equipment in many different systems in many different sectors such as common control systems) or significant operational changes necessitated by a public health crisis (e.g., understaffing and/or unavailable personnel with specialized expertise, lack of PPE, etc.).

Most sectors have performed some level of analysis where equipment and systems are most critical to their operations, but few (if any) have a detailed understanding of how *simultaneous* loss of those systems or equipment across multiple modes or sectors could escalate consequences to unexpected levels. **The NIAC recommends performing common cause failure analysis from a multi-sector viewpoint,** which could provide critical insights about unrecognized national and regional vulnerabilities beyond today's more sector-specific focus. Specifically, studying how critical supply chains and services could be disrupted through common cause failures would provide insights to help identify critical cross-sector initiatives that could help to lower vulnerabilities across sectors.

7. Prioritize Standard Setting in the Areas of Threat Modeling, Network Segmentation, Access Provisioning and Privileged Account Management

In the arena of cybersecurity, it is important to prioritize the areas where standard setting would be most beneficial. **The NIAC recommends prioritizing standard setting in the following areas:**

- Threat modeling/vulnerability assessments;
- Network segmentation;
- Access provisioning;
- Privileged account management;
- Patch management; and

- Clear pathways for real time sharing of legally protected information (such as between the health care sector, law enforcement and regulatory communities).

It was noted that Information Sharing and Analysis Centers (ISACs) can be used to increase the effectiveness of cross-sector information sharing and provide a safe harbor from potential legal liability associated with this level of information sharing.

Standards developed in these critical areas must apply to software and hardware operating system suppliers and not just users of critical information systems. Critical infrastructure providers who are represented in the NIAC (which range from airline to water to communication and energy service providers) are effectively end users dependent on those critical operating systems. As a result, the definition of "providers of critical infrastructure" should not be limited to these end-use providers but must include the developers and vendors of the operating systems upon which end-use providers depend.

8. Pilot-Test the Benefits that Additional Third-Party Certifications Can Provide to Sector and Cross-sector Stakeholders

Third-party certifications have become a commonly accepted requirement to participate globally in many supply chains. For example, many organizations will only buy products and services from organizations with approved ISO-9001 quality management systems, ISO-14001 environmental management systems or IS0-27001 information security management systems. The federal government now requires certain cybersecurity systems to be in place for federal contracts (e.g., CMMC certification and NIST Risk Management Framework conformance). Expanding requirements for third-party certification for cybersecurity, disaster preparedness or even pandemic preparedness could help to provide co-dependent stakeholders with confidence that their partners are demonstrating due diligence in managing their shared risks. **The NIAC recommends a pilot test to identify the benefits of additional third-party certifications.**

Third-party verification and certification can also be a basis for granting business incentives between stakeholders that encourage adoption of enhanced, voluntary cybersecurity standards beyond minimal cybersecurity regulations. Incentives to consider include financial incentives (e.g., discounted pricing/fees for certified organizations), operational incentives (e.g., priority service/scheduling or reduced operational red tape), or even a vertical supply chain vendor certification as a pre-condition to supplying the needs of critical infrastructure providers. A project of this type would engage a set of stakeholders to develop the protocols and incentives and help to identify trusted third-party agents to conduct the necessary validation and certification activities.

9. Develop Methods to Ensure Timely Delivery of the Infrastructure Support Provided by the Infrastructure Investment and Jobs Act and the Inflation Reduction Act

Through the Infrastructure Investment and Jobs Act (IIJA) and the Inflation Reduction Act (IRA), Congress has provided an unprecedented level of funding to support infrastructure development across many sectors. Although the NIAC acknowledges the importance of appropriate legal requirements to govern any disposition of federal funds, **the NIAC recommends a renewed effort to ensure that the infrastructure funding under this legislation can be delivered in a timely and responsible way.** Specifically, federal and state procurement models should be analyzed to facilitate use of alternative delivery methods other than the traditional "design-bid-build" model based on procurement of the lowest bid. Alternative procurement

methods could include, for example, progressive design-build awards that allow projects to move forward in a more timely and structured way.

For instance, in many areas of the country, our national waterways infrastructure needs to be repaired or rebuilt. The U.S. Army Corps of Engineers (Corps) funding rules do not appear to allow the Corps to use future revenues to move forward on these projects through public-private partnership agreements. The NIAC recommends that federal procurement rules be re-examined to ensure timely but responsible funding of critical infrastructure projects in accordance with IIJA and the IRA.

10. Ensure Consistency in International Trade Requirements and "Buy America" Mandates in Federal, State and Local Contracts

The NIAC recommends that government officials ensure consistency in international trade requirements and "Buy America" mandates in federal, state and local contracts. Some NIAC members develop critical infrastructure which must compete in international markets. One example discussed on this topic was that if the federal government were to set more consistent mandates on use of sustainable green methods to produce steel, such action would have the potential to avert several today's supply chain issues and allow for quick mobilization of domestic steel production in case of natural disaster or intentional attack.

11. Examine Development of Additional Mechanisms and Forums to Enhance Opportunities for Cross-Sector Collaboration

The work of the NIAC has underscored fundamental commonalities—namely how representatives from very different industries and sectors can come together to identify common barriers to cross-sector collaboration and develop specific recommendations that would enhance such collaboration. The NIAC recommends that the federal government, working with the NIAC and others, **examine enhancing existing forums and processes and potentially develop new ones to further these efforts.** This review could include developing processes for collaborating with industry on the standard-setting process described in Recommendation #2. The NIAC looks forward to serving as a resource to effectuate this recommendation.

Voluntary or Mandatory Critical Infrastructure Standards

Although NIAC members recognized the value of voluntary coordination and collaboration among private sector entities and between the private and public sectors, given the cross-sector interdependencies of critical infrastructure, there was a consensus that **in key areas such as cybersecurity, it is time to move toward more mandatory standards rather than relying solely on appeals to altruism or consideration of best practices.** This is not a criticism of the public or private sectors but simply a recognition that when dealing with critical infrastructure, a weak link in the chain can have significant implications for other sectors that depend on that same critical infrastructure. One NIAC member stated the following:

> "Private business views voluntary standards as additional cost and thus must weigh the benefits and downsides to meeting such standards. This creates a negative headwind to compliance and immediately creates uncertainty and inequity in products, thus depleting the security of the entire interconnected critical infrastructure system—we are only as strong as our weakest link."

For the same reason, industries that operate in multiple jurisdictions (ranging from the electric sector to the maritime and healthcare sectors) bear increased costs and decreased efficiencies because they must respond to multiple and sometimes conflicting government assessments of risk and appropriate mitigation steps. NIAC members noted that such common standards have been developed within the European Union,[4] and stress that involvement of the private sector along with other stakeholders is key to developing effective standards capable of implementation.[5]

The NIAC's view is that any standards related to the protection and resilience of critical infrastructure be outcome-based: they should focus on the objective to be achieved while leaving flexibility for how an individual meets the standard's requirements. As a shorthand for this concept, the NIAC recommends that any mandatory standards focus on the *what* (i.e., the objective to be achieved) rather than dictating the *how* (i.e., the details of how the standard is to be met by any individual or group of critical infrastructure providers). Appendix A of this report is a list and brief description of standards applying to various critical infrastructure providers that, in the NIAC's view, represent good examples of effective performance-based standards.

Although there are many areas where development of mandatory standards could be appropriate, as a matter of prioritization, the NIAC members noted that the physical security or cybersecurity of critical infrastructure and the delivery of essential services should receive the highest priority because they impact public safety. As noted by one NIAC member:

> "I believe standards must be mandated to be fully effective since collaboration requires similar commitments across many parts of the economy, where incentives to make improvements are not always aligned. It is critical that industry input is closely considered in the establishment of mandates to be sure that such mandates are practically feasible."

The NIAC also highlighted that any standards addressing the security of critical infrastructure assets not only focus on the ultimate provider but also reach all critical suppliers in the supply chain that manufacture the hardware and software components providers rely upon. For example, it is not effective to place cybersecurity compliance standards on providers of critical infrastructure without applying the same standards up the chain to those who provide operating systems providers depend upon.

Call to Action

Due to the ambitious timeline given by the NSC's tasking, the NIAC worked quickly to pull its network of resources from across the critical infrastructure industry to share challenges they face when considering cross-sector collaboration. The **nine barriers** to cross-sector collaboration and **eleven recommendations** identified in this report are the product of this impactful six-week study, and this report offers the government many suggestions for potential policy changes.

---

[4] See e.g., Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) | Shaping Europe's digital future (europa.eu)

[5] The process for developing the Interim Final Rule adopting Chemical Facility Anti-Terrorism Standards (CFATS) could be seen as an example of a successful process that involved significant industry as well as public reach-out by the federal government. See How It All Began: The History and Making of the CFATS Program | CISA.

The NIAC urges the President to consider these recommendations for immediate and long-term implementation to improve the nation's critical infrastructure resilience and security through increasingly essential collaboration across sectors.

Appendix A: Examples of Performance-Based Standards for Providers of Critical Infrastructure

1. North American Electric Reliability Corporation Cybersecurity Standards

- **Performance Measure CIP-002-5.1:** This rule requires companies to establish and maintain a cybersecurity risk management program that is based on industry best practices. The performance measure specifies that the program must include policies, procedures and processes for identifying, assessing and mitigating cybersecurity risks.
- **Performance Measure CIP-003-7.1:** This rule requires companies to have a documented security management process for critical cyber assets. The performance measure specifies that the process must include procedures for identifying, classifying and protecting critical assets from cyber-attacks.
- **Performance Measure CIP-004-7.1:** This rule requires companies to have a documented personnel and training program that includes cybersecurity awareness training for all employees. The performance measure specifies that the program must be updated regularly to reflect new threats and best practices.
- **Performance Measure CIP-007-6.1**: This rule requires companies to have a documented system security plan for each critical cyber asset. The performance measure specifies that the plan must include a risk assessment, a security control baseline and procedures for monitoring and managing the asset's security.

***NIAC's Comment**: Overall, these performance-based rules provide a framework for companies to establish and maintain effective cybersecurity programs that protect the electric grid from cyber threats. By measuring their performance against these rules, companies can identify areas for improvement and ensure that their cybersecurity practices are up-to-date and effective.*

2. Transportation Security Administration (TSA) Pipeline Cybersecurity Standards

- **TSA Security Directive 2c; Section I:** TSA has significantly revised the Security Directive initially issued in July 2021 to provide owner/operators with more flexibility to meet the intended security outcomes while ensuring sustainment of the cybersecurity enhancements accomplished through this Security Directive series. The transition to a more flexible, performance-based approach requires all owner/operators to submit a Cybersecurity Implementation Plan for TSA approval. This plan, once approved by TSA, will set the security measures and requirements against which TSA will inspect for compliance.
- **TSA Security Directive 2c, Requirement B, 2:** The Cybersecurity Implementation Plan must provide the information required by Sections III.A. through III.E. of this Security Directive and describe in detail the owner/operator's defense-in-depth plan, including physical and logical security controls, for meeting each of the requirements in Sections III.A. through III.E.

***NIAC's Comment**: Instead of mandating in detail the types of tools, functions, processes and specific controls which an owner/operator must implement, TSA Security Directive 2c requires each owner/operator to create a Cybersecurity Implementation Plan (CIP) which details how they intend to meet the outcomes the TSA describes later in the directives. In each of the specific TSA Security Directive requirements, it is noteworthy that specific timelines are not mandated, and most requirements are at the outcome/strategic level. The requirement also provides for the development of exception processes where safety or operational impacts may need to be considered. As such, they focus on the outcomes they want achieved and leave it to*

owner/operators to describe how they plan to comply/achieve those outcomes (along with when and how). This is all to be documented in a CIP, which then is reviewed by the TSA, and once approved, will form the basis for future inspection and regulatory review.

3. Federal Risk and Authorization Management Program (FedRAMP) for Cloud Technologies

- **FedRAMP** is a government-wide program that promotes the adoption of secure cloud services across the federal government by providing a standardized approach to security and risk assessment for cloud technologies.

NIAC's Comment: *FedRAMP establishes a standardized approach to security and risk assessment for federal agencies that can then be applied by each agency to meet its specific cloud service needs. The objective-based standard also drives security in the private sector as all cloud service providers that wish to do business with the federal government must receive their FedRAMP authorization.*

4. Payment Card Industry (PCI) Security Standards

- **PCI standards** have been established by a set of companies from the payment industry coming together to develop baselines for security conformance as well as means for third party compliance testing. Standards are developed through collaborative processes overseen by the PCI Standards Security Council.

NIAC's Comment: *One of the pillars of the PCI Standard Setting process is its flexibility and adaptability. The goals of the process are described by the PCI Standards Security Council as:*

- *Evolving security standards and validation programs to support a range of environments, technologies and methodologies for achieving security. This ensures standards and resources that support and enable safe commerce have the flexibility to use different approaches to meet those standards.*
- *Increasing standards alignment and consistency of PCI standards to minimize redundancy and support effective implementation.*

Appendix B: Acknowledgements

Subcommittee Members

Manu Asthana (Chair), President and CEO, PJM

Alan Armstrong, President and CEO, Williams Inc.

Joshua Descant, CEO, REV/REV Business

Michael Hayford, CEO, NCR Corporation

Connie Lau, President and CEO (Retired), Hawaiian Electric Industries (Former)

Pasquale Romano, President and CEO, ChargePoint

Conrad Vial, Senior Vice President and Chief Clinical Officer, Sutter Health

Sadek Wahba, Chairman and Managing Partner, I Squared Capital

Christopher Wiernicki, Chairman, President and CEO, American Bureau of Shipping

Craig Glazer, Vice President, Federal Government Policy, PJM

Dan Antilley, Executive Vice President and Chief Security Officer, NCR Corporation

K.N. Gunalan, AECOM

Jamey Barbas, New York State Thruway Authority

Member Points of Contact

Janet Britton, REV/REV Business

Amanda Mertens Campbell, Williams Inc.

Colton Ching, Hawaiian Electric Company, Inc.

Beth Keolanui, Sutter Health

Katie Tomarchio, ChargePoint

David Walker, American Bureau of Shipping

Subcommittee Briefers

Anne Neuberger, Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technologies

Jennifer Pedersen, Deputy Assistant Director (Acting), National Risk Management Center (NRMC), CISA

Subcommittee Expert

Carol Haddock, Houston Public Works

Appendix C: Definitions

Term	Common Definition
Access Provisioning	Coordinating user accounts, password management, email authorizations, and other tasks.
Common Cause Failure	When multiple failures occur in a short period of time, due to a common cause.
Cross-Sector Collaboration	When two or more organizations work together across sectors to achieve mutually beneficial outcomes.
Cybersecurity Hygiene	The steps that users of computers and other devices take to maintain system health and minimize risk.
GridEx	The largest grid security exercise in North America
Network Segmentation	Dividing a computer network into smaller parts to improve network performance and security.
Privileged Account Management	Privileged Account Management (PAM) is a domain within Identity and Access Management (IdAM) focusing on monitoring and controlling the use of privileged accounts.
Stafford Act	Gives the president the power to declare a national emergency as a response to a national disaster.
Threat Modeling	Activities for improving security by identifying threats, and then defining countermeasures to prevent or mitigate them.
Third-Party Certifications	When an independent organization reviews processes and independently determines the final product meets specific standards for safety, security, or performance.
Third-Party Verifications	When a company uses an outside organization to review and confirm the accuracy of information.

Appendix D: Acronyms and Abbreviations

Acronym/ Abbreviation	Definition
CEO	Chief Executive Officer
CFATS	Chemical Facility Anti-Terrorism Standards
CIP	Cybersecurity Implementation Plan
CISA	Cybersecurity and Infrastructure Security Agency
CMMC	Cybersecurity Maturity Model Certification
Corps	U.S. Army Corps of Engineers
EISAC	Electricity Information Sharing and Analysis Center
EV	Electronic Vehicles
FAST	Fixing America's Surface Transportation
FedRAMP	Federal Risk and Authorization Management Program
IIJA	Infrastructure Investment and Jobs Act
IRA	Inflation Reduction Act
IT	Information Technology
NIAC	National Infrastructure Advisory Council
NIST	National Institute of Standards and Technology
NRMC	National Risk Management Center
NSC	National Security Council
PCI	Payment Card Industry
PPE	Personal protective equipment
Subcommittee	Cross-Cutting Infrastructure Policy Challenges Subcommittee
TSA	Transportation Security Administration
U.S.	United States

Appendix E: References

Be Pro Be Proud. https://www.beprobeproud.org/.

CISA Chemical Security. "How It All Began: The History and Making of the CFATS Program." Cybersecurity and Infrastructure Security Agency. Last modified June 7, 2022. https://www.cisa.gov/news-events/news/how-it-all-began-history-and-making-cfats-program.

"Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)." European Commission. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

ESCC Electricity Subsector Coordinating Council. https://www.electricitysubsector.org/.

Federal Energy Regulatory Commission. https://www.ferc.gov/.

"Fixing America's Surface Transportation Act or 'FAST Act.'" U.S. Department of Transportation. Last modified December 4, 2015. https://www.transportation.gov/fastact.

"GridEx VII." E-ISAC Electricity Information and Analysis Center. https://www.eisac.com/s/gridex.

PCI Security Standards Council. 2019. "Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards." Pcisecuritystandards.org. 2019. https://www.pcisecuritystandards.org/.

"Pipeline Security Guidelines | Transportation Security Administration." https://www.tsa.gov/travel/frequently-asked-questions/pipeline-security-guidelines.

"Program Basics | FedRAMP.gov." https://www.fedramp.gov/.

"Stafford Act." FEMA. https://www.fema.gov/disaster/stafford-act.

"Standards." https://www.nerc.com/pa/Stand/Pages/default.aspx.