NIAC The President's National Infrastructure Advisory Council

Future Focus Study

Strengthening the NIAC Study Process

May 2017

DRAFT

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.dhs.gov/national-infrastructure-advisory-council.

Table of Contents

I. Executive Summary

For more than 15 years, the President's National Infrastructure Advisory Council (NIAC) has provided insights into the challenges and risks facing the Nation's critical infrastructure. It conducted 27 studies that produced 270 recommendations on what the Federal Government can do to reduce infrastructure risks and assist the private sector in risk mitigation.

The NIAC heard from senior leaders in government and industry that the Council is viewed as an independent voice on crosscutting critical infrastructure issues. Its studies provide objective insights, comprehensive research, and clear solutions to improve critical infrastructure security and resilience.

In preparation for a new Administration, the NIAC was asked to evaluate its prior work to identify ways it can improve its study process, develop more actionable recommendations, and identify potential topics that could be examined in future studies. Although NIAC studies are viewed as valuable and influential, the change in Administration provided an opportunity for the Council to evaluate its work and identify ways to be even more impactful in the future.

Strengthening the NIAC Study Process

The NIAC Future Focus Study Working Group interviewed senior leaders in government and the private sector, including current and former NIAC members; reviewed prior recommendations and studies; and conducted open-source research. The Working Group derived the following insights on NIAC work from this review:

1. The role and capabilities of the NIAC are often not well understood.
2. NIAC recommendations do not always reach the right people to drive action.
3. NIAC studies could make a greater impact by delivering interim recommendations as the study progresses.
4. Comprehensive, detailed reports may be too dense for easy use by all stakeholders.
5. Recommendations that are clearly outside of an agency's existing mission, budget, and authority—or do not identify specific actions—may not gain traction.

Specific Process Improvements

To address these opportunities, the Working Group identified ways to be more effective and efficient in the NIAC study process and to produce more impactful recommendations. The following process improvements were approved by the Council at its February 16, 2017 Quarterly Business Meeting (QBM) and will be codified in the NIAC's bylaws:

- Conduct scoping studies prior to full NIAC studies to further define topics and better understand the current risk landscape; and engage in an iterative tasking process with the White House and National Security Council (NSC) to ensure study outcomes have maximum value.
- As appropriate, provide recommendations at multiple points throughout a study to support immediate action. Direct recommendations at a specific agency, considering its budget, mission, and authority.
- Engage national experts earlier in the process—for example, during the scoping study—and continue that engagement through interviews, panel discussions, and briefings to gather original insights.

- Deliver final recommendations and study materials in a format that provides the right level of detail to the right audience to drive action; and conduct strategic outreach following public release and approval of NIAC recommendations to increase awareness.

Potential Topics for Future NIAC Study

The NIAC was tasked to develop a list of potential future topics that would be relevant, have impact, and add value to critical infrastructure security and resilience. The Working Group developed potential topics based on an analysis of previously covered topics; open-source research; and insights from interviews with Federal Government leaders, private-sector partners, and NIAC members. Candidate topics were required to:

- Address an urgent national critical infrastructure problem that could cascade across sectors and jurisdictions;
- Require joint action by the private and public sectors;
- Focus on risks to sectors or functions that threaten national or economic security and/or human health and safety;
- Consider cross-sector interdependencies; and
- Result in potential solutions that could be applied broadly across multiple sectors.

The Working Group prioritized potential topics further by asking whether a NIAC study would add significant value on the topic, address a gap in an existing body of work, provide an opportunity for Federal solutions, and result in short-term and long-term recommendations. This analysis resulted in seven topics that the NIAC could study at the request of the President:

1. Incorporating resilience into Federal capital planning and recovery investments
2. Using insurance to recognize and reward investment in resilience
3. Public-private, cross-sector, and regional information sharing
4. Cross-sector interdependency risks during long-duration energy disruptions
5. Port infrastructure security and resilience
6. Workforce trends affecting critical infrastructure security and resilience
7. Security and resilience of oil and natural gas transit by pipeline and rail

Moving Forward

The NIAC is well-positioned to examine the most pressing risks facing the Nation's critical infrastructure and has the ability to develop actionable solutions for the Federal Government. The process improvements approved by the NIAC in its February QBM are within the Council's existing authorities under its executive order and charter. These improvements do not make any fundamental changes to how the NIAC operates, but rather allow it to better respond to the more dynamic risk environment the Nation faces. The NIAC has already taken steps to implement these process improvements through this study and its task to scope a cyber study, which is currently in process.

II. Study Methodology

The President's National Infrastructure Advisory Council (NIAC) was established to examine the most important risks facing our Nation: how to protect and secure the infrastructure that underpins the economy, national security, and public health. For more than 15 years, the Council has provided insights into the challenges and risks facing the Nation's critical infrastructure and provided 270 recommendations on what the Federal Government can do to address these risks and assist the private sector.

Charge to the NIAC

The NIAC was tasked to **review past studies and recommendations** to identify ways it can improve the development of future studies and recommendations to make them even more impactful. The Council was also asked to **consider new areas for future studies** based on trends, known gaps, and vulnerabilities, and to provide an analytically informed list of recommended study topics for consideration by the new Administration. The NIAC was simultaneously tasked with conducting a scoping study for a cyber study that the Council could be tasked with in 2017. The Working Group conducted a Cyber Scoping Study in parallel to this effort and reported results separately.

Study Structure

To conduct this study focused on strengthening the NIAC study process, the Council formed the Future Focus Study Working Group made up of eight NIAC members, to examine existing processes and prior recommendations.

To complete the study, the Working Group:

- Interviewed 20 senior leaders in government and the private sector, including current and former NIAC members (See Appendix A for a list of report contributors);
- Built upon the analysis of prior recommendations completed by the former NIAC Designated Federal Officer (DFO) (See Appendix D);
- Conducted an in-depth examination of two previous NIAC studies to identify best practices and the characteristics of successful NIAC recommendations (See Appendix E and Appendix F); and
- Examined the role of NIAC compared to other senior executive councils (See Appendix G).

The study resulted in:

- Insights on the impact of NIAC studies.
- Process improvements that were approved by the NIAC and codified in its bylaws.
- A list of seven potential topics for future studies.

III. Strengthening the NIAC Study Process

The NIAC Future Focus Study Working Group interviewed senior leaders in government and the private sector, including current and former NIAC members; reviewed prior recommendations and studies; and conducted open-source research to review the effectiveness of NIAC studies.

Insights on NIAC Studies

NIAC studies provide objective insights, comprehensive research, and clear solutions to improve critical infrastructure security and resilience. The Future Focus Study identified the following areas for study improvement:

1. **The role and capabilities of the NIAC are often not well understood**. Senior leaders in government and industry may not understand NIAC's role and capabilities, due in part to the variety of councils that have similar missions, engage with the private sector, and have chief executive officer (CEO) members. Clarifying the roles and capabilities of these bodies will reduce confusion and help implement NIAC recommendations.
2. **NIAC recommendations do not always reach key stakeholders who can drive action**. The NIAC transmits its reports to the White House through the Homeland Security Secretary and presents its recommendations during public meetings. But this process may exclude key stakeholders in Federal agencies and the private sector who can help implement recommendations.
3. **NIAC studies could make a greater impact by delivering interim recommendations as the study progresses**. NIAC studies are typically completed in 9–18 months. While this in-depth topical review is valuable, by waiting to the end of the study to deliver all of its recommendations the Council may miss opportunities to influence key policy decisions.
4. **Comprehensive, detailed reports may be too dense for easy use by all stakeholders**. To capture the breadth of data and evidence to support NIAC study findings and recommendations, final NIAC study reports can exceed 200 pages. While rich in detail, the reports are not easily digested by all stakeholders, which may hinder implementation.
5. **Recommendations that are clearly outside of an agency's existing mission, budget, and authority—or do not identify specific actions—may not gain traction.** The most successful recommendations—ones that were acted upon by an agency or sector—from past NIAC studies identified a specific agency with the budget, mission, and authority to take action, and were aligned with agency priorities or existing initiatives or with national goals.

Specific Process Improvements

The NIAC identified several ways to be more effective and efficient in its study process and to produce more impactful recommendations. The following process improvements were approved by the Council at its February 16, 2017 Quarterly Business Meeting (QBM) and will be codified in the NIAC's bylaws.

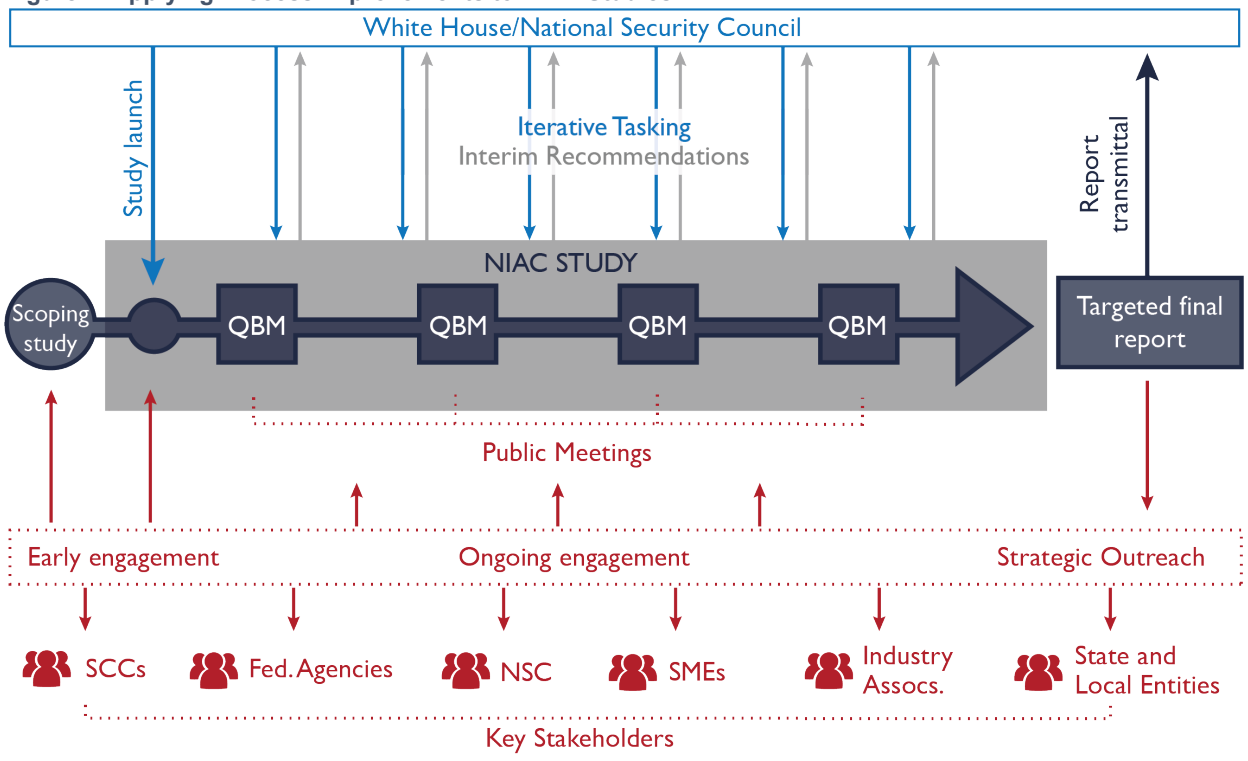
- Conduct scoping studies prior to full NIAC studies to further define topics and better understand the current risk landscape. This will help the NIAC to identify the most crucial issues to examine and avoid any duplication of effort.
- Engage in an iterative tasking process with the White House and National Security Council (NSC) to ensure outcomes have maximum value.

- Continuously engage with and enable the White House to ask questions or provide insights throughout the process.
- As appropriate, provide recommendations at multiple points throughout a study to support immediate action. Recommendations should be directed at a specific agency, considering the existing budget, mission, and authority of the agency; and align with national policy goals and objectives

- Engage national experts earlier in the study process through interviews, panel discussions, and briefings to gather original insights, and conduct extensive research into the given topics.
- Deliver final recommendations and study materials in a format that provides the right level of detail to the right audience to drive action.
- Conduct strategic outreach following public release and approval of NIAC recommendations to increase awareness of the NIAC and its recommendations.

To implement the identified process improvements, the NIAC needs to update the typical study process to be more dynamic and flexible. For example, the Council should provide recommendations at multiple points throughout a study to support immediate action, and engage key stakeholders—such as Sector Coordinating Councils (SCCs) and subject matter experts (SMEs)—earlier in the study process, starting with a scoping study. The following graphic demonstrates how these process improvements could work in practice.

Figure 1. Applying Process Improvements to NIAC Studies



The approved process improvements build on prior success. Most recently, in the 2016 *Water Sector Resilience* study report the NIAC recommended the U.S. Department of Homeland Security (DHS) and the U.S. Environmental Protection Agency work with other key agencies and stakeholders to conduct a joint tabletop exercise to test resilience during a large-scale disruption. Agencies with clear mission and authority were identified in the recommendation, and the study engaged members of the Water Sector Coordinating Council who were integral in driving action on the exercise. Planning for the exercise started in the fall of 2016.

IV. Potential Topics for Future NIAC Study

As part of this effort, the NIAC was tasked to develop a list of potential future topics that would be relevant, have impact, and add value based on analysis of previously covered topics and insights from Federal Government leaders, private-sector partners, and NIAC members. An overview of these topics is included in the text box below. More detailed descriptions, including suggested study charges, are included in Appendix B. Appendix C provides a timeline of NIAC study topics to date.

Topic 1: Incorporating resilience into Federal capital planning and recovery investments. The Administration has indicated its plans to invest up to $1 trillion in infrastructure. An investment of this size offers an enormous opportunity to build resilience into the Nation's infrastructure and ensure that investment decisions made today deliver the best possible value over the life of the infrastructure.

Topic 2: Using insurance to recognize and reward investment in resilience. Insurance is often seen as an important market mechanism to help differentiate and reward companies that invest in security and resilience to lower their risks, without new regulations. A NIAC study could determine if there is a role for the Federal Government to improve policies, information, and tools to enable the insurance industry to incentivize good risk management practices.

Topic 3: Public-private, cross-sector, and regional information sharing. Despite enormous efforts to address barriers and breakdowns to public-private intelligence sharing since the September 11th attacks and key examples of success, getting the right information to the right people at the right time remains one of the most intractable issues for critical infrastructure partners.

Topic 4: Cross-sector interdependency risks during long-duration energy disruptions. A widespread disruption of the power grid or fuel supply lasting weeks or months has significant national security, human safety, and economic consequences. As our digital economy grows and sectors become more intertwined and automated, the risk of systemic failure becomes more likely, but it is also very difficult to define and measure.

Topic 5: Port infrastructure security and resilience. America's dependence on ports means that even light physical damage to a major U.S. port can result in significant economic impacts that can cascade across national markets. Prior work has identified a myriad of risks to ports, but there is a need to identify how to incorporate resilience into Federal funding and other efforts.

Topic 6: Workforce trends affecting critical infrastructure security and resilience. The Nation's critical infrastructure systems rely on a skilled workforce to operate them effectively and reliably. The workforce challenge is two-fold: 1) increasing automation requires a new set of skills and experience, and 2) older workers with extensive experience are retiring without adequate transfer of knowledge and skills.

Topic 7: Security and resilience of oil and natural gas transit by pipeline and rail. Pipelines, rail transit, and the oil and natural gas industries are regulated at the Federal and State level. These sectors face risks similar to other critical infrastructure sectors, such as aging infrastructure, extreme weather, terrorism, and cyberattacks. A NIAC study could identify ways to promote resilience within the current regulatory structure.

Appendix A. Acknowledgements

Working Group Members

Process Evaluation and Path Forward

Joan McDonald (Co-Chair), Principal, JMM Strategic Solutions

Beverly Scott, Ph.D., CEO, Beverly Scott Associates, LLC (NIAC Vice Chair)

Jan Allman, President, CEO, and General Manager, Marinette Marine Corporation

Cyber Scoping Study

Mike Wallace (Co-Chair), Former Vice Chairman and COO, Constellation Energy

Robert Carr, Founder and Chairman, Give Something Back Foundation; and Founder and former CEO, Heartland Payment Systems

Ben Fowke, Chairman, President, and CEO, Xcel Energy

Constance Lau, President and CEO, Hawaiian Electric Industries, Inc. (NIAC Chair)

Keith Parker, General Manager and CEO, Metropolitan Atlanta Rapid Transit Authority

Interviewees and Report Contributors

Scott Aaronson, Executive Director, Security and Business Continuity, Edison Electric Institute

Rich Baich, Chief Information Security Officer, Wells Fargo and Company; Chair, Financial Services Sector Coordinating Council (FSSCC)

Cherri Black, Critical Infrastructure Strategist, Idaho National Laboratory

Alfred R. Berkeley, III, Chairman, Princeton Capital Management, and former NIAC Chair, Vice Chair, and member

John Carlson, Chief of Staff, Financial Services Information Sharing and Analysis Center (FS-ISAC); Vice Chair, FSSCC

R. James Caverly, Adjunct Research Staff Member, Institute for Defense Analyses; and former Director, Partnership and Outreach Division, Office of Infrastructure Protection (IP), U.S. Department of Homeland Security (DHS)

Darrell Darnell, Senior Associate Vice President for Safety and Security, The George Washington University; former National Security Council (NSC) staff

Caitlin Durkovich, Director, Toffler Associations; and former Assistant Secretary, IP, DHS

Albert J. Edmonds, Lt. Gen. USAF (Ret.); Chairman and CEO of Edmonds Enterprise Services, Inc.; CEO of Logistics Applications, Inc.; and current NIAC member

Tom Fanning, Chairman, President, and CEO of Southern Company; Chair of the Federal Reserve Bank of Atlanta; Chairman of the Edison Electric Institute; and Co-Chair of the Electricity Subsector Coordinating Council (ESCC)

Glenn Gerstell, General Counsel, National Security Agency (NSA); and former NIAC member

Eric Goldstein, Branch Chief, Partnership and Engagement, Office of Cybersecurity and Communications, DHS; former Senior Counselor to the Undersecretary, National Protection and Programs Directorate (NPPD), DHS

Margaret E. Grayson, President, Commercial Sector of Consulting Services Group; and current NIAC member

Patricia A. Hoffman, Principal Deputy Assistant Secretary and Acting Assistant Secretary, Office of Electricity Delivery and Energy Reliability, U.S. Department of Energy

Elena Kim-Mitchell, Director, Private Sector Partnerships, Office of Partnership Engagement, Office of the Director for National Intelligence (ODNI)

Bob Kolasky, Acting Deputy Under Secretary, NPPD, DHS; Acting Assistant Secretary, IP, DHS

Saba Long, Owner, Obelisk Strategies

Monica Maher, Director for Cybersecurity, NSC

Lisa McFadden, Program Manager in the Water, Science, and Engineering Center, Water Environment Federation

Nathaniel T. Millsap Jr., Director of Industrial Security and Technology, Marinette Marine Corporation

Richard Moore, Associate Director for Security Policy and Plans, U.S. Department of Transportation

Kevin Morley, Ph.D., Manager of Federal Relations, Government Affairs Office, American Water Works Association

Stephanie Morrison, Director, Critical Infrastructure Policy, NSC

Bill Nelson, President and CEO, FS-ISAC

Kshemendra Paul, former Program Manager of the Information Sharing Environment, ODNI

Brian Peretti, Director, Office of Critical Infrastructure Protection and Compliance Policy, U.S. Department of Treasury

Mary Peters, Principal, Mary Peters Consulting; former U.S. Secretary of Transportation; and former Federal Highway Administrator

Amy Pope, Nonresident Senior Fellow, The Atlantic Council; former Deputy Assistant to the President; and Deputy Homeland Security Advisor, NSC; and current NIAC member

Frank Prager, Vice President, Policy and Federal Affairs, Xcel Energy

Jonathan Reeves, Manager, Office of Emergency Management, District of Columbia Water and Sewer Authority; Chair, Water Sector Coordinating Council (Water SCC)

Scott Seu, Senior Vice President, Public Affairs, Hawaiian Electric Company

Robert Stephan, Colonel USAF (Ret.); Executive Director, Gryphon Scientific; and former Assistant Secretary, IP, DHS

Rivka Tadjer, Chief of Staff, Give Something Back Foundation

Brian Tishuk, General Counsel, FS-ISAC; Executive Director of the FSSCC

Ahsha Tribble, Ph.D., Deputy Regional Administrator, Federal Emergency Management Agency, Region 9; and former NSC staff

Robert Walters, Vice President of Construction and Engineering, Davidson Water, Inc.; Vice Chair, Water SCC

Nancy Wong, former Designated Federal Officer, NIAC

Department of Homeland Security Study Support Resources

Ginger Norris, Designated Federal Officer, NIAC, IP, DHS

Beth Ward, Nexight Group, LLC

Jack Eisenhauer, Nexight Group, LLC

Megan Wester, BayFirst Solutions, LLC

Appendix B. Review of Potential Topics for Future NIAC Study

The National Security Council (NSC) asked the President's National Infrastructure Advisory Council (NIAC) to develop a list of potential future topics that would be relevant, have impact, and add value to critical infrastructure security and resilience. The Future Focus Study Working Group developed potential topics based on an analysis of previously covered topics; open-source research; and insights from interviews with Federal Government leaders, private-sector partners, and current and former NIAC members.

Screening Criteria

As part of the process, candidate topics were required to:

- Address an urgent national critical infrastructure problem that could cascade across sectors and jurisdictions;
- Require joint action by the private and public sectors;
- Focus on risks to sectors or functions that threaten national or economic security and/or human health and safety;
- Consider cross-sector interdependencies; and
- Result in potential solutions that could be applied broadly across multiple sectors.

The Working Group prioritized potential topics further by asking whether a NIAC study would add significant value on the topic, address a gap in an existing body of work, provide an opportunity for Federal solutions, and result in short-term and long-term recommendations. This resulted in the selection of the following seven topics that the NIAC could be tasked with in the future.

Potential Future Topics

Topic 1 Incorporating resilience into Federal capital planning and recovery investments

Across the board, U.S. critical infrastructure faces aging assets and a significant funding gap for repair and replacement, compounded by an increasingly complex threat environment. To meet this need, the Administration has indicated a forthcoming investment of $1 trillion in America's infrastructure.[1] Most of these projects will be expected to withstand an unpredictable risk environment—from extreme weather to cyber threats to population growth—for at least the next 30 to 50 years. An investment of this size offers an enormous opportunity to build resilience into the Nation's infrastructure and ensure that investment decisions made today deliver the best possible value over the life of the infrastructure.

Federal capital planning, disaster recovery investments, and permitting decisions each offer mechanisms to incorporate resilience requirements, ensuring that selected projects are providing the best long-term value by considering long-term maintenance costs, the ability of infrastructure to withstand an extreme event, and other costs that may accrue over the life of the infrastructure. Resilience standards, requirements, and criteria for resilience in federally funded infrastructure projects is currently not well-defined.

[1] Zanona, "Trump's infrastructure plan: What we know," *The Hill*, 2017.

Suggested Study Charge: *Review current Federal funding and regulation for infrastructure investment and identify how criteria for resilience could be applied to federally funded infrastructure projects both in new infrastructure development—including new digital infrastructure—and rebuilding following an event.*

Prior NIAC Work: Multiple NIAC studies have recognized the need to build resilience into infrastructure investments and capital planning decisions, including the 2015 *Transportation Sector Resilience* study, 2014 *Critical Infrastructure Security and Resilience Research and Development Plan* study, 2013 *Strengthening Regional Resilience* study, and 2010 *A Framework for Establishing Critical Infrastructure Resilience Goals*.

Discussion: The Nation's critical infrastructure is aging, and there is a significant funding gap of $5.6 trillion needed through 2040 to make the necessary investments in infrastructure, according to the 2016 *Failure to Act* report from the American Society of Civil Engineers (ASCE).[2] This investment gap is coupled with a capital planning process that does not adequately take into account emerging threats—such as more sophisticated cyberattacks and extreme weather events—nor effectively prioritize resilience innovations that may be more costly to build but that reduce the need for costly upgrades and repairs down the line.

The Administration's infrastructure plan is currently taking shape, and the President has indicated his desire to cut regulatory red tape as part of this plan.[3] Project sponsors and investors often cite Federal permitting processes as a source of delay and uncertainty in planning for the delivery and financing of infrastructure projects, noting that predictability in permitting requirements is essential to mitigating risk. Over the past three years, Federal agencies have worked to expedite the review and permitting of more than 50 major infrastructure projects—including bridges, transit, railways, ports, roads, and renewable energy projects—while protecting communities and the environment; during this time, more than 30 of those projects have completed the permitting process. For example, Federal agencies completed the permitting and review for the Tappan Zee Bridge in 1.5 years, which would normally take three to five years.[4]

Well-defined criteria for resilience in Federal funding decisions will allow the Federal Government to provide clear project requirements to the private sector that reduce uncertainty and encourage innovation; maintain speed and efficiency during competitive selection; and extract maximum value from infrastructure investments over the lifetime of new assets.

Topic 2 Using insurance to recognize and reward investment in resilience

In competitive markets, owners and operators struggle to invest in security and resilience measures that protect against uncertain risks. Insurance is often seen as an important market mechanism to help differentiate and reward companies that invest in security and resilience to lower their risks, without new regulations. Yet the insurance industry lacks effective methods to measure and value risk reduction based on a company's risk management practices and level of mitigation. Is there a role for government to improve policies, information, and tools that would enable the insurance industry to offer policies that incentivize good risk management practices and discourage reliance on a Federal disaster safety net?

Suggested Study Charge: *Examine the challenges and barriers preventing the insurance market from appropriately assessing and encouraging resilience, and identify measures Federal and State governments could take to promote incentives for risk mitigation and resilient practices in underwriting.*

Prior NIAC Work: NIAC studies as early as 2005 have examined the potential for new market forces to incentivize resilience investments. The 2013 *Strengthening Regional Resilience* study recognized the need for a paradigm shift in the way the nation funds resilience, recommending new financial incentives or

[2] American Society of Civil Engineers, *Failure to Act: Closing the Infrastructure Investment Gap for America's Economic Future,* 2016.
[3] Zanona, "Trump's infrastructure plan: What we know," *The Hill*, 2017.
[4] U.S. Department of Treasury Office of Economic Policy, *Expanding Our Nation's Infrastructure through Innovative Financing,* 2014.

practices that shift spending away from disaster recovery and toward resilience. Most recently, the 2015 *Transportation Sector Resilience* study recommended the use of insurance to incentivize these investments. The role of insurance in critical infrastructure protection was discussed as early as the Council's 2005 *Risk Management Approaches to Critical Infrastructure Protection* study.

Discussion: As Federal disaster declarations have increased and the Federal Government bears escalating recovery costs, insurance reform offers a promising mechanism to encourage pre-disaster infrastructure upgrades; promote resilience innovations that typical regulations often discourage; and share disaster risks and costs across the public and private sector. Risk models indicate that the annual likelihood of severe weather causing at least $1 billion in insured losses in the United States is 92 percent.[5] Hurricane Katrina, and more recently Superstorm Sandy, demonstrate that extreme weather can create enormous local destruction and disruption with rippling economic impacts and service disruptions across large regions. Yet the significant infrastructure upgrades needed to address low-probability, high-consequence events do not receive adequate investment, in part because these events are difficult to predict.

Baseline risk management practices do not exist for all critical infrastructure sectors and cannot be leveraged as a "gold standard" for the private industry in seeking coverage. In addition, emerging or evolving threats—such as cybersecurity—need to be included in future discussions about insurance reform. The NIAC has heard in its work on previous studies that insurance could be used to incentivize these needed investments, but it is difficult to set a value on resilience.

Topic 3 Public-private, cross-sector, and regional information sharing

Information on threats to infrastructure, potential vulnerabilities, and likely impacts underlies nearly every security decision made by owners and operators of critical infrastructure. Despite enormous efforts to address barriers and breakdowns to public-private intelligence sharing since the September 11th attacks and key examples of success, getting the right information to the right people at the right time remains one of the most intractable issues for critical infrastructure partners. Individual sectors have established common partnership mechanisms through the Government Coordinating Councils (GCCs) and Sector Coordinating Councils (SCCs) and through information-sharing platforms, such as Information Sharing and Analysis Centers (ISACs), that permit actionable and timely information sharing. Though they follow common models, the partnership councils and ISACs operate effectively with strong engagement in some sectors, but have gained little traction in others. Understanding why effectiveness differs could inform efforts to replicate success across the critical sectors.

Suggested Study Charge*: Examine current collaboration processes (at executive and operational levels) and identify measures and structures to promote and strengthen information and resource sharing across sectors and within and across regions.*

Prior NIAC Work: The 2012 *Intelligence Information Sharing* study recommended solutions to improve information-sharing authorities and how they are implemented; identify intelligence requirements; improve the content, value, and timeliness of information products delivered to industry; and better leverage critical infrastructure partner capabilities for counterintelligence. This study built on prior findings in the 2004 *Evaluation and Enhancement of Information Sharing and Analysis* study and 2006 *Public-Private Sector Intelligence Coordination* study. The 2015 *Executive Collaboration for the Nation's Strategic Infrastructure* study also recommended a CEO-level framework as key elements to successful partnership and information sharing.

[5] Executive Office of the President of the United States, *Standards and Finance to Support Community Resilience,* 2016.

Discussion: The U.S. Intelligence Community collects information on infrastructure threats and vulnerabilities that can inform owners and operators as they decide which assets to protect, which resilience investments to make, where security upgrades are needed, how to plan for potential disasters, and how to prevent an incident or respond in the immediate aftermath. In turn, owners and operators that report incidents, attack attempts, and suspicious activity to public-sector partners can help intelligence officials and law enforcement identify trends and coordinated attacks. Information sharing among private-sector partners within and across sectors is equally critical. Yet effective information-sharing mechanisms require trusted relationships, engaged partners, and sufficient resources to analyze and share information rapidly and safely.

There are many dedicated platforms to information sharing with critical infrastructure partners, including the coordinating councils (SCCs and GCCs), ISACs, the Homeland Security Information Network Critical Infrastructure (HSIN-CI), classified intelligence briefings for cleared owners and operators, the National Cybersecurity and Communications Integration Center (NCCIC), and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), among many others.[6] Some platforms operate more effectively than others and have gained more traction and trust from private-sector partners. In October 2016, the U.S. Department of Homeland Security (DHS) released the *Critical Infrastructure Threat Information Sharing Framework*, which aims to clarify the process, partners, and mechanisms for multi-directional information sharing in the critical infrastructure community across the public and private sectors.[7]

In the 2015 Sector-Specific Plans, infrastructure owners and operators in nearly every sector identified many of the same information-sharing challenges described in the NIAC's 2012 study. The roles of DHS, the Intelligence Community, and State/local law enforcement, along with their authority and capabilities, are still not fully understood within the private sector. Owners and operators do not see information sharing with the private sector as a high priority for the Intelligence Community as a whole, and the information they receive is not always relevant or actionable. Even when information is relevant, it may not be disseminated in a timely or efficient manner. There is little incentive and much disincentive for sharing information both within the infrastructure protection/Intelligence Community and within competitive industries. These barriers are particularly acute with respect to cyber intelligence.

Conversely, several organizations and partnerships have successfully surmounted these barriers. The Financial Services ISAC, for example, is viewed as a timely and authoritative information source among a highly competitive sector. The Electricity Subsector Coordinating Council (ESCC) offers another example of engagement at the executive level to address and mitigate high-priority threats through information sharing and collaboration. Improving information sharing across the board requires a better understanding of why information-sharing efforts using similar models succeed in some cases and fail in others.

[6] U.S. Department of Homeland Security (DHS), "Information Sharing: A Vital Resource for Critical Infrastructure Security," 2017.
[7] U.S. Department of Homeland Security (DHS), *Critical Infrastructure Threat Information Sharing Framework: A Reference Guide for the Critical Infrastructure Community,* 2016.

Topic 4 Cross-sector interdependency risks during long-duration energy disruptions

A widespread disruption of the power grid or fuel supply lasting weeks or months has significant national security, human safety, and economic consequences. As our digital economy grows and sectors become more intertwined and automated, the risk of systemic failure becomes more likely, but it is also very difficult to define and measure. Current multi-sector response and recovery planning largely focuses on short-term disasters. High-impact threats, like a massive cyber attack, an electromagnetic pulse (EMP), or coordinated attacks on critical delivery infrastructure, could create long-term disruptions over wide geographic areas by, for example, draining spare equipment reserves. A long-duration energy disruption exposes unidentified risks across the tightly integrated lifeline sectors, and leads to coordination and resource gaps that slow recovery.

Suggested Study Charge: *Building on prior studies on the energy infrastructure and cross-sector risks, examine the interdependencies, avenues for engagement, and response capabilities between lifeline infrastructures during a long-term energy disruption. Identify Federal actions or mechanisms to incentivize cross-sector risk management and improve cross-sector engagement, planning, and resource sharing for major disruptions.*

Prior NIAC Work: The 2010 *A Framework for Establishing Critical Infrastructure Resilience Goals* study examined the Energy Sector's resilience to a major energy disruption and risks to interdependent sectors. The 2013 *Strengthening Regional Resilience* study's case study on Superstorm Sandy illustrated how lifeline sector interdependencies can permit a domino effect of disruptions regionally, and how long-term disruptions to power and fuels exacerbated risks and failures long after the initial event. The study recommended the Federal Government facilitate cross-sector partnerships in key regions to address major events, and provide data and forecasting models on climate change and severe weather events. The 2009 *Framework for Dealing with Disasters and Related Interdependencies* study similarly recommended cross-sector, public-private planning and exercises to address interdependencies.

Discussion: Numerous studies have examined cross-sector interdependencies and recommended coordinated planning and response strategies, yet multi-sector disaster response planning still largely focuses on managing impacts in the first few days. A long-duration energy disruption of months or even years could create more severe disruptions, exacerbate existing interdependency risks, and expose gaps in roles and responsibilities.

For example, the EMP from a high-altitude detonation of a nuclear weapon over the United States or a severe solar storm could both damage critical equipment (i.e., transformers) and threaten stability of the bulk power system. The most severe solar storm could take four to 10 years to recover from with a cost of up to $2 trillion.[8] A March 2016 U.S. Government Accountability Office (GAO) study concluded that the U.S. Department of Energy (DOE), DHS, and industry "have not established a coordinated approach to identifying and implementing key risk management activities to address EMP risks."[9] In response, the ESCC formed an EMP task force that will determine the vulnerability of high-voltage and electronic equipment; provide a scientific basis for investments to mitigate EMP threats; and inform response and recovery efforts.[10]

[8] Kramer, "We're shockingly unprepared for an extreme weather event that could fry Earth's power grid," 2016.
[9] U.S. Government Accountability Office (GAO), "Critical Infrastructure Protection: Federal Agencies Have Taken Actions to Address Electromagnetic Risks, but Opportunities Exist to Further Assess Risks and Strengthen Collaboration," 2016.
[10] Electricity Subsector Coordinating Council (ESCC), "ESCC Initiatives," 2017.

The potential risks to the power grid from such high-impact, low-probability events have been well studied by the North American Electric Reliability Council (NERC) and others, but successive impacts to interdependent sectors for a disruption of months to years are less clear.

A long-duration disruption to oil and natural gas delivery infrastructure could create similar issues. Aging infrastructure, disruptions to pipeline or rail delivery infrastructure, and cyberattacks could create long-term disruptions under certain conditions. As experienced during Superstorm Sandy, disruptions to oil and gas transit can have cascading effects on other lifeline sectors. In the immediate aftermath, response and recovery was delayed because first responders were tasked with navigating complex Federal, State, and local regulations to prioritize fuel transport, smaller fuel owners and operators did not have backup generation, and there was a lack of real-time information on available fuel supplies. The large geographic footprint of the industry and its importance to other sectors requires increased public-private collaboration.

While a number of risk management practices and programs have been put into place (often through NIAC recommendations) to protect against identified threats and emerging vulnerabilities, the role of cross-sector engagement has not been highly emphasized as a means for lessening the severity and occurrence of cascading impacts.

Topic 5 Port infrastructure security and resilience

America's dependence on ports means that even light physical damage to a major U.S. port can result in significant economic impacts that can cascade across national markets. A lack of sufficient maintenance and modernization for the Nation's ports creates an inability to handle larger loads from a growing economy. Ports are experiencing increased congestion, lack of modernization to port infrastructure and intermodal infrastructure, and new threats from cyber risks and terrorism. Past studies and exercises have characterized the myriad risks facing the Nation's ports and cross-sector consequences and have identified new technologies and practices to mitigate risks. Federal funding for port infrastructure, however, has decreased, and even in cases where modernization projects are approved, the process may take decades to complete. With limited funding, new investments may not appropriately prioritize resilience.

Suggested Study Charge: *Building on the 2015 Transportation Resilience Study, review current and proposed Federal funding and regulation for new/refurbished port assets and identify criteria for resilience that could be beneficially applied to federally funded infrastructure projects.*

Prior NIAC Work: The 2015 NIAC *Transportation Sector Resilience* study examined the security and resilience of freight infrastructure. A case study of the Ports of Los Angeles and Long Beach evaluated five different transportation disruption scenarios, which consisted of both natural and manmade disasters.

Discussion: With the expansion of the Panama Canal, ships are now being built larger than ever and the majority of Atlantic and Gulf ports are not naturally deep enough to accommodate these ships. Ports plan to spend almost $155 billion between 2016 and 2020 on modernization, expansion, and maintenance, but public funding is only expected to be a fraction of that investment.[11] While ports are making these investments, a commensurate investment is not being made in the infrastructure that connects to the ports, such as roads, rail, and inland waterways and navigation channels. New Federal funding for these needed freight improvements is expected to be about $11 billion during the same time period, but estimates project that the total need is about $29 billion, according to the 2017 ASCE report.[12]

Numerous studies and exercises have examined risks to port infrastructure and their implications, including studies by the GAO, the Center for Risk and Economic Analysis of Terrorism Events, and the Federal

[11] American Association of Port Authorities, "Survey Shows U.S. Ports Plan Big Investments In Capital Projects," 2016.
[12] American Society of Civil Engineers, *2017 Infrastructure Report Card: Ports,* 2017.

Maritime Commission. Investment in technologies such as radiation detection and radio-frequency identification (RFID) enabled containers would decrease security risks. The U.S. Department of Transportation (DOT) and the Federal Emergency Management Agency (FEMA) both have established grant programs to provide Federal funding for risk mitigation.

Topic 6 Workforce trends affecting critical infrastructure security and resilience

The Nation's critical infrastructure systems rely on a skilled workforce to operate them effectively and reliably. These systems are becoming more digital and automated, but the workforce responsible for these systems may not have the skills needed to protect or recover from disasters. Critical infrastructure workforce challenges are compounded by the retirement of older workers with extensive operational experience without an adequate transfer of knowledge and skills.

Suggested Study Charge: *Review the expansive body of existing recommendations (including infrastructure-related ones from the Commission on Enhancing National Cybersecurity) and identify any additional infrastructure-specific actions that are warranted.*

Prior NIAC Work: The NIAC has made more than two dozen recommendations related to workforce issues and conducted a study in 2006 focused specifically on workforce preparation and education. A number of these recommendations were fully or partially accepted for implementation by relevant Federal agencies.

Discussion: By 2030, the number of U.S. workforce retirees is projected to be more than 20 percent of the population.[13] Skilled workers with technical expertise in several areas of critical infrastructure—particularly the Energy Sector and cybersecurity—need to be replaced by a skilled workforce to meet operational needs. To usher in the next generation of workers, all industries need to increase opportunities for education, recruitment, and training.

There is already a large body of recommendations tasking the government with mitigating these risks. One thing that is not currently being addressed is the role of the Department of Education in engaging younger students to pursue future careers in infrastructure. However, the DOE, U.S. Department of Defense, Office of Personnel Management, and Office of Management and Budget all have programs for recruitment and training in place that target universities and recent graduates. Assessments of ongoing programs are required to ensure that these initiatives are actively mitigating the risks of large-scale retirement. Several sectors identified aging workforce as a risk in their 2015 *Sector-Specific Plans*, but many also highlighted steps the sectors are taking to mitigate this risk.

Topic 7 Security and resilience of oil and natural gas transit by pipeline and rail

Oil and natural gas are primarily transported through pipelines and freight rail. Pipelines, rail transit, and the oil and natural gas industry are regulated at the Federal and State level, and face risks similar to other sectors, such as aging infrastructure, extreme weather, terrorism, and cyberattacks. The July 2013 derailment and explosion of a train carrying crude oil in Quebec, Canada illustrated the severe consequences to human health and safety and to economic security if there is an incident during the transit of these fuels.[14] The large geographic footprint of the industry and its importance to other sectors requires increased public-private collaboration.

Suggested Study Charge: *Review the current status of oil and natural gas transport regulations and identify 1) factors that inhibit security and resilience outcomes and 2) specific changes to regulation that would remove barriers and promote resilience.*

[13] Ortman, Jennifer M., Victoria A. Velkoff, and Howard Hogan, "An Aging Nation: The Older Population in the United States," 2014.
[14] The Canadian Press, "Two years later: rebuilding after the Lac-Mégantic train derailment," 2015.

Prior NIAC Work: The 2015 NIAC *Transportation Sector Resilience* study examined freight rail disruptions, including the transit of crude oil. The 2013 NIAC *Strengthening Regional Resilience* study included a case study on Superstorm Sandy that examined the impact to the oil and natural gas sector. Interdependencies between the electricity and fuel sectors highlight the need for increased cross-sector communication and coordination with public emergency managers.

Discussion: The Nation relies on a widespread network of rail and pipelines to transport oil and natural gas, which are crucial fuels for homes, businesses, manufacturing, and transit. U.S. refinery receipts of domestic crude oil by rail increased more than sevenfold from 2008 to 2012, from 4 million barrels to 30 million barrels, according to a 2014 GAO report examining oil and natural gas transit.[15] Additionally, about 2.5 million miles of pipeline transport two-thirds of the Nation's natural gas, crude oil, and other materials, covering more than 200,000 miles of railroad track. The increased use of rail for transporting crude oil is due to the increases in crude oil production in North Dakota, Texas, and other states, which have exceeded the capacity of existing pipelines to move oil from production areas to refineries, according to the 2014 GAO report.[16]

Between 2014 and 2016, DOT has taken more than 30 actions to work with industry to address risks and prevent derailments, including a proposed rule in July 2016 to require railroads to develop comprehensive plans to respond to derailments and help protect communities near railroads."[17]

The Hazardous Materials Grant Program through the Pipeline and Hazardous Materials Safety Administration (PHMSA) provides emergency preparedness grants and is funded by fees collected from hazardous materials shippers and carriers.[18] While regulations and standards are in place and regulatory bodies recognize an increased need for infrastructure maintenance and improved safety, private companies shoulder the majority of improvement costs. The GAO report included a common recommendation that DOT along with the administrator of PHMSA review pipeline safety policies and further improve emergency response planning requirements.

[15] U.S. Government Accountability Office (GAO), "Oil and Gas Transportation: Department of Transportation is Taking Actions to Address Rail Safety, but Additional Actions Are Needed to Improve Pipeline Safety," 2014.
[16] Ibid.
[17] U.S. Department of Transportation (DOT), Pipeline and Hazardous Materials Safety Administration (PHMSA), "PHMSA Proposes New Safety Oil Spill Response Plans and Information Sharing for High-Hazard Flammable Trains," 2016.
[18] U.S. Department of Transportation, Pipeline and Hazardous Materials Safety Administration (PHMSA), "Hazardous Materials Grant Program," 2017.

Appendix C. Timeline of NIAC Studies

The President's National Infrastructure Advisory Council (NIAC) has conducted 27 in-depth studies since 2001 on high-priority critical infrastructure topics, resulting in 270 recommendations to reduce risk and improve security and resilience. Below is a brief summary of each study.

2016

JUL **WATER SECTOR RESILIENCE**

Examined key security and resilience issues in the Water Sector that could impact interconnected lifeline sectors, and recommended actions to highlight the criticality of water services, respond to emerging risks, and start to address the significant challenge of funding needed improvements to water and wastewater infrastructure.

2015

APR **EXECUTIVE COLLABORATION FOR THE NATION'S STRATEGIC INFRASTRUCTURE**

Recommended how to effectively engage chief executive officers (CEOs) in public-private partnerships by establishing a council of senior-executive decision--makers from the Electricity Subsector and Water, Transportation, Communications, and Financial Services Sectors.

JUL **TRANSPORTATION SECTOR RESILIENCE**

Examined the security and resilience of the Nation's complex transportation systems, which are primarily owned and operated by the private sector and State and local governments. The study identified the urgent need to provide funding and guidance to ensure the safe, secure, reliable, and efficient movement of people and goods.

2014

NOV **CRITICAL INFRASTRUCTURE SECURITY RESILIENCE NATIONAL RESEARCH AND DEVELOPMENT PLAN**

Identified cross-sector research and development priorities and recommended how public-private partnerships could facilitate national priority investments in support of the national research and development plan called for in Presidential Policy Directive 21 (PPD-21).

2013

NOV **STRENGTHENING REGIONAL RESILIENCE**

Reviewed the challenges and successes associated with achieving regional resilience, and recommended steps the Federal Government can take to help regions become more resilient.

NOV **IMPLEMENTATION OF EO 13636 AND PPD-21**

Addressed three primary aspects of Executive Order (EO) 13636 and PPD-21, including the revision of the National Infrastructure Protection Plan, the enhancement of information sharing between government and the private sector, and the development and adoption of the voluntary cybersecurity framework.

2012

JAN **INTELLIGENCE INFORMATION SHARING REPORT**

Examined all stages of the intelligence cycle—requirements generation, information collection, analysis, and dissemination—and made recommendations to advance bi-directional information sharing between critical infrastructure owners and operators and government.

2010

OCT **OPTIMIZATION OF RESOURCES FOR MITIGATING INFRASTRUCTURE DISRUPTIONS**

Provided a framework for how and where the infrastructure protection and resilience mission of the Department of Homeland Security can better support the broad national mission of community resilience.

OCT **A FRAMEWORK FOR ESTABLISHING CRITICAL INFRASTRUCTURE RESILIENCE GOALS**

Evaluated resilience practices in the Electricity Subsector and Nuclear Sector, and developed a framework that could be applied to all critical infrastructure sectors to test and improve their resilience practices.

2009

JUL **FRAMEWORK FOR DEALING WITH DISASTERS AND RELATED INTERDEPENDENCIES**

Assessed the Nation's ability to respond to and recover from major disasters that result in prolonged loss of infrastructure services expanding beyond a local area, and recommended actions to improve response and recovery.

SEP **CRITICAL INFRASTRUCTURE RESILIENCE**

Examined the steps government and industry should take to best integrate resilience and protection into a comprehensive risk-management strategy.

2008

JAN **CHEMICAL, BIOLOGICAL, AND RADIOLOGICAL EVENTS AND THE CRITICAL INFRASTRUCTURE WORKFORCE**

Examined the impact of chemical, biological, and radiological events on the critical infrastructure workforce, and recommended ways to strengthen the Nation's ability to respond to these events.

APR **THE INSIDER THREAT TO CRITICAL INFRASTRUCTURES**

Defined the insider threat for both physical and cyber realms, outlined obstacles to addressing this potential threat, and recommended near-term solutions to protect critical infrastructure from this threat.

OCT **CRITICAL INFRASTRUCTURE PARTNERSHIP STRATEGIC ASSESSMENT**

Assessed the effectiveness of the public-private partnership for critical infrastructure protection and identified opportunities to strengthen collaboration that will reduce risks to critical infrastructures.

2007

JAN **CONVERGENCE OF PHYSICAL AND CYBER TECHNOLOGIES AND RELATED SECURITY MANAGEMENT CHALLENGES**

Identified areas of potential control-systems vulnerability and recommended policy changes to enable effective public-private partnerships to improve the cybersecurity posture of these critical infrastructure systems.

JAN **THE PRIORITIZATION OF CRITICAL INFRASTRUCTURE FOR A PANDEMIC OUTBREAK IN THE UNITED STATES**

Conducted a sector-assessment survey to understand the private sector's needs and abilities during a pandemic, identified cross-sector interdependencies and how they can affect pandemic response, and recommended ways to ensure that critical infrastructure workforce receive priority during an event.

2006

APR **WORKFORCE PREPARATION, EDUCATION, AND RESEARCH**

Examined and provided recommendations on how the United States can ensure it is training the workforce needed to protect the Nation's critical infrastructure and cyber systems.

JUL **PUBLIC-PRIVATE SECTOR INTELLIGENCE COORDINATION**

Recommended policy changes to improve how the Intelligence Community coordinates with critical infrastructure owners and operators. The study brought together leaders from each of the critical infrastructure sectors and representatives from the Nation's key intelligence agencies, and highlighted the importance of CEO engagement.

2005

OCT **SECTOR PARTNERSHIP MODEL IMPLEMENTATION**

Provided advice and recommendations for the structure, function, and implementation of the Sector Partnership Model proposed in the Interim National Infrastructure Protection Plan.

OCT **RISK MANAGEMENT APPROACHES TO PROTECTION**

Identified practices of risk quantification and modeling, risk tolerance and risk acceptance, and effective and ineffective risk-management attributes.

2004

JAN **VULNERABILITY DISCLOSURE FRAMEWORK**

Provided a common understanding of and developed standard practices for disclosing and managing vulnerabilities in networked information systems.

JAN **CROSS SECTOR INTERDEPENDENCIES AND RISK ASSESSMENT GUIDANCE**

Identified interdependencies and examined how to coordinate incident management between the critical infrastructures.

APR BEST PRACTICES FOR GOVERNMENT TO ENHANCE THE SECURITY OF NATIONAL CRITICAL INFRASTRUCTURES

Presented a framework for evaluating the applicability of government intervention across and within sectors, and identified a number of best practices for government when considering intervention to encourage a more sustained and effective security posture.

JUL EVALUATION AND ENHANCEMENT OF INFORMATION SHARING AND ANALYSIS

Analyzed the current environment for information sharing and analysis across the critical infrastructure sectors and made recommendations to the government regarding enhancements, increased effectiveness, and broader influence across industries.

OCT PRIORITIZING CYBER VULNERABILITIES

Investigated the relative vulnerability of critical infrastructure sectors to cyberattack. *Hardening the Internet*, published in October 2004, provided recommendations based on findings from this report.

OCT COMMON VULNERABILITY SCORING SYSTEM

Proposed an open and universal vulnerability scoring system, with the ultimate goal of promoting a common understanding of vulnerabilities and their impact.

OCT HARDENING THE INTERNET

Provided recommendations to the Federal Government to work with industry to protect network infrastructure, computers, and devices connected to the Internet. *Prioritizing Cyber Vulnerabilities*, published in October 2004, investigates and ranks the relative vulnerability of critical infrastructure sectors.

Appendix D. Highlights from Review of Prior NIAC Recommendations

The former Designated Federal Officer (DFO) for the President's National Infrastructure Advisory Council (NIAC) analyzed Council reports and recommendations published between 2004 and 2015 and presented the findings at the September 16, 2016 NIAC Quarterly Business Meeting (QBM). This analysis served as a foundation for the Future Focus Study examination of prior studies and recommendations. Through the prior DFO's work, the Working Group was able to identify correlations between the implementation status and agencies that were assigned recommendations.

This appendix highlights some of the key findings from the former DFO's analysis, which supported the Working Group's findings. The appendix also includes a summary of additional analysis done as part of the Future Focus Study.

Agency Acceptance of NIAC Recommendations[19]

As an advisory council, the NIAC does not have the authority to enforce implementation of its recommendations. However, it can reach out to agencies to request updates on the status of implementation. By reaching out to different agencies, the former DFO was able to identify the status of the 265 recommendations made by the Council up to 2015 (the NIAC's *Water Sector Resilience* study was published in July 2016 after the analysis was completed, and included five major recommendations). The table below provides a summary of the results.

Table 1. Definition of Implementation Status

Status	Number of Recs	Percent of Recs	Definition
Fully Accepted	194	73%	Accepted for full implementation by the agencies identified to take action in recommendations
Partially Accepted	16	6%	Accepted by some of the entities identified in the recommendation
Not Accepted	16	6%	Recommendations will not be implemented by agencies for a variety of reasons
Under Review	39	15%	Assigned agencies are determining the feasibility of implementation
TOTAL	265	100%	

[19] This section provides an overview of the September 16, 2016 QBM presentation, and references information that was presented during the meeting. This information was supplemented by interviews with the former DFO.

According to the QBM presentation, the NIAC's mission has evolved over the years, leading the Council to transition to making more recommendations focused on changes in strategy and policy, which can take a longer period of time to implement. For example, some national strategies are only updated every five years, which can delay implementation. It was also reported that a number of recommendations accepted or under review were incorporated into Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (PPD-21) and Executive Order 13636: Improving Critical Infrastructure Cybersecurity (both signed in February 2013). More complex recommendations that involve multiple agencies can take longer to implement because of the need to coordinate with a number of entities. The QBM presentation also included the following observations:

NIAC Study Observations

1. NIAC advice is far-sighted
    a. The Council identified issues and risks, and proposed approaches years before they were recognized as priorities (e.g., insider threat, convergence of physical and cyber infrastructure challenges, cross-sector dependencies)
2. NIAC advice is impactful due to:
    a. High acceptance rate for implementation
    b. Extensive research conducted during studies and data is collected from a wide range of sources and perspectives
    c. Inclusiveness of participants in study development, including academia; State, local, tribal, and territorial governments; and other members of the critical infrastructure community

Characteristics of Effective Recommendations

1. Specificity of actions to take
2. Specificity of accountability (the NIAC advises the President and agency heads)
3. Understanding and incorporating required precursors as recommendations to achieve a specific identified outcome (e.g., legislation, policy, authorities, organizational structure)
4. Recognition of potential time required, and identifying milestones to measure progress

Additional Findings from the Future Focus Study

The review conducted as part of the Future Focus Study confirmed the former DFO's initial findings, and identified two additional areas:

- **Specifying an agency to implement a recommendation improved its acceptance**. Building on the prior analysis, the Future Focus Study examined the role that agency identification played in the acceptance of recommendations for implementation. It found that a little less than half of the prior recommendations named a specific agency to implement the action. Of those recommendations with a specific agency named, more than two-thirds were fully accepted for implementation. This analysis also found that later reports more consistently and frequently named specific agencies to undertake specific actions. This analysis was supported anecdotally through interviews.
- **Study recommendations included several common themes regardless of topic**. Five major themes were identified: 1) intelligence information sharing, 2) cross-sector dependencies, 3) cybersecurity, 4) executive engagement, and 5) workforce security strategies. These foundational topics continued to appear within recommendations, emphasizing their importance in critical infrastructure security and resilience.

Appendix E. Review of Intelligence Information Sharing Study

For the Future Focus Study, the Working Group examined the President's National Infrastructure Advisory Council's (NIAC) 2012 *Intelligence Information Sharing: Final Report and Recommendations* report to identify the characteristics of successful recommendations and reports, and better understand barriers to implementation. It did this by tracking actions taken to implement the recommendations through open-source research and interviews. This appendix provides an overview of the 2012 report and the actions taken to implement recommendations, and provides lessons learned that could be applied to future NIAC studies.

The 2012 report successfully drove action of key agencies by calling attention to an important topic, providing thorough analysis of the current environment, demonstrating the importance of two-way information sharing and the need for change, and naming specific agencies in recommendations.

However, the report could have been more effective if the study involved discussions with more agencies earlier in the process and in a more organized fashion, and included formal communications and action plans to guide the rollout of the report to agencies. These lessons learned will assist the NIAC with producing reports and recommendations in the future.

2012 Report Summary and Observations

Information sharing is perhaps the most important factor in the protection and resilience of critical infrastructure. [20] Information on threats to infrastructure and their likely impact underlies nearly every security decision made by owners and operators, including which assets to protect, how to make operations more resilient, how to plan for potential disasters, when to ramp up to higher levels of security, and how to respond in the immediate aftermath of a disaster.[21]

The NIAC originally studied intelligence information sharing in 2006 in its report titled *Public-Private Intelligence Coordination*. In 2010, the Administration requested the NIAC re-examine the topic. To examine the effectiveness and maturity of bi-directional information sharing between government and private-sector critical infrastructure owners and operators, the NIAC conducted 60 original interviews; analyzed different stages of the intelligence cycle across multiple sectors; conducted five in-depth case studies; and developed an extensive 228-page report that includes seven comprehensive findings and eight recommendations for the President. The report, *Intelligence Information Sharing: Final Report and Recommendations*, was published on January 10, 2012.

Overarching Observations

The 2012 study cited five overarching observations that provided the context for its detailed findings and recommendations. Below is a brief summary of the observations (More detailed information, including the findings are included in the report):

[20] NIAC, *Intelligence Information Sharing*, 2012.
[21] NIAC, *Intelligence Information Sharing*, 2012.

1. The public-private sector component of the infrastructure protection mission is not receiving the high priority that is commensurate with its vital importance to the Nation's economic health and security.
2. The unique knowledge and analysis capabilities offered by the private sector are not widely understood by government, and where they are understood, the processes to leverage these capabilities are not in place.
3. Public- and private-sector incentives for sharing information are not aligned to serve the infrastructure protection mission.
4. The Federal intelligence sharing enterprise is complex and often confusing.
5. The U.S. Department of Homeland Security (DHS) does not serve as an effective champion and leader for intelligence information-sharing interests of the private sector in the overall infrastructure protection mission within the Federal Intelligence Community and other government agencies.

2012 Report Recommendations

The overarching recommendation of the NIAC was that **the Administration should clearly and strongly assert the role and priority of critical infrastructure protection and resilience to national security, economic growth, and the well-being of its citizens**.

The NIAC's eight recommendations are briefly summarized below (more detailed recommendations can be found in the report):

Table 2. NIAC 2012 Intelligence Information Sharing Recommendations

1	**Assert the Priority of Infrastructure Protection and Resilience in National Security**—Through a Presidential Policy Directive or other policy mechanism, the White House should direct DHS and the Intelligence Community to: weigh issues of harm to critical sectors against other missions in all operations; collect infrastructure intelligence needs and evaluate terrorist targets in critical sectors; and prepare a quadrennial report on infrastructure protection intelligence sharing.
2	**Improve the Implementation and Accountability of Existing Authorities**—Improve performance and accountability and help mature DHS's role as a member of the Federal Intelligence Community.
3	**Improve Information Content by Leveraging Partner Capabilities**—DHS should work with each Sector-Specific Agency (SSA) to implement a robust intelligence requirements process.
4	**Improve the Value of Information Products to Industry Risk-Management Practices**—The Office of the Director of National Intelligence (ODNI), working jointly with DHS, should establish new intelligence dissemination product formats to create tailored and practical products that help owners and operators protect assets and improve business continuity.
5	**Build Accepted Practices for Timely Information Delivery**—All Federal mechanisms for sharing intelligence information should be examined with the goal of simplifying pathways, eliminating redundancy, and ensuring consistency of the information delivered.

6	**Capitalize on Private-Sector Capabilities for Counterterrorism Solutions**—The Federal Government should capitalize on the information collection and analysis capabilities of private-sector partners, and use this knowledge base to improve existing products and processes.
7	**Enhance Fusion Center Capabilities as One Mechanism for Sharing**—Where appropriate, DHS should guide fusion centers to establish an information-sharing function with owners and operators as part of a critical infrastructure protection and resilience mission.
8	**Develop an Action Plan to Implement Accepted Recommendations**—DHS should coordinate the preparation of an Intelligence Sharing Action Plan that describes in detail how Federal agencies plan to implement the recommendations.

Assessment of Recommendation Implementation

After its publication, the report and its recommendations drew action from the White House, U.S. Department of Energy (DOE), the Program Manager for the Information Sharing Environment (PM-ISE), the Federal Bureau of Investigation (FBI), ODNI, and offices within DHS, including the Office of Intelligence and Analysis (I&A) and the National Protection and Programs Directorate (NPPD) Office of Infrastructure Protection (IP). The following table summarizes information-sharing actions linked to the report's recommendations and aligns actions with specific recommendations. The actions taken were described in the 2013 *ISE Annual Report to Congress*, 2013 *ISE Strategic Implementation Plan for Information Sharing and Safeguarding*, agency presentations at NIAC Quarterly Business Meetings, and interviews.

Table 3. Agency Actions to Implement 2012 NIAC Recommendations

Agency	Action	Recommendations
DHS	Formed an interagency task force to examine implementation of PPD-21 and EO 13636.	1 2
	Established a working group of cross-sector representatives to assess the relevance of intelligence data and its usefulness to critical infrastructure owners and operators across multiple sectors. Following a successful pilot, DHS developed a concept of operations to implement the capability.	3 4 6
	Developed an enterprise-wide approach to efficiently make relevant fusion center analytic products available to the private sector via the Homeland Security Information Network-Critical Infrastructure (HSIN-CI) and its Critical Infrastructure Community of Interest.	3 4 6
	Developed a process to engage relevant critical infrastructure stakeholders prior to the dissemination of analytic products to private-sector partners.	3 4 6
NPPD IP	Migrated HSIN-CI to a new platform to improve private-sector partners' access to sensitive but unclassified information.	4 5
	Expanded sector access to the Suspicious Activity Reporting Tool.	4 5
ODNI	Conducted an assessment that confirmed the need to improve the provision of relevant, actionable intelligence to critical infrastructure stakeholders.	4 5

Agency	Action	Recommendations
White House	National Strategy for Information Sharing and Safeguarding specified the need to "establish information-sharing processes and sector-specific protocols with private-sector partners to improve information quality and timeliness" as a priority.	1 2
	PPD-21 established national policy on critical infrastructure security and resilience, and establishes a shared responsibility among Federal, State, local, tribal, and territorial entities as well as public and private owners and operators of critical infrastructure.	1 2
	EO 13636 directed increases in the volume, timeliness, and quality of cyber threat information shared with private-sector entities.	1 2
DHS, DOE	Sponsored a classified cyber-threat briefing for chief executive officers (CEOs) of electric utilities from across the Nation; led to a major executive-level industry initiative to identify the requirements and dedicate the necessary resources to address this sector-specific cyber threat.	3 4 6
DHS, PM-ISE	Fusion center stakeholders established a Working Group on Private-Sector Best Practices. The PM-ISE and DHS are supporting the working group's efforts to accelerate private-sector engagement capabilities of fusion centers.	7
NPPD IP, DHS I&A	Developed the Infrastructure Protection Field Resource Toolkit to enhance critical infrastructure information sharing and analytical capabilities across the National Network.	7
PM ISE	With the National Fusion Center Association, established and developed objectives for a working group on private-sector engagement.	7
DHS, FBI	Developed standard procedures for making relevant fusion center products accessible to critical infrastructure owners and operators via HSIN-CI and socialized best practices with ISE agencies.	7
ODNI	Developed decision options and doctrine that established the private sector as a partner and recipient of threat information.	2
ODNI, DHS, FBI	Identified and developed plans that incorporated a unified approach for tools that provide near real-time situational awareness of critical infrastructure vulnerabilities and interdependencies across the Intelligence Community (IC).	4 5
	Identified and documented public-private partnership best practices for Sector-Specific Agencies (SSAs).	2 3 5
	Identified and addressed gaps in training and analytic products related to emerging threats (e.g., insider threat, supply chain, and counterintelligence).	4 6
FBI	Identified FBI products that could be useful to critical infrastructure owners and operators; developed and implemented a dissemination plan.	5 6
DHS, ODNI	Facilitated sessions with SSA and Sector Coordinating Council (SCC) representatives and IC analysts to better understand threats to sectors and to identify potentially useful information for critical infrastructure sectors.	3 4

Agency	Action	Recommendations
ODNI	Set up 16 online, unclassified collaboration sites for sectors and subsectors to help SSAs to reach out to people with expertise in the IC and to provide a forum to collaborate.	4 5
N/A	Not implemented.	8

Lessons Learned for Future NIAC Studies

Through interviews, reviews of the analysis conducted by the former DFO, and open-source research, some key characteristics were identified that helped drive action following the 2012 report's release.

How the Report Supported Implementation

- **Focused on an Important and Relevant Topic**—Before the report was published, some government agencies were already examining information sharing with the private sector and considered it an important issue to analyze and understand. The report addressed a problem these agencies recognized: information sharing with the private sector was not as streamlined nor as effective as it could be. As a result, agencies were interested in the insights from the report.

- **Accurately Summarized the Current Landscape**—Agencies were able to learn from this analysis and gain a more detailed understanding of information-sharing relationships, processes, and shortcomings. This built agency trust in the report, and also helped give agencies insight into how they could address information-sharing issues.

- **Provided Specific Evidence to Demonstrate the Need for Change**—The analysis and recommendations provided agencies with a record of issues and specific examples for why information sharing should be a priority for critical infrastructure sectors. This helped agencies show why change was needed in information-sharing processes, and helped justify funding and supporting these initiatives.

- **Named Specific Agencies in Recommendations**—Naming agencies in recommendations drove change by motivating those specific agencies to act, outlining specific ways those agencies could improve information sharing.

- **Directed the White House to Institute Policy**—The first recommendation called on the White House to release policy that prioritized critical infrastructure information sharing. In turn, the White House included critical infrastructure and private-sector information-sharing initiatives in the *National Strategy for Information Sharing and Safeguarding*, Presidential Policy Directive on Critical Infrastructure Security and Resilience (PPD-21), and Executive Order on Improving Critical Infrastructure Cybersecurity (EO 13636). These policies set formal priorities for agencies, which drove information-sharing improvements that aligned with recommendations in the NIAC report.

- **Allowed Agencies to Prioritize the Issues**—The NIAC is a presidential advisory board, which brings importance to its recommendations. Agencies stated this helped them demonstrate the need for change, and also facilitated collaboration between agencies that may not have otherwise prioritized such collaboration.

Suggestions for Future Improvements

- **Involve Stakeholders Earlier and throughout the Report Process**—Involving stakeholders from key agencies and sectors earlier in the process, and in a more organized fashion would have built more buy-in for the report. This also may have prevented some misinformation. Although agencies thought the report accurately portrayed the overall information-sharing landscape, and valued the detail in the case studies, there were some minor errors in the report, such as what specific types of information one agency collects. Involving the agencies earlier and more thoroughly in the process would prevent this in the future. Collaborating with agencies earlier in the process would also help them better plan how to implement recommendations and allow for more coordination for implementation.

- **Include More Agencies**—Many agencies are involved in critical infrastructure. The NIAC should aim to include as many agencies as possible in the creation of a report and within the report itself, especially moving beyond agencies, other than DHS.

- **Have More Formal Communications and Action Plans**—Some agencies heard of the report via word of mouth, rather than being formally notified about the report's publication. Having a formal communication plan for the report would allow relevant agencies to be contacted in an organized fashion that would assist with recommendation implementation and more effectively drive change. Additionally, the report's eighth recommendation—for DHS to coordinate the preparation of an Intelligence Sharing Action Plan that describes in detail how Federal agencies plan to implement the recommendations—was never implemented. Having a formal plan of action that defines key agency roles and responsibilities after the report is published and assigns a timeline to these tasks would allow for a more organized implementation effort and for results to be more easily tracked.

Appendix F. Review of Studies on Executive Collaboration

The President's National Infrastructure Advisory Council (NIAC) recognizes the importance of chief executive officer (CEO) engagement and collaboration: based on analysis of prior recommendations, NIAC has made 41 recommendations related to senior executive or CEO engagement over 11 years and across 16 NIAC studies. As part of its Future Focus Study, the Council sought to track when CEO engagement recommendations were successfully implemented, what barriers may have existed, and ultimately why CEO engagement continues to be a theme in critical infrastructure security and resilience. To do this, the NIAC tracked CEO engagement recommendations and conducted an in-depth review of the NIAC's most recent report related to CEO engagement, *Executive Collaboration for the Nation's Strategic Infrastructure Study*, published in 2015.

The 2015 CEO Engagement Study was a unique study. For example, it was the first time that the White House requested clarification of NIAC recommendations. The study was also focused on a complicated topic that involves entities from across all levels of government, and companies and organizations of varying sizes with different expectations and needs.

Lessons Learned for Future NIAC Studies

The review of the 2015 study—coupled with tracking of other recommendations through interviews, open-source research, and analysis of prior recommendations—identified the following lessons learned:

- **A champion is crucial for driving action**. The recommendations that moved forward did so because there was an industry executive who was involved in the study process, or who was provided with the study and a clear explanation of how the recommendations would benefit them and their industry. This executive champion had the ability to facilitate collaboration between industry and government.
- **Private sector can move quicker than government**. Private-sector executives were able to take action—even when the Federal Government did not—because they saw a clear value proposition.
- **Not all CEO engagement is created equally**. Financial Services and Communications Sectors and the Electricity Subsector have many similar characteristics, which creates a common model. It is more difficult, however, to apply the same model to other sectors, such as Transportation—with nine separate modes and regionally focused systems—and Water, which is extremely localized with thousands of systems across the Nation.
- **Federal agencies lack an understanding of how executives operate**. CEOs do not participate in executive councils or other public-private partnerships unless there is a clear value proposition for them and they view participation as an effective use of their time. For example, CEOs desire short, concise meetings with clear asks and a need for decisions.
- **Key stakeholders must be engaged in a study**. Improving understanding of NIAC recommendations, the context, and the research behind them, requires engaging key stakeholders throughout a study.
- **A unifying purpose and message is key**. It is crucial to clearly and simply articulate cyber and physical threats, and identify next steps that need to be taken to help CEOs break down barriers and work together to prepare and respond to threats. Doing so presents a clear value proposition.

Example of Successful Implementation

During the course of this study, a recommendation from the NIAC's 2010 study report, *A Framework for Establishing Critical Infrastructure Resilience*, was repeatedly referenced as an example of effective implementation of a NIAC recommendation. The recommendation called on the President to "Initiate an executive-level dialogue with electricity and nuclear sector CEOs on the respective roles and responsibilities of the private and public sectors in addressing high-impact infrastructure risks and potential threats, using an established private-sector forum for high-level, trusted discussions between industry executives and government leaders."

Following the final approval and report's release, it was provided to the heads of the Edison Electric Institute (EEI) and Nuclear Energy Institute (NEI) by one of the study's co-chairs. The associations saw value in the recommendation and sent two letters of support to the President—one before and one after the Fukushima Daiichi nuclear disaster in 2011. The recommendation served as a catalyst for meetings between industry CEOs and U.S. Department of Energy Secretary Steven Chu and Homeland Security Secretary Janet Napolitano in July 2012, and eventually led to the formation of the Joint Electric Executive Committee (JEEC) in January 2013.[22] The JEEC transitioned to become the Electricity Subsector Coordinating Council (ESCC) that operates today, which is held up as a model of senior executive-level engagement.

Interviewees highlighted the combination of factors that came together to implement the recommendation, including 1) an executive-level champion, 2) value proposition for the sector, and 3) a galvanizing incident.

"It's in the moment of the highest need for collaboration that have crystallized for everybody—government executives and industry executives—the value of working together," Scott Aaronson, EEI Executive Director, told the Working Group in December 2016.

The Importance of CEO Engagement

The NIAC has repeatedly recommended the need to engage senior executives in the public and private sectors to improve critical infrastructure security and resilience. The NIAC has a unique perspective, and it understands that senior executives provide four crucial functions:

1. **Set strategic direction** by providing thought leadership and establishing desired outcomes;
2. **Set priorities** by clearly communicating what matters, and what is needed to reach desired outcomes;
3. **Apply resources,** including money, people, and executive time; and
4. **Exercise accountability** to hold people responsible for results, and adjust as needed.

CEOs have many calls on their time, which means that there must be a clear value proposition for them to participate in public-private efforts. Any engagement must also make the best use of their time, by either quickly and concisely providing executives with the information they need, or requiring a decision from them. CEOs rely on capable staff to provide them with what they need to know to make decisions.

[22] ESCC, Brochure, March 2017.

History of CEO Engagement Recommendations

The NIAC has made 41 recommendations related to CEO engagement over 11 years and 16 NIAC studies. Key recommendations include:

- Develop a voluntary executive-level information-sharing mechanism between critical infrastructure CEOs and senior intelligence officers (2006 *Public-Private Intelligence Coordination* study report, reaffirmed in 2012 *Intelligence Information Sharing* study report)
- Educate executive leaders on cyber risk to critical infrastructure control systems, and the significance of this risk to business operational safety and sustainability (2007 *Convergence of Physical and Cyber Technologies and Related Security Management Challenges* study report)
- Encourage high-level dialogues to advance the national critical infrastructure security and resilience mission through strengthened engagement with senior executive leadership in industry and government (2008 *The Insider Threat to Critical Infrastructures* study report, 2008 *Critical Infrastructure Partnership Strategic Assessment* study report)
- Collaborate with critical infrastructure owners and operators when developing resilience policies to ensure clarity of outcomes, actionable approaches, and develop relationships and practices ahead of an event (2009 *Critical Infrastructure Resilience* study report)
- Define roles and responsibilities of private and public sectors for high-impact infrastructure risks and potential threats, and implement prior NIAC recommendations for executive-level engagement (2010 *A Framework for Establishing Critical Infrastructure Resilience* study report)
- Establish partnerships and information sharing at the senior executive level to leverage combined public-private resources for large-scale, persistent threats (2012 *Intelligence Information Sharing* study report)
- Develop senior-executive partnerships within the lifeline sectors and encourage public-private cross-sector partnerships at the State and local level to strengthen regional resilience (2013 *Strengthening Regional Resilience* study report)
- Develop a summary of EO 13636 and PPD-21 targeted at CEOs to increase the understanding of the critical infrastructure security and resilience mission, and how it can benefit businesses (2013 *Implementation of EO 13636 and PPD-21* study report)

2015 Executive Collaboration for the Nation's Strategic Infrastructure

Overview

The NIAC was tasked in 2014 to provide its perspective on the benefits and challenges of engagement with CEO-level senior decision makers for public-private partnership and coordination. It was also asked to recommend a model for communicating with CEOs. A Working Group was established to respond to the tasking, and met 25 times and interviewed 19 subject-matter experts. The aim of the study was to further advance public-private partnerships by looking at cross-sector strategic concerns, encourage implementation of past NIAC recommendations, and encourage future recommendations to be developed through CEO-level engagement.

More detailed information, including the report findings and recommendations, can be found in the 2015 *Executive Collaboration for the Nation's Strategic Infrastructure* study report.

Analysis of Recommendation Implementation

The 2015 report produced seven recommendations based in two overarching categories: five recommendations provided a framework to engender CEO-level engagement, and the remaining two focused on core elements of communicating future recommendations to CEOs.

The central recommendation was the creation of a Strategic Infrastructure Executive Council (SIEC) with membership of CEOs or senior executive decision makers and their counterpart agencies in the Electricity Subsector and Water, Transportation, Communications, and Financial Services Sectors. The purpose of the council would be to identify national priorities and develop joint or coordinated action plans and agreements to implement them. The SIEC would operate under the Critical Infrastructure Partnership Advisory Council (CIPAC) and have a permanent budget line item to provide staff, analytic resources, and administrative support.

Similar to the recommendation in the 2010 study report, the private sector saw value in the NIAC's recommendation to form the senior executive council from key sectors to facilitate and accelerate the delivery of cross-sector solutions.

The ESCC highlighted as a priority for 2017 the formation of the Strategic Infrastructure Coordinating Council (SICC) with senior executives from the Electricity Subsector, and the Communications and Financial Services Sectors. The SICC would provide a way for the sectors to identify mutual priorities; develop and exercise cross-sector incident response plans and protocols; and better align systems, processes, and technologies across sectors. The SICC would "serve as a focal point for government engagement with strategic infrastructure in steady-state and during crises."[23]

At the time of the Future Focus Study, there had been no reported action at the government level. But a separate advisory council that reports directly to the Secretary of Homeland Security cited the NIAC's recommendation. In a *Cybersecurity Incident Response* report released in June 2016, the Homeland Security Advisory Council (HSAC) Cybersecurity Subcommittee cited the NIAC's recommendation to form the SIEC as a "promising option" for cross-sector coordination.[24] The HSAC report specifically highlighted the need for coordination between the Electricity Subsector and the Financial Services and Communications Sectors.

[23] ESCC, ESCC Initiatives, March 2017.

[24] HSAC, *Final Report of the Cybersecurity Subcommittee, Part I: Incident Response*, June 2016.

Appendix G. NIAC's Distinct Role Among Other Infrastructure Councils

The President's National Infrastructure Advisory Council (NIAC) found during interviews there is confusion about the roles, membership, and purpose of the many councils operating in the critical infrastructure space, indicating a need for clarity on NIAC's distinct role.

The councils are divided between partnership councils aimed at coordinating among different stakeholders, and advisory councils that provide recommendations and solutions on key topics. There are also a number of business groups with CEO membership focused on national economic security, such as the U.S. Chamber of Commerce, Business Executives for National Security, and the Business Roundtable. The work of these groups may deal with critical infrastructure security and resilience as it relates to their overall mission.

All of these bodies do important work to support critical infrastructure, but in many ways their focus is limited to the specific sector or mission. The NIAC is different in that it provides recommendations to the President on national-level critical infrastructure risks. It looks across all critical infrastructure sectors and examines high-magnitude risks that could shut down America's infrastructure, most of which is owned by the private sector and State and local governments.

The appendix provides an overview of the partnership councils that operate under the National Infrastructure Protection Plan (NIPP) and Federal advisory councils under the purview of the U.S. Department of Homeland Security (DHS).

Partnership Councils

There are a number of critical infrastructure sector partnerships that operate under the NIPP and Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience, which establish the framework for public-private partnerships to "share critical threat information, risk mitigation, and other vital information and resources."[25]

- **Sector Coordinating Councils** (SCCs) are "self-organized and self-governed councils that enable critical infrastructure owners and operators, their trade associations, and other industry representatives" focused on sector-specific strategies, policies, and activities; and facilitate collaboration with government.
- **Government Coordinating Councils** (GCCs) are the "government counterpart for each SCC to enable interagency and cross-jurisdictional coordination."
- The **Federal Senior Leadership Council** (FSLC) comprises senior officials from the designated Sector-Specific Agencies (SSAs) and other Federal departments to facilitate enhanced Federal communication and coordination.
- The **State, Local, Tribal, and Territorial Government Coordinating Council** (SLTTGCC) is a forum for cross-jurisdictional coordination for SLTT guidance, strategies, and programs.
- The **Regional Consortium Coordinating Council** (RC3) supports the coordination of existing regional groups in efforts to promote resilience activities in public and private sectors.

[25] DHS, "Critical Infrastructure Sector Partnerships" Webpage, Last updated December 30, 2016.

- **Interagency Security Committee** (ISC) members include chief security officers and other senior executives from 54 Federal agencies and departments that aims to enhance the physical security and protection of nonmilitary Federal facilities in the United States.
- **Critical Infrastructure Cross-Sector Council** members include the chairs and vice chairs of the SCC, which use the council as a forum to coordinate on cross-sector issues and interdependencies.

Federal Advisory Councils

There are a number of Federal advisory councils designed to provide expert advice and insights to Federal agencies or the President. This section is focused on the councils under the purview of DHS: the Homeland Security Advisory Council (HSAC), the National Security Telecommunications Advisory Committee (NSTAC), and NIAC.

The HSAC membership includes national leaders from emergency services; representatives from public health fields; State, local, and tribal officials; national policy makers; academics; private-sector representatives; and owners and operators of critical infrastructure. It provides advice and recommendations to the Secretary of Homeland Security on topics given priority by the Secretary. Although this can include critical infrastructure, it can also include a broader set of topics and issues.

NIAC is most similar to the NSTAC, which is a presidential advisory council that also receives support through DHS. However, the NSTAC is focused on communications issues related to national security and emergency preparedness. The table below includes key comparisons of NIAC and NSTAC, specifically scope, authorities, membership characteristics, and work products.

Table 4. Comparison of NIAC and NSTAC

	National Infrastructure Advisory Council (NIAC)	National Security Telecommunications Advisory Committee (NSTAC)
Scope	• **All critical infrastructure sectors**: The NIAC advises the President on the security and resilience of critical infrastructure sectors and their functional systems, physical assets, and cyber networks.	• **Communications Sector**: NSTAC advises the President on improving the availability and reliability of telecommunication services and national security and emergency preparedness telecommunications.
Authority	• Executive Order 13231 (established NIAC in 2001) • Derives authority from Presidential Policy Directive 21 (PPD-21) Critical Infrastructure Security and Resilience, which established national policy on critical infrastructure security and resilience and clarifies relationships across the Federal Government to advance the national unity of effort, enable efficient information exchange, and implement analysis function to	• Executive Order 12382 (established NSTAC in 1982) • Derives authority from Presidential Policy Directive 53 (PPD-53) National Security Telecommunications Policy, which established the need for a national security telecommunications policy and the need for the Nation's telecommunications to provide for responsive support for operational control of the armed forces and support for the vital functions of

	National Infrastructure Advisory Council (NIAC)	National Security Telecommunications Advisory Committee (NSTAC)
	inform planning and operational decisions for critical infrastructure. • Operates under the provisions of the Federal Advisory Committee Act (FACA)	worldwide intelligence collection and diplomatic affairs. • Operates under the provisions of the Federal Advisory Committee Act (FACA)
Operations	• U.S. Department of Homeland Security (DHS) provides administrative and financial support • Council reports to the President through the Secretary of DHS	• U.S. Department of Homeland Security (DHS) provides administrative and financial support • Council reports to the President through the Secretary of DHS
Subcommittee Creations	• The DFO has discretion over the creation of subcommittees.	• The DFO has discretion over the creation of subcommittees.
Current Membership	• No more than 30 members who are appointed by the President • The NIAC currently has 28 members (as of January 30, 2017)	• No more than 30 members who are appointed by the President • The NSTAC currently has 22 members (as of February 15, 2017)
Characteristics of Membership	• Members should be senior executive leaders with experience in critical infrastructure sectors; institutions of higher education; environmental and climate resilience; or State, local, and tribal governments. • Members also should have senior executive leadership responsibilities for the availability and reliability, including security and resilience, of critical infrastructure sectors. • Members serve as Special Government Employees who are retained to perform temporary duties without compensation.	• Members are appointed to represent elements of the information technology and telecommunications industry. • Members are ***not*** Special Government Employees. They do not receive compensation.
Examples of Work Products	• The NIAC primarily conducts in-depth studies on physical and cyber risks to the designated critical infrastructure sectors and recommends solutions that reduce risks and improve security and resilience. • Prior studies have addressed topics focused on how to:	• NSTAC produces a variety of work products, from newsletters to in-depth reports to letters on high-priority topics. • Prior work products have focused on: ○ Cloud computing security controls for national security and emergency preparedness

	National Infrastructure Advisory Council (NIAC)	National Security Telecommunications Advisory Committee (NSTAC)
	○ Improve intelligence information sharing across government and industry ○ Identify and reduce complex cyber risks, particularly for cyber-physical systems that operate critical processes ○ Better prepare and respond to disruptions that can ripple across multiple infrastructure systems and paralyze services to entire regions	○ Review of National Cybersecurity and Communications Integration Center ○ National security and emergency preparedness implications of a nationwide public safety broadband network ○ The Internet of Things ○ Big Data Analytics
Public Requirement	• NIAC meetings are open to the public unless a determination is made by the appropriate DHS official in accordance with DHS policy and directives that the meeting should be closed.	• NSTAC meetings are open to the public unless a determination is made by the appropriate DHS official in accordance with DHS policy and directives that the meeting should be closed.

Appendix H. References

Aftergood, Steven. 2013. "What's the Difference Between and Executive Order and a Directive?" *Secrecy News,* Federation of American Scientists, February 14. Accessed March 23, 2017. http://fas.org/blogs/secrecy/2013/02/eo_pd/.

American Association of Port Authorities. "Survey Shows U.S. Ports Plan Big Investments In Capital Projects." Press Release, April 6, 2017. Accessed March 23, 2017. http://www.aapa-ports.org/advocating/PRdetail.aspx?itemnumber=21209.

American Society of Civil Engineers. *2017 Infrastructure Report Card: Ports*. 2017. Accessed March 30, 2017. http://www.infrastructurereportcard.org/wp-content/uploads/2017/01/Ports-Final.pdf.

American Society of Civil Engineers. *Failure to Act: Closing the Infrastructure Investment Gap for America's Economic Future*. 2016. Accessed April 3, 2017. http://www.infrastructurereportcard.org/wp-content/uploads/2016/05/2016-FTA-Report-Close-the-Gap.pdf.

Business Executives for National Security (BENS). 2016. "About BENS." Accessed March 23, 2017. http://www.bens.org/page.aspx?pid=406.

Business Executives for National Security (BENS). 2016. "Improving the Business of National Security." Accessed March 23, 2017. http://www.bens.org/Improvingthebusinessofnationalsecurity.

Business Roundtable. 2016. "About." Accessed March 23, 2017. http://businessroundtable.org/about.

Business Roundtable. 2016. "Technology, Internet & Innovation." Accessed March 23, 2017. http://businessroundtable.org/issues/technology-internet-innovation/committee.

Bakir, Niyazi Onur. 2007. "A Brief Analysis of Threats and Vulnerabilities in the Maritime Domain." University of Southern California, Center for Risk and Economic Analysis of Terrorism Events. Non-published Research Reports, Paper 5.

Commission on Enhancing National Cybersecurity. 2016. *Report on Securing and Growing the Digital Economy*. Accessed April 20, 2017. https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf.

Congressional Research Service (CRS). *Executive Orders: Issuance, Modification, and Revocation*. 2014. Accessed March 23, 2017.

Ehlers, Torsten. 2014. *Understanding the challenges for infrastructure finance*. Working Paper No. 454. Bank for International Settlements. Accessed March 30, 2017. http://www.bis.org/publ/work454.pdf.

Electricity Subsector Coordinating Council (ESCC). Brochure. March 2017. Accessed March 20, 2017. http://www.electricitysubsector.org/ESCCBrochure.pdf?v=1.5.

Electricity Subsector Coordinating Council (ESCC). ESCC Initiatives. March 2017. Accessed April 3, 2017. http://www.electricitysubsector.org/ESCCInitiatives.pdf?v=1.6.

Executive Office of the President of the United States. 2013. *Economic Benefits of Increasing Electric Grid Resilience to Weather Outages*. Accessed April 4, 2017. https://energy.gov/sites/prod/files/2013/08/f2/Grid%20Resiliency%20Report_FINAL.pdf.

Executive Office of the President. 2016. *National Electric Grid Security and Resilience Action Plan*. Accessed April 21, 2017. https://www.whitehouse.gov/sites/whitehouse.gov/files/images/National_Electric_Grid_Action_Plan_06Dec2016.pdf.

Executive Office of the President. 2012. *National Strategy for Information and Safeguarding*. Accessed April 21, 2017. https://obamawhitehouse.archives.gov/sites/default/files/docs/2012sharingstrategy_1.pdf.

Executive Office of the President of the United States. *Standards and Finance to Support Community Resilience*. 2016. Accessed April 3, 2017. https://obamawhitehouse.archives.gov/sites/default/files/omb/reports/omb_resilience_finance_report.pdf.

Federal Emergency Management Agency. "Port Security Grant Program." Last updated 2016. Accessed March 31, 2017. https://www.fema.gov/port-security-grant-program.

Federal Maritime Commission Bureau of Trade Analysis. 2015. U.S. Container Port Congestion & Related International Supply Chain Issues: Causes, Consequences & Challenges. Accessed March 31, 2017. http://www.fmc.gov/assets/1/Page/PortForumReport_FINALwebAll.pdf.

Homeland Security Advisory Council (HSAC). *Final Report of the Cybersecurity Subcommittee, Part I: Incident Response*. June 2016. Accessed April 3, 2017. https://www.dhs.gov/sites/default/files/publications/HSAC_Cybersecurity_IR_FINAL_Report.pdf.

Kelly-Detwiler, Peter. 2014. "Failure to Protect U.S. Against Electromagnetic Pulse Threat Could Make 9/11 Look Trivial Someday." Forbes. July 31. Accessed March 30, 2017. https://www.forbes.com/sites/peterdetwiler/2014/07/31/protecting-the-u-s-against-the-electromagnetic-pulse-threat-a-continued-failure-of-leadership-could-make-911-look-trivial-someday/#14e9fb697a14.

Korte, Gregory. 2014. "Obama issues 'executive orders by another name'," *USA Today*, December 17. Accessed March 23, 2017. http://www.usatoday.com/story/news/politics/2014/12/16/obama-presidential-memoranda-executive-orders/20191805/.

Kousky, Carolyn, Erwann O. Michel-Kerjan, and Paul A Raschly. 2013. *Does Federal Disaster Assistance Crowd Out Private Demand for Insurance*? Risk Management and Decision Processes Center. The Wharton School, University of Pennsylvania. Accessed April 4, 2017. http://opim.wharton.upenn.edu/risk/library/WP2013-10_FedDisasterAssistance.pdf.

Kramer, Sarah. 2016. "We're shockingly unprepared for an extreme weather event that could fry Earth's power grid," Business Insider, April 2. Accessed April 3, 2017. http://www.businessinsider.com/solar-storm-effects-electronics-energy-grid-2016-3.

Library of Congress. 2016. "About CRS." Accessed March 23, 2017. https://www.loc.gov/crsinfo/about/.

National Council of ISACs. "About NCI." Accessed March 31, 2017. https://www.nationalisacs.org/about-nci.

National Infrastructure Advisory Council (NIAC). *A Framework for Establishing Critical Infrastructure Resilience Goals.* 2010. Accessed March 23, 2017.

https://www.dhs.gov/sites/default/files/publications/niac-framework-establishing-resilience-goals-final-report-10-19-10-508.pdf.

National Infrastructure Advisory Council (NIAC). *Best Practices for Government to Enhance the Security of National Critical Infrastructure.* 2004. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/niac-best-practices-ci-security-final-report-04-13-04-508.pdf.

National Infrastructure Advisory Council (NIAC). *Chemical, Biological, and Radiological Events and the Critical Infrastructure Workforce*. 2008. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/niac-chemical-biological-radiological-final-report-01-08-08-508.pdf.

National Infrastructure Advisory Council (NIAC). *Clarifications on Executive Collaboration for the Nation's Strategic Infrastructure: Responses to National Security Council Questions.* 2015. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/niac-ceo-report-response-nsc-final-12-01-15-508.pdf.

National Infrastructure Advisory Council (NIAC). *Common Vulnerability Scoring System*. 2004. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/niac-common-vulnerability-scoring-final-report-10-12-04-508.pdf.

National Infrastructure Advisory Council (NIAC). *Convergence of Physical and Cyber Technologies and Related Security Management Challenges*. 2007. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/niac-physical-cyber-final-report-01-16-07-508.pdf.

National Infrastructure Advisory Council (NIAC). *Critical Infrastructure Partnership Strategic Assessment*. 2008. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/niac-ci-partnership-assessment-final-report-10-14-08-508.pdf.

National Infrastructure Advisory Council (NIAC). *Critical Infrastructure Resilience.* 2009. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/niac-critical-infrastructure-resilience-final-report-09-08-09-508.pdf.

National Infrastructure Advisory Council (NIAC). *Critical Infrastructure Security Resilience National Research and Development Plan*. 2014. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/NIAC-CISR-RD-Plan-Report-Final-508.pdf.

National Infrastructure Advisory Council (NIAC). *Cross Sector Interdependencies and Risk Assessment Guidance*. 2004. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/niac-interdependencies-risk-assess-final-report-01-13-04-508.pdf.

National Infrastructure Advisory Council (NIAC). *Evaluation and Enhancement of Information Sharing and Analysis*. 2004. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/niac-eval-enhance-info-sharing-final-report-07-13-04-508.pdf.

National Infrastructure Advisory Council (NIAC). *Executive Collaboration for the Nation's Strategic Infrastructure*. 2015. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/niac-executive-collaboration-final-report-508.pdf.

National Infrastructure Advisory Council (NIAC). *Framework for Dealing with Disasters and Related Interdependencies*. 2009. Accessed March 23, 2017.

https://www.dhs.gov/sites/default/files/publications/niac-framework-dealing-disasters-final-report-07-14-09-508.pdf.

National Infrastructure Advisory Council (NIAC). *Hardening the Internet*. 2004. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/niac-hardening-internet-final-report-10-12-04-508.pdf.

National Infrastructure Advisory Council (NIAC). *Implementation of EO 13636 and PPD-21.* 2013. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/niac-eo-ppd-implem-final-report-11-21-13-508.pdf.

National Infrastructure Advisory Council (NIAC). *Intelligence Information Sharing Report*. 2012. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/niac-intel-info-sharing-final-report-01-10-12-508.pdf.

National Infrastructure Advisory Council (NIAC). "Meeting Minutes for the December 1, 2015 Quarterly Business Meeting." Accessed April 20, 2017. https://www.dhs.gov/sites/default/files/publications/niac-qbm-minutes-12-01-15-508.pdf.

National Infrastructure Advisory Council (NIAC). "Meeting Minutes for the June 12, 2014 Quarterly Business Meeting." Accessed April 20, 2017. https://www.dhs.gov/sites/default/files/publications/NIAC-QBM-Minutes-06-12-14-508.pdf.

National Infrastructure Advisory Council (NIAC). "Meeting Minutes for the June 30, 2015 Quarterly Business Meeting." Accessed April 20, 2017. https://www.dhs.gov/sites/default/files/publications/niac-qbm-minutes-06-30-15-508_0.pdf.

National Infrastructure Advisory Council (NIAC). "Meeting Minutes for the March 20, 2015 Quarterly Business Meeting." Accessed April 20, 2017. https://www.dhs.gov/sites/default/files/publications/niac-qbm-minutes-03-20-15-508.pdf.

National Infrastructure Advisory Council (NIAC). "Meeting Minutes for the November 21, 2013 Quarterly Business Meeting." Accessed April 20, 2017. https://www.dhs.gov/sites/default/files/publications/niac-qbm-minutes-11-21-13-508.pdf.

National Infrastructure Advisory Council (NIAC). "Meeting Minutes for the November 14, 2014 Quarterly Business Meeting." Accessed April 20, 2017. https://www.dhs.gov/sites/default/files/publications/niac-qbm-minutes-11-14-14-508.pdf.

National Infrastructure Advisory Council (NIAC). "Meeting Minutes for the September 5, 2014 Quarterly Business Meeting." Accessed April 20, 2017. https://www.dhs.gov/sites/default/files/publications/NIAC-QBM-Minutes-09-05-14-508.pdf.

National Infrastructure Advisory Council (NIAC). *Optimization of Resources for Mitigating Infrastructure Disruptions.* 2010. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/niac-optimization-resources-final-report-10-19-10-508.pdf.

National Infrastructure Advisory Council (NIAC). *Prioritizing Cyber Vulnerabilities*. 2004. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/niac-cyber-vulnerabilties-final-report-10-12-04-508.pdf.

National Infrastructure Advisory Council (NIAC). *Public-Private Sector Intelligence Coordination*. 2006. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/niac-intelligence-coordination-final-report-07-11-06-508.pdf.

National Infrastructure Advisory Council (NIAC). *Risk Management Approaches to Protection.* 2005. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/niac-risk-management-final-report-10-11-05-508.pdf.

National Infrastructure Advisory Council (NIAC). *Sector Partnership Model Implementation*. 2005. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/niac-sector-partnership-implem-final-report-10-11-05-508.pdf.

National Infrastructure Advisory Council (NIAC). *Strengthening Regional Resilience*. 2013. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/niac-regional-resilience-final-report-11-21-13-508.pdf.

National Infrastructure Advisory Council (NIAC). *The Insider Threat to Critical Infrastructures*. 2008. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/niac-insider-threat-final-report-04-08-08-508.pdf.

National Infrastructure Advisory Council (NIAC). *The Prioritization of Critical Infrastructure for a Pandemic Outbreak in the United States*. 2007. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/niac-pandemic-outbreak-final-report-01-17-07-508.pdf.

National Infrastructure Advisory Council (NIAC). *Transportation Sector Resilience*. 2015. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/niac-transportation-resilience-final-report-07-10-15-508.pdf.

National Infrastructure Advisory Council (NIAC). *Vulnerability Disclosure Framework.* 2004. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/niac-vulnerability-framework-final-report-01-13-04-508.pdf.

National Infrastructure Advisory Council (NIAC). *Water Sector Resilience*. 2016. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/niac-water-resilience-final-report-508.pdf.

National Infrastructure Advisory Council (NIAC). *Workforce Preparation, Education and Research*. 2006. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/niac-workforce-education-final-report-04-11-06-508.pdf.

National Infrastructure Advisory Council Bylaws. 2015. Washington, DC: National Infrastructure Advisory Council (NIAC), U.S. Department of Homeland Security (DHS).

"National Infrastructure Advisory Council Concept of Operations." 2015. Washington, DC: National Infrastructure Advisory Council, U.S. Department of Homeland Security (DHS).

"National Infrastructure Advisory Council Standard Operating Procedure Manual." 2015. Washington, DC: National Infrastructure Advisory Council, U.S. Department of Homeland Security (DHS).

National Sheriffs' Association. 2011. "Partnership for Critical Infrastructure Security." Accessed March 23, 2017. http://www.sheriffs.org/sites/default/files/uploads/documents/pcis_webinar_slides_2011-10-27.pptx.

Office of the Program Manager, Information Sharing Environment (PM-ISE). *Information Sharing Environment: Annual Report to the Congress*. June 30, 2013. https://www.ise.gov/sites/default/files/2013_ISE_Annual_Report_Final.pdf.

Office of the Program Manager, Information Sharing Environment (PM-ISE) and National Security Staff. *Strategic Implementation Plan for the National Strategy for Information Sharing and Safeguarding.* December 2013.

North American Electric Reliability Corporation. 2010. High-Impact, Low-Frequency Event Risk to the North American Bulk Power System. Accessed April 5, 2017. https://energy.gov/sites/prod/files/High-Impact%20Low-Frequency%20Event%20Risk%20to%20the%20North%20American%20Bulk%20Power%20System%20-%202010.pdf.

Ortman, Jennifer M., Victoria A. Velkoff, and Howard Hogan. "An Aging Nation: The Older Population in the United States." May 2014. U.S. Census Bureau. Accessed April 3, 2017. https://www.census.gov/prod/2014pubs/p25-1140.pdf.

The Canadian Press. 2015. "Two years later: rebuilding after the Lac-Mégantic train derailment," *Global News*, July 6. Accessed March 31, 2017. http://globalnews.ca/news/2094045/two-years-later-rebuilding-after-the-lac-megantic-train-derailment/.

The White House. 2014. "What's a Continuing Resolution and Why Does It Matter?" Accessed March 23, 2017. https://www.whitehouse.gov/blog/2014/09/19/what-s-continuing-resolution-and-why-does-it-matter.

The White House. 2016. "About OSTP." Accessed March 23, 2017. https://www.whitehouse.gov/ostp/about.

The White House. *Economic Report of the President*. 2016. Accessed April 7, 2017. https://obamawhitehouse.archives.gov/sites/default/files/docs/ERP_2016_Book_Complete%20JA.pdf.

The White House. 2016. "National Science and Technology Council." Accessed March 23, 2017. https://www.whitehouse.gov/ostp/nstc.

The White House. *Presidential Directive/NSC-53*. 1979. Accessed March 23, 2017. https://www.jimmycarterlibrary.gov/documents/pddirectives/pd53.pdf.

The White House. *Presidential Policy Directive – Critical Infrastructure Security and Resilience*. 2013. Accessed March 23, 2017. https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

U.S. Chamber of Commerce (Chamber). 2016. "About Us: Advocacy." Accessed March 23, 2017. https://www.uschamber.com/about-us/about-us-chamber/advocacy.

U.S. Chamber of Commerce (Chamber). 2016. "Infrastructure: Our Position." Accessed March 23, 2017. https://www.uschamber.com/infrastructure?tab=position#timeline.

U.S. Department of Energy Office of Electricity Delivery and Energy Reliability. "National SCADA Test Bed." Accessed March 30, 2017. https://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity/national-scada-test-bed.

U.S. Department of Energy Office of Electricity Delivery and Energy Reliability. "Recovery Act: Smart Grid Investment Grant (SGIG) Program." Accessed March 30, 2017. https://energy.gov/oe/information-center/recovery-act-smart-grid-investment-grant-sgig-program.

U.S. Department of Energy Office of Electricity Delivery and Energy Reliability. 2017. The Quadrennial Energy Review (QER), Second Installment: Transforming the Nation's Electricity System. Accessed April 3, 2017. https://energy.gov/epsa/quadrennial-energy-review-qer.

U.S. Department of Homeland Security (DHS). 2016. "Critical Infrastructure Partnership Advisory Council Sector Charters and Membership." Accessed March 23, 2017. https://www.dhs.gov/cipac-sector-charters-and-membership.

U.S. Department of Homeland Security (DHS). *Aviation Sector Coordinative Council.* 2011. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/Aviation-SCC-Charter-508.pdf.

U.S. Department of Homeland Security (DHS). *Charter of the Federal Senior Leadership Council.* 2015. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/FSLC-Charter-2015-508.pdf.

U.S. Department of Homeland Security (DHS). *Charter of the Nuclear Sector Government Coordinating Council.* 2015. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/nuclear-gcc-charter-2015-508.pdf.

U.S. Department of Homeland Security (DHS). *Charter of the Pipeline Working Group Pipeline Sector Coordinating Council Charter*. 2014. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/Pipeline-SCC-Charter-508.pdf.

U.S. Department of Homeland Security (DHS). *Charter of the Water Sector Coordinating Council*. 2014. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/Water-SCC-Charter-2014-508.pdf.

U.S. Department of Homeland Security (DHS). *Chemical Sector Coordinating Council Charter*. 2015. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/Chemical-SCC-Charter-2015-508.pdf.

U.S. Department of Homeland Security (DHS). *Chemical Sector Government Coordinating Council Charter*. 2014. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/Chemical-GCC-Charter-2014-508.pdf.

U.S. Department of Homeland Security (DHS). *CIPAC Dams Sector Coordinating Council (DSCC) Charter.* 2015. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/cipac-dams-scc-charter-2015-508.pdf.

U.S. Department of Homeland Security (DHS). *Commercial Facilities Government Coordinating Council Charter*. 2015. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/Commercial-Facilities-GCC-Charter-signed-2015-508.pdf.

U.S. Department of Homeland Security (DHS). *Commercial Facilities Sector Coordinating Council Charter*. 2015. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/Commercial-Facilities-SCC-Charter-2015-508.pdf.

U.S. Department of Homeland Security (DHS). *Communications Government Coordinating Council Charter*. 2013. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/cipac-comms-gcc-charter-508.pdf.

U.S. Department of Homeland Security (DHS). "Critical Infrastructure Sector Partnerships" Webpage. Last updated December 30, 2016. Accessed April 6, 2017. https://www.dhs.gov/critical-infrastructure-sector-partnerships.

U.S. Department of Homeland Security (DHS). *Critical Infrastructure Threat Information Sharing Framework: A Reference Guide for the Critical Infrastructure Community*. 2016. Accessed April 4, 2017. https://www.dhs.gov/sites/default/files/publications/ci-threat-information-sharing-framework-508.pdf.

U.S. Department of Homeland Security (DHS). *Critical Manufacturing Sector Government Coordinating Council Charter*. 2015. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/Critical-Manufacturing-GCC-Charter-03-15-508.pdf.

U.S. Department of Homeland Security (DHS). *Critical Manufacturing Sector Coordinating Council Charter.* 2015. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/Critical-Manufacturing-SCC-Charter-2015-508.pdf.

U.S. Department of Homeland Security (DHS). *Dams Sector Government Coordinating Council Charter*. 2015. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/Dams-GCC-Charter-March-2015-508.pdf.

U.S. Department of Homeland Security (DHS). *Defense Industrial Base Sector Coordinating Council Charter.* 2006. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/DIB-SCC-Charter-2006-508.pdf.

U.S. Department of Homeland Security (DHS). *Electricity Sub-Sector Coordinating Council Charter.* 2013. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/Energy-Electricity-SCC-Charter-2013-508.pdf.

U.S. Department of Homeland Security (DHS). *Emergency Service Sector Coordinating Council (ESSCC) Organizational and Governance Structure July 2008.* 2008. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/ES-SCC-Charter-2008-508.pdf.

U.S. Department of Homeland Security (DHS). *Emergency Services Sector Government Coordinating Council Charter.* 2015. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/ES-GCC-Charter-signed-508.pdf.

U.S. Department of Homeland Security (DHS). *Energy Sector Government Coordinating Council Charter.* 2014. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/Energy-GCC-Charter-2014-508.pdf.

U.S. Department of Homeland Security (DHS). *Executive Order 12382—President's National Security Telecommunications Advisory Committee.* 1982. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/Executive%20Order%2012382_0.pdf.

U.S. Department of Homeland Security (DHS). *Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security.* 2015. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/FSSCC-Charter-03-15-508.pdf.

U.S. Department of Homeland Security (DHS). *Food and Agriculture Sector Government Coordinating Council Charter.* 2014. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/FAGCC-Council-Charter-508.pdf.

U.S. Department of Homeland Security (DHS). *Food and Agriculture Sector Coordinating Council Governance Principles and Operating Procedures.* 2004. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/FASCC-Governance-Document-508.pdf.

U.S. Department of Homeland Security (DHS). *Government Facilities Government Coordinating Council Charter.* 2015. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/cipac-govt-facilities-gcc-charter-2015-508.pdf.

U.S. Department of Homeland Security (DHS). *Healthcare and Public Health Sector Government Coordinating Council Charter*. 2016. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/hph-gcc-charter-2016-508.pdf.

U.S. Department of Homeland Security (DHS). *Healthcare and Public Health Sector Coordinating Council Comprehensive Charter*. 2014. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/Healthcare-SCC-Charter-2014-508.pdf.

U.S. Department of Homeland Security (DHS). *Highway and Motor Carrier Sector Coordinating Council Operating Charter.* 2014. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/Highway-Motor-Carrier-SCC-Charter-508.pdf.

U.S. Department of Homeland Security (DHS). *Homeland Security Advisory Council Charter*. 2017. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/HSAC%20Charter%209MAR2017%20final.pdf.

U.S. Department of Homeland Security (DHS). 2017. "Information Sharing: A Vital Resource for Critical Infrastructure Security." Accessed April 3. https://www.dhs.gov/information-sharing-vital-resource.

U.S. Department of Homeland Security (DHS). *Information Technology Government Coordinating Council Charter.* 2015. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/IT-GCC-Charter-2015-508.pdf.

U.S. Department of Homeland Security (DHS). *National Infrastructure Advisory Council Charter*. 2015. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/niac-charter-2015-508.pdf.

U.S. Department of Homeland Security (DHS). *Nuclear Sector Coordinating Council Charter.* 2008. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/CIPAC-Nuclear-SCC-Charter-508.pdf.

U.S. Department of Homeland Security (DHS). *Oil and Natural Gas Sector Coordinating Council.* 2016. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/energy-ong-scc-charter-2016-508.pdf.

U.S. Department of Homeland Security (DHS). *Operating Charter of the Communications Sector Coordinating Council.* 2012. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/cipac-comms-scc-charter-508.pdf.

U.S. Department of Homeland Security (DHS). *Operating Charter of the Information Technology Sector Coordinating Council*. 2006. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/IT-SCC-Operating-Charter-2006-508.pdf.

U.S. Department of Homeland Security (DHS). *President's National Security Telecommunications Advisory Committee Charter.* 2015. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/NSTAC%20Charter%20Renewal_CMOts_filed%203NOV2015.pdf.

U.S. Department of Homeland Security (DHS). *President's Working Group on Financial Markets' Sponsorship of the Financial and Banking Information Infrastructure Committee.* 2003. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/Financial-Banking-Charter-2003-508.pdf.

U.S. Department of Homeland Security (DHS). "2015 Sector-Specific Plans." Accessed March 29, 2017. https://www.dhs.gov/2015-sector-specific-plans.

U.S. Department of Homeland Security (DHS). *State, Local, Tribal and Territorial Government Coordinating Council Charter.* 2014. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/SLTTGCC-Charter-508.pdf.

U.S. Department of Homeland Security (DHS). *The Defense Industrial Base (DIB) Government Coordinating Council (GCC) Charter.* 2006. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/DIB-GCC-Charter-2006-508.pdf.

U.S. Department of Homeland Security (DHS). *The Defense Industrial Base (DIB) Government Coordinating Council (GCC) Charter.* 2006. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/DIB-GCC-Charter-2006-508.pdf.

U.S. Department of Homeland Security (DHS). *Transportation Sector Government Coordinating Council Charter.* 2014. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/Transportation-GCC-Charter-2014-508.pdf.

U.S. Department of Homeland Security (DHS). *Water Sector Government Coordinating Council Charter November 2014*. 2014. Accessed March 23, 2017. https://www.dhs.gov/sites/default/files/publications/Water-GCC-Charter-2014-508.pdf.

U.S. Department of Homeland Security (DHS). *Executive Order 13231: Critical Infrastructure Protection in the Information Age.* 2001. Accessed March 23, 2017. https://www.dhs.gov/xlibrary/assets/executive-order-13231-dated-2001-10-16-initial.pdf.

U.S. Department of Transportation Maritime Administration. "TIGER Grants." Accessed April 3, 2017. https://www.marad.dot.gov/ports/office-of-port-infrastructure-development-and-congestion-mitigation/tiger-grants/.

U.S. Department of Transportation Pipeline and Hazardous Materials Safety Administration (PHMSA). "Gas Transmission and Hazardous Liquid Pipelines in the United States." Accessed March 26, 2017.

https://www.phmsa.dot.gov/staticfiles/PHMSA/ImageCollections/Images/Public_NPMSMap_A_noFOUO_pipelines_only.jpg.

U.S. Department of Transportation Pipeline and Hazardous Materials Safety Administration (PHMSA). 2017. "Hazardous Materials Grant Program." Accessed March 31. https://www.phmsa.dot.gov/hazmat/grants.

U.S. Department of Transportation Pipeline and Hazardous Materials Safety Administration (PHMSA). "PHMSA Proposes New Safety Oil Spill Response Plans and Information Sharing for High-Hazard Flammable Trains," Press Release, July 13, 2016. https://www.phmsa.dot.gov/hazmat/phmsa-proposes-new-safety-oil-spill-response-plans-and-information-sharing-for-high-hazard-flammable-trains.

U.S. Department of Treasury Office of Economic Policy. *Expanding Our Nation's Infrastructure through Innovative Financing*. September 2014. Accessed March 23, 2017. https://www.treasury.gov/resource-center/economic-policy/Documents/3_Expanding%20our%20Nation's%20Infrastructure%20through%20Innovative%20Financing.pdf.

U.S. Department of the Treasury (U.S. Treasury). 2016. "Mission, Vision, and Values." Accessed March 23, 2017. https://www.fiscal.treasury.gov/fsabout/fs_mvv.htm.

U.S. Government Accountability Office (GAO). "Critical Infrastructure Protection: Federal Agencies Have Taken Actions to Address Electromagnetic Risks, but Opportunities Exist to Further Assess Risks and Strengthen Collaboration." 2016. Accessed April 4, 2017. https://www.gao.gov/assets/680/676030.pdf.

U.S. Government Accountability Office (GAO). "Critical Infrastructure Protection: DHS Has Made Progress in Enhancing Critical Infrastructure Assessments, but Additional Improvements are Needed." Testimony before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Committee on Homeland Security, House of Representatives. 2016. Accessed April 6, 2017. http://www.gao.gov/assets/680/678344.pdf.

U.S. Government Accountability Office (GAO). "Oil and Gas Transportation: Department of Transportation is Taking Actions to Address Rail Safety, but Additional Actions Are Needed to Improve Pipeline Safety." August 2014. Accessed April 3, 2017. http://www.gao.gov/assets/670/665404.pdf.

U.S. Government Publishing Office. *How Our Laws Are Made*. 2007. Accessed March 23, 2017. https://www.gpo.gov/fdsys/pkg/CDOC-110hdoc49/pdf/CDOC-110hdoc49.pdf.

Zanona, Melanie. 2017. "Trump's infrastructure plan: What we know." *The Hill*, January 13. Accessed April 3, 2017. http://thehill.com/policy/transportation/314095-trumps-infrastructure-plan-what-we-know.