December 12, 2019

The Honorable Donald J. Trump
President of the United States
The White House
1600 Pennsylvania Avenue, N.W.
Washington, DC

Dear Mr. President,

On September 5, 2019, the National Security Council tasked the President's National Infrastructure Advisory Council (NIAC) to examine how the federal government and private industry can collaborate seamlessly to confront urgent cyber risks in the most critical and highly targeted private infrastructure.

Mr. President, escalating cyber risks to America's critical infrastructures present an existential threat to continuity of government, economic stability, social order, and national security. U.S. companies find themselves on the front lines of a cyber war they are ill-equipped to win against nation-states intent on disrupting or destroying our critical infrastructure. **Bold action is needed to prevent the dire consequences of a catastrophic cyber attack on energy, communication, and financial infrastructures.**

The nation is not sufficiently organized to counter the aggressive tactics used by our adversaries to infiltrate, map, deny, disrupt, and destroy sensitive cyber systems in the private sector. To fix this, the Council recommends the following actions:

Make Cyber Intelligence Actionable

1. Establish the Critical Infrastructure Command Center (CICC) to improve the real-time sharing and processing of private and public data—including classified information—between co-located government intelligence analysts and cyber experts with clearances from companies and functions at greatest risk (Section 9(a), E.O. 13800). The CICC will foster the trust and collaboration essential to develop the actionable intelligence and threat mitigations needed to counter rapidly evolving threats to our nation's critical infrastructure.
2. Direct the Intelligence Community to raise the priority of collecting, detecting, identifying, disseminating, and rapidly declassifying information on efforts by nation-state and non-state actors to exploit or otherwise attack critical infrastructure in the United States. This should be a Priority 1 topic within the National Intelligence Priorities Framework as a critical part of our national security.
3. Conduct a one-day Top Secret/Sensitive Compartmented Information (TS/SCI) briefing to CEOs of identified energy, communications, and financial services companies to build a compelling case for company action to counter serious cyber threats and to facilitate operationalizing the CICC.
4. Use the upcoming National Level Exercise 2020 to pilot the CICC model by bringing together cleared private sector experts with intelligence officers and representatives from other key government agencies, such as law enforcement and sector-specific agencies, to collaboratively analyze classified threats and understand resulting consequences to critical infrastructure.

Protect Highly Critical Cyber Systems by Establishing the Federal Cybersecurity Commission

5. Issue an Executive Order to create the Federal Cybersecurity Commission (FCSC) as an independent U.S. government entity to mitigate catastrophic cyber risks to critical infrastructure that have potential

national security impacts. The Commission offers a bold new approach for the streamlining of regulatory authorities to achieve cyber mitigations in the private sector and counter extraordinary cyber threats, in consultation with an executive partnership of industry executives and government leaders.

6. Convene a symposium of select Cabinet Secretaries, regulators, Office of Management and Budget (OMB) officials, CEOs, and industry representatives to clarify the functions, roles, responsibilities, and processes of the Commission, based on the more detailed work done by the NIAC.

Modernize Legal Authorities to Improve Cyber Defense

7. Direct the Department of Justice to analyze existing legal authorities: 1) to determine the ability of government to direct the private sector to implement cyber mitigations, and 2) to identify legal barriers that prevent the private sector from implementing requested mitigations and sharing information with the government.

Secure the Supply Chain of Critical Cyber Components

8. Provide liability protection to allow blacklisting and whitelisting of critical cyber products used in private critical infrastructure, similar to the authority provided in 10 CFR Part 21 for the nuclear industry and to the Department of Energy's (DOE) enhanced procurement authority.

9. Continue and expand programs at the DOE's national laboratories and other ongoing initiatives by each sector to independently test vendor equipment for vulnerabilities and report the results to private companies.

Mr. President, America's companies are fighting a cyber war against multi-billion-dollar nation-state cyber forces that they cannot win on their own. Incremental steps are no longer sufficient; bold approaches must be taken. Your leadership is needed to provide companies with the intelligence, resources, and legal protection necessary to win this war and avoid the dire consequences of losing it. Establishing the CICC and FCSC will empower our nation to meet, engage, and thwart those who choose to target our critical infrastructure.

On behalf of our fellow NIAC members, we thank you for the opportunity to serve our country through participation in this Council. We stand ready to provide additional details and discussion about this important subject.

Michael J. Wallace
Former Vice Chairman and COO, Constellation Energy
Working Group Member

William J. Fehrman
President and CEO,
Berkshire Hathaway Energy
Working Group Member

J. Rich Baich
CISO,
AIG, Inc.
Working Group Member

Richard H. Ledgett, Jr.
Former Deputy Director,
National Security Agency
Working Group Member

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

Dr. Beverly Scott
CEO
Beverly Scott Associates, LLC
NIAC Vice Chair

Transforming the U.S. Cyber Threat Partnership

December 2019

Table of Contents

About the NIAC

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

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

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

National Security Council Tasking and Study Scope

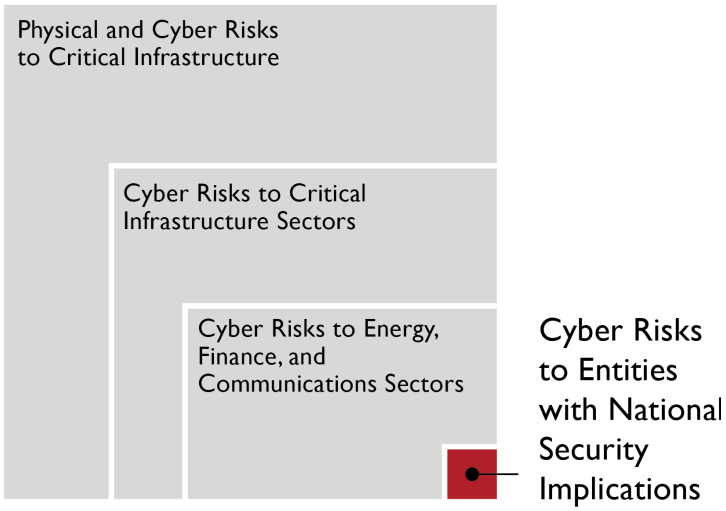
Escalating cyber risks to America's critical infrastructures present an existential threat to continuity of government, economic stability, social order, and national security. This conclusion is supported by a wealth of prior studies, including those conducted by the NIAC, the National Security Telecommunications Advisory Committee, the Commission on Enhancing National Cybersecurity, and the 2019 Worldwide Threat Assessment of the U.S. Intelligence Community. Despite the many actions taken to date, current efforts have not produced the bold steps needed to properly defend our most critical assets, causing us to fall further behind.

On September 5, 2019, the National Security Council tasked the NIAC to examine how the federal government and private industry can collaborate seamlessly to manage urgent cyber risks in the most critical and highly targeted private infrastructures. A Working Group of four NIAC members was formed to complete the task. For the purposes of this study, references to the private sector or companies encompass any infrastructure that is not federally owned and/or operated.

Given the severity of current cyber threats and the multitude of challenges in addressing them, the Working Group focused on how to protect the most at-risk entities and functions within the energy, financial services, and communications sectors (Figure 1). A disruptive cyber attack on key assets within these sectors could result in catastrophic regional or national effects on public health and safety, economic security, or national security.[1]

This fast-track effort built on the foundation of prior studies and recommendations, classified threat briefings, and the Working Group members' experiences, and did not require the extensive research conducted for other NIAC studies (see Appendix C for a list of prior studies and references). The Working Group conducted three in-person work sessions with senior government and industry leaders to gather input and insights to inform its recommendations (see Appendix B for a list of contributors). The Working Group supplemented these discussions with focused research and interviews with experts.

Figure 1. Study Scope



The study's narrow focus is not intended to conflict with or replace ongoing initiatives to improve cybersecurity in all sectors or other efforts to increase coordination and partnership between sectors and government.

[1] Executive Office of the President, "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (E.O. 13800)," May 11, 2017, https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

Compelling Case for Urgent Action

The 2019 Worldwide Threat Assessment of the U.S. Intelligence Community paints an ominous picture of cyber threats to U.S. critical infrastructure:[2]

- *China has the ability to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline for days to weeks—in the United States.*
- *Russia has the ability to execute cyber attacks in the United States that generate localized, temporary disruptive effects on critical infrastructure—such as disrupting an electrical distribution network for at least a few hours—similar to those demonstrated in Ukraine in 2015 and 2016.*
    - *Moscow is mapping our critical infrastructure with the long-term goal of being able to cause substantial damage.*
- *Iran has been preparing for cyber attacks against the United States and our allies. It is capable of causing localized, temporary disruptive effects—such as disrupting a large company's corporate networks for days to weeks—similar to its data deletion attacks against dozens of Saudi governmental and private-sector networks in late 2016 and early 2017.*

The nation risks unprecedented catastrophic failure of critical functions due to our increasing reliance on cyber systems that underpin nearly every aspect of commerce and our daily lives. Recent cyber attacks demonstrate growing capabilities for adversaries to disrupt critical infrastructure from thousands of miles away. These include the cyber attack on a nuclear plant in India in September 2019,[3] a March 2019 denial-of-service attack on wind and solar generating facilities in the United States,[4] the breach of a U.S. nuclear power plant's network in 2017,[5] the 2017 NotPetya attack that affected systems in multiple sectors throughout the world,[6] and the 2015 and 2016 cyber attacks on Ukraine's electric grid.[7]

The need to act is urgent:

1. Nation-states and other well-resourced adversaries have intensified their efforts to infiltrate and gain control of the cyber networks of key U.S. critical infrastructures (energy—specifically electricity and natural gas, financial services, and communications), which are vital for continuity of government, public safety, economic stability, and national security.

2. Private sector companies are on the front lines of a cyber war they are ill-equipped to fully understand, thwart, or counter against nation-states intent upon disrupting and destroying critical infrastructure. Protecting national security from nation-states is not a part of their operating model.

---

[2] Daniel R. Coats, "Statement for the Record, Worldwide Threat Assessment of the U.S. Intelligence Community," Before the Senate Select Committee on Intelligence, January 29, 2019, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.
[3] Debak Das, "An Indian nuclear power plant suffered a cyberattack. Here's what you need to know," *The Washington Post*, November 4, 2019, https://www.washingtonpost.com/politics/2019/11/04/an-indian-nuclear-power-plant-suffered-cyberattack-heres-what-you-need-know/.
[4] Robert Walton, "First cyberattack on solar, wind assets revealed widespread grid weaknesses, analysts say," *Utility Dive*, November 4, 2019, https://www.utilitydive.com/news/first-cyber-attack-on-solar-wind-assets-revealed-widespread-grid-weaknesse/566505/.
[5] Sonam Sheth, "Hackers breached a US nuclear power plant's network, and it could be a 'big danger,'" *Business Insider,* June 29, 2017, https://www.businessinsider.com/nuclear-power-plant-breached-cyberattack-2017-6.
[6] Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
[7] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

3. Despite massive capabilities and investment across government and the private sector, the nation has been unable to rapidly harness and direct resources to mitigate the most serious cyber threats facing these key infrastructures.

4. Executive-driven public-private partnership is the most effective way to ensure joint action and mobilize resources to implement solutions in the private sector. Existing structures have not yet been effective in addressing the most urgent and dangerous cyber risks.

5. It is not a matter of if, but when, an attack will happen. **Our window of opportunity to thwart a cyber 9-11 attack before it happens is closing quickly**.

Fundamental Principles

The NIAC's recommendations are predicated on a set of fundamental principles that affirm the shared responsibility of government and industry to protect U.S. critical infrastructure.

1. **Industry and government must partner to protect our critical infrastructure** from nation-state attacks to ensure the security and common defense of the United States. This shared responsibility requires that government help defend private infrastructure from sophisticated cyber attacks just as it defends against nuclear attacks.

2. **Priority should be placed on the most critical infrastructures that underpin national security** and other critical functions, with the ability to expand the model to defend other critical infrastructure, and then the nation writ large. The approach must be adaptable to enable cost-effective participation of small- and medium-sized enterprises, which may have limited technical or financial resources to achieve the same level of protection.

3. **The private sector cost to achieve national security objectives is beyond that required to meet normal commercial interests**. The government has a responsibility to provide appropriate channels to compensate companies for implementing extraordinary measures of cyber protection, including through federal tax relief, cost sharing, regulatory cost recovery approval, or other methods.

4. **The private sector has a responsibility to help the government understand the implications of cyber risks to company systems.** Attacks in cyberspace happen at network speed, and our processes and methods must correspond to this reality. The private sector and the government must communicate information in real time to enable them to react, respond to, and mitigate cyber threats.

5. **Making cybersecurity intelligence/information actionable allows government and industry to effectively defend the country at network speed.** This approach is not intended as a substitute or replacement of existing cybersecurity standards (e.g., National Institute of Standards and Technology Cybersecurity Framework) that improve cyber hygiene throughout critical infrastructure. Rather, it recognizes that the government must prioritize severe national cyber risks and accelerate the sharing of threat information to enable private companies to mitigate risks at machine speed.

6. **A provision to regulate industry actions must exist as a last resort to ensure necessary cyber protection against extraordinary nation-state threats.** Voluntary action, supported by incentives and market mechanisms, is the most desirable and effective way to achieve private sector cybersecurity. However, certain regulatory powers must be available to the U.S. government to protect critical national infrastructures and systems in extreme circumstances to ensure national security. In some cases, regulations may provide certain legal protections needed for commercial operations.

Urgent and Comprehensive Approach

Incremental cybersecurity improvements cannot keep pace with the rapid, asymmetric offensive strategies used by nation-states to infiltrate, map, and compromise the cyber networks of U.S. critical infrastructure. The past 20 years of well-meaning government efforts have shown that our national approach to securing the cyber assets of critical infrastructure is far less than optimal. Radical new approaches are needed that combine the extensive capabilities and resources of government and industry to protect private sector networks where failure could result in catastrophic impacts on public safety, economic stability, and national security.

New models that realign traditional public and private sector roles and responsibilities will likely require new legislation that will take time to implement—time we do not have.

The NIAC recommends a two-track approach:

1) **URGENT Action**: Pursue solutions that address urgent, near-term cyber risks that have national security implications and that can be implemented rapidly using existing authorities.
2) **COMPREHENSIVE Solution**: Design the ideal model for an assured measure of protection informed by an executive-driven public-private partnership. This approach would likely require legislation.

We recognize that bold new approaches that realign established responsibilities and programs in the federal government are hard to achieve. Building support among affected stakeholders and gaining consensus to act take time and resolve. But we must begin working toward the ideal long-term solution now. We also cannot ignore the urgent security threats that our critical infrastructure owners and operators face today. Our two-track approach ensures that we address the urgent needs of today while working toward a sustainable long-term solution.

Strategies and Recommendations

Four strategies are needed to respond to catastrophic cyber risks to the energy, communications, and financial services sectors: 1) Make Cyber Intelligence Actionable, 2) Protect Highly Critical Cyber Systems by Establishing the Federal Cybersecurity Commission, 3) Modernize Legal Authorities to Improve Cyber Defense, and 4) Secure the Supply Chain of Sensitive Cyber Components. The NIAC developed specific recommendations to achieve each of these strategies.

Make Cyber Intelligence Actionable

Company access to classified threats to company cyber infrastructure is vital for mitigating risks. However, intelligence information sharing is impeded by three key factors: 1) insufficient clearances for private sector managers, 2) limited understanding of how a cyber threat could disrupt, disable, or damage a company's enterprise, and 3) delays in translating aggressive cyber threats into actionable mitigations.

These factors limit the ability of the federal government to provide clarity on the magnitude of the risk and the steps companies must take to mitigate risks to their systems in a timely manner.

Recommendations

1. **Establish the Critical Infrastructure Command Center (CICC)** to improve the real-time sharing and processing of private and public data—including classified information—between co-located government intelligence analysts, cyber experts with clearances from companies and functions at greatest risk (Section 9(a), E.O. 13800), and key government agencies, including sector-specific agencies, law enforcement, and the intelligence community. The CICC will foster the trust and collaboration essential to develop the actionable intelligence and threat mitigations needed to counter rapidly evolving threats to our nation's critical infrastructure.
    a. Company and government intelligence and cyber experts would work side-by-side at a 24/7 watch floor to receive cyber threat information in real-time, understand implications of that threat for company systems (and more broadly national security, economic stability, and public safety), and enable company-specific and sector-wide mitigation actions.
    b. Participating companies would provide cleared personnel to staff the watch floor, including individuals with a broad understanding of company assets and experience with rapid executive decision making. Such personnel would have appropriate access to the company systems.
    c. The Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) should lead the development of the CICC in its role as the central department for sharing cybersecurity information between government and industry authorized under the Cybersecurity Information Sharing Act of 2015.
    d. In time, the bi-directional information sharing of the CICC should become multi-directional, so that what is learned in one sector flows rapidly to others.
2. **Direct the Intelligence Community to raise the priority** of collecting, detecting, identifying, disseminating, and rapidly declassifying information on efforts by nation-state and non-state actors to exploit or otherwise attack critical infrastructure in the United States. This should be a Priority 1 topic within the National Intelligence Priorities Framework as a critical part of our national security.

3. **Conduct a one-day Top Secret/Sensitive Compartmented Information (TS/SCI) briefing to CEOs** of identified energy, communications, and financial services companies to build a compelling case for company action to counter serious cyber threats and to facilitate operationalizing the CICC.
    a. The briefing is intended only for the companies identified to be part of the CICC to reinforce the need for immediate action.
4. **Use the upcoming National Level Exercise (NLE) 2020 to pilot the CICC model** by bringing together cleared private sector experts with intelligence officers and representatives from other key government agencies, such as law enforcement and sector-specific agencies, to collaboratively analyze classified threats and understand resulting consequences to critical infrastructure.
    a. The NLE is based on real-world incidents and brings together thousands of individuals from across all levels of government and the private sector. The NLE would be an opportunity for the agencies most directly involved in the CICC—DHS, Department of Energy (DOE), Department of the Treasury, Department of Defense (DOD), and Federal Communications Commission (FCC)—to identify how the model could be used to identify and mitigate cyber risks for the most at-risk entities and functions identified.

Protect Highly Critical Cyber Systems by Establishing the Federal Cybersecurity Commission

There is a growing recognition that government institutions have not been organized and optimized to help address cybersecurity threats from nation-state adversaries (and those that act like them) who are intent on disrupting or destroying private critical infrastructure. As a result, it is often unclear where private sector owners and operators should turn to obtain information and assistance from the government in addressing and responding to urgent cyber threats.

The Council believes that the severity and speed of international cyber threats demand a new, centralized approach that allows businesses and government to integrate real-time information, determine actions needed by both the private sector and the government, respond at network speed, and bring to bear the expertise, capabilities, and authorities of federal agencies.

Recommendations

5. **Issue an Executive Order to create the Federal Cybersecurity Commission (FCSC)** as an independent U.S. government entity to mitigate catastrophic cyber risks to critical infrastructure that have potential national security impacts. The Commission offers a bold new approach for the streamlining of regulatory authorities to achieve cyber mitigations in the private sector and counter extraordinary cyber threats, in consultation with an executive partnership of industry executives and government leaders.
    a. The FCSC would not replace existing regulatory and oversight agencies. Rather, it would serve as a bridge between the government and the identified companies in the energy, financial services, and communications sectors to help mitigate the most urgent cyber issues. For other federal agencies, the FCSC would provide cyber expertise and potentially serve as a clearinghouse for cyber-related issues in the three sectors (see Appendix A for a full description).

6. **Convene a symposium** of select Cabinet Secretaries, regulators, Office of Management and Budget (OMB) officials, CEOs, and industry representatives to clarify the functions, roles, responsibilities, and processes of the Commission, based on the work done by the NIAC.

    a. Creating a new federal entity requires in-depth discussions with invested stakeholders to ensure that the FCSC is not duplicating efforts and that it has the scope intended by the NIAC. The symposium is an opportunity to gather broader input to ensure the ultimate success of the Commission.

    b. While the creation of the FCSC could be accomplished by executive order, legislation will likely be required to provide the Commission with the authorities and funding needed to be fully operational. The President should include the FCSC in his budget submission to Congress.

Modernize Legal Authorities to Improve Cyber Defense

Many of our nation's laws and regulations could not have envisioned the way cyber systems and networks would underpin and connect our most critical infrastructure functions. In some ways, these laws and regulations have hindered proactive cybersecurity efforts by diverting company resources to comply with outdated regulations at the expense of more cutting-edge cybersecurity investments to counter emerging threats. New laws and regulations have created a patchwork of authorities that in some cases has not been applied in real-world situations.

The NIAC found in its 2017 *Securing Cyber Assets* study that the federal government has tremendous capabilities and authorities, but these are scattered across a wide swath of agencies, departments, and sub-units.[8] Private sector companies require legal clarity before they can apply resources to measures that could prevent or mitigate cyber attacks.

Recommendations

7. **Direct the Department of Justice** to analyze existing legal authorities: 1) to determine the ability of government to direct the private sector to implement cyber mitigations, and 2) to identify legal barriers that prevent the private sector from implementing requested mitigations and sharing information with the government.

    a. An initial analysis conducted by the Working Group indicates that the Defense Production Act, the Federal Power Act, and the SAFETY Act all contain provisions that could enable the government to direct cyber mitigations in critical infrastructure sectors and provide liability protections to companies that implement certain technologies. However, more guidance and interpretation from the federal government is needed to understand the extent of these powers and under what circumstances they could be used in response to nation-state cyber threats.

[8] National Infrastructure Advisory Council, *Securing Cyber Assets: Addressing Urgent Threats to Critical Infrastructure*, August 2017, https://www.dhs.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf.

Secure the Supply Chain of Critical Cyber Components

Hardware, software, and service providers rely on a complex international supply chain that at times has allowed nation-states to introduce components and malware into digital equipment used in critical infrastructures. Compromised components provide adversaries with a foothold into company networks and systems that allows them to map, control, and ultimately disrupt or destroy critical functions.

Under the National Defense Authorization Act for Fiscal Year 2014, the Secretary of Energy has the authority to use classified threat information to end contracts or eliminate companies from contract competitions without providing cause if it is based on classified information.[9] To our knowledge, the DOE has yet to use this authority.

Voluntary efforts and initiatives exist today to improve supply chain security of information and communications technology. The federal government has supply chain risk management practices and standards required for federal procurement. However, voluntary standards and leveraging federal guidelines are not enough to protect the most highly targeted and at-risk companies.

Existing cyber attack reporting requirements are not supply-chain specific and do not appear to limit the liability of an entity reporting information. The ability to share information on security issues with devices and components would be a step toward helping companies shore up security within the supply chain. Current laws and regulations do not adequately support this type of information sharing between companies.

Recommendations

8. **Provide liability protection to allow blacklisting and whitelisting** of critical cyber products used in private critical infrastructure, similar to the authority provided in 10 CFR Part 21 for the nuclear industry and to the DOE's enhanced procurement authority.
9. **Continue and expand programs at the DOE's national laboratories** and other ongoing initiatives by each sector to independently test vendor equipment for vulnerabilities and report the results to private companies.
    a. A key role the federal government can play is the independent testing and validating of vendor equipment.
    b. The NIAC supports ongoing initiatives and working groups focused on supply chain, including the Information and Communications Technology (ICT) Supply Chain Risk Management Task Force, and would encourage their continuation and expansion.

[9] U.S. Government Accountability Office, "Nuclear Supply Chain: NNSA Should Notify Congress of its Recommendations to Improve the Enhanced Procurement Authority," August 8, 2019, https://www.gao.gov/assets/710/700794.pdf.

Call to Action

The White House must move swiftly to implement our two-track approach:

1) **URGENT Action:** Pursue solutions that address urgent, near-term cyber risks that have national security implications and that can be implemented rapidly.

2) **COMPREHENSIVE Solution:** Design the ideal model for an assured measure of protection informed by an executive-driven public-private partnership. This approach would likely require legislation.

The time to act is now. The President should immediately appoint a senior leader to oversee the implementation of recommendations in this report.

The NIAC stands ready to continue to support the President in this area, and will continue to follow developments closely, so as to provide timely follow-up perspectives to the President, as appropriate. Moreover, we recommend that a status update on the recommendations in this report be provided to the NIAC within three months, including the actions being taken and planned to implement these recommendations.

Escalating cyber risks to America's critical infrastructures present an existential threat to continuity of government, economic stability, social order, and national security. We need to act now.

Appendix A: Federal Cybersecurity Commission

The protection of critical infrastructure is a shared responsibility between industry and government that has grown more important as nation-states and non-state actors seek to infiltrate private sector cyber networks with the intent to disrupt and destroy them. Today, the federal government is not effectively organized to reflect this new paradigm, in which public and private partners must quickly share intelligence about cyber threats and have clear authorities and lines of communications to respond to cyber attacks at network speed. Existing gaps and overlaps in cybersecurity responsibilities among government entities and between government and the private sector create the potential for misunderstanding, miscommunication, and lapses in cyber protection, detection, and response.

Mission

The Federal Cybersecurity Commission (FCSC) is proposed as an independent U.S. government agency, overseen by Congress, dedicated to mitigating catastrophic cyber risks to the most targeted and critical private infrastructure companies, whose failure could threaten national security. A key feature of the FCSC is that it will have limited regulatory authority and will work in close collaboration with an executive-driven public-private partnership represented by senior executives from relevant industry and government entities.

Vision

The long-term vision of the FCSC will be to ensure the confidentiality, integrity, and availability of cyber systems used in private sector critical infrastructure, where failure could result in catastrophic impacts on national security, public safety, and economic stability for the United States.

Scope

The efforts of the FCSC will be narrowly focused on a small number of critically important infrastructures and assets in the private sector. The FCSC will:

- Focus on three vitally important sectors—**energy** (electricity and natural gas), **communications**, and **financial services**—which underpin the operations of other critical infrastructures and functions.
- Focus on the most at-risk entities and/or functions within these critical infrastructures that would have national security consequences if they were to fail.
- Focus on cyber threats by nation-state and non-state actors to exploit, deny, or otherwise attack these critical infrastructures to bring about consequences that threaten national security.

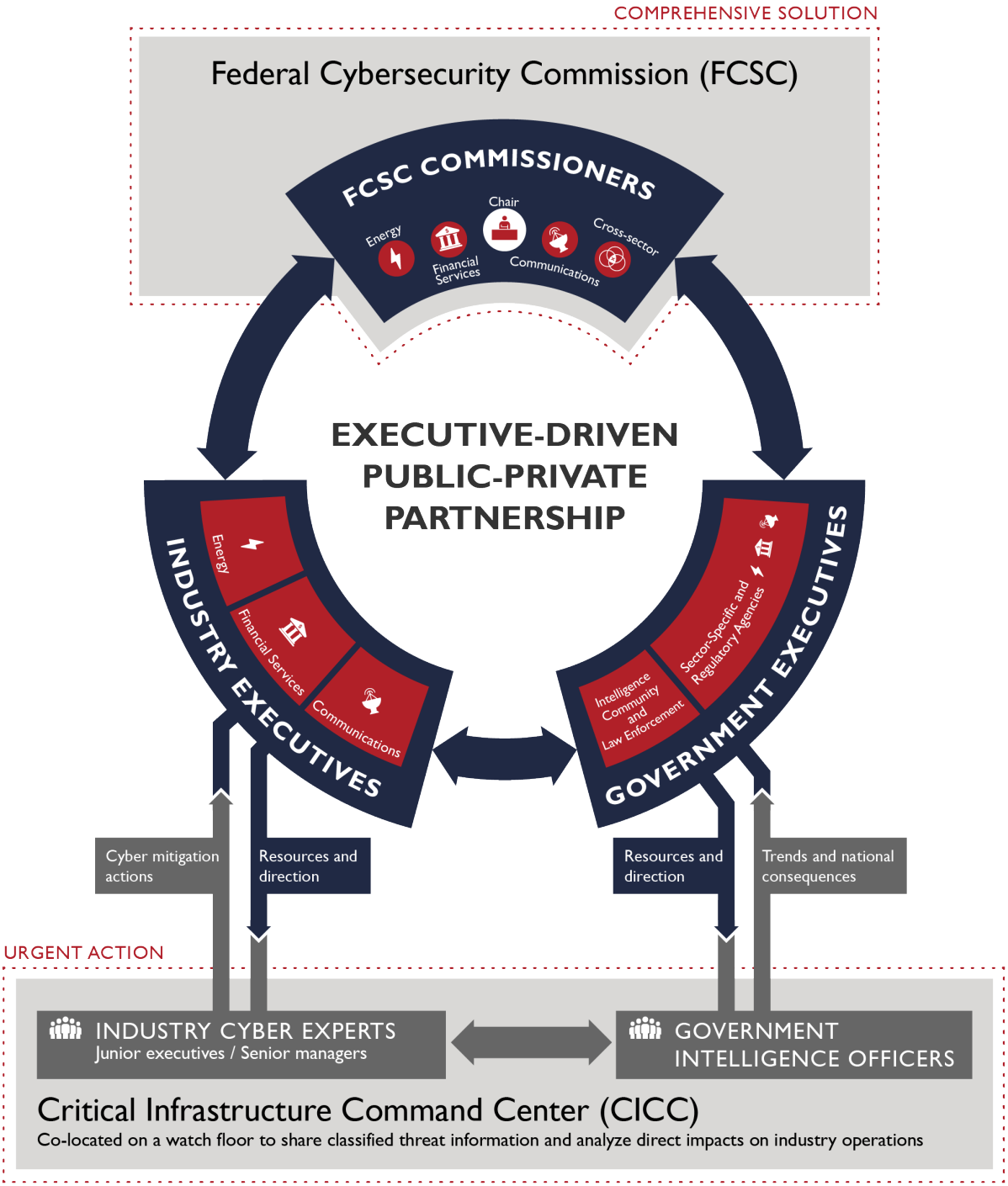
Roles

The FCSC bridges the distinct roles and responsibilities of the federal government and the private sector, which must be unified when attacks on private infrastructure equate to attacks on the nation. The FCSC provides the structure and necessary authorities to:

- Rapidly identify and direct companies to implement industry-led mitigations to counter severe cyber threats (including preventive/protective measures and response/recovery measures).
- Provide liability protection to private companies that act on mitigation measures as directed to thwart attacks.

- Accelerate intelligence sharing and analysis of nation-state threats to industry-owned systems, leveraging the CICC.
- Advise on government response to identified infrastructure threats.
- Set standards, rules, and/or regulations to ensure information technology (IT) and operational technology (OT) equipment and supply chain integrity.
- Harmonize conflicting or duplicative regulations that impede cybersecurity.
- Provide a last-resort regulatory backstop to ensure critical measures are implemented.

Figure 2. FCSC Structure



Structure and People

The FCSC will be the convener, coordinator, central clearinghouse, and regulator as a last resort for cybersecurity efforts for these most at-risk entities. To be effective, it must work collaboratively with an executive-driven public-private partnership composed of senior leaders from the three sectors and key federal agencies (Figure 2). It must also draw upon and act on intelligence and infrastructure impact information from the CICC.

Under the FCSC, private sector and government executives are expected to act collaboratively, quickly, proactively, and decisively to serious and immediate threats to critical infrastructure assets or functions to meet national security needs, while respecting the roles and responsibilities of each side of the partnership.

FCSC Commissioners

The FCSC will be led by five Commissioners: three sector-specific commissioners (energy, financial services, and communications), one cross-sector commissioner, and one chair. Commissioners will have ultimate authority over rules and actions needed to mitigate cyber risks in private sector infrastructure that have severe national security impacts. Commissioners will be appointed by the President.

Responsibilities

- Direct the expert technical and administrative staff to help assess, communicate, and implement necessary industry actions to ensure compliance with cyber mitigations in the private sector that are deemed to be essential for ensuring national security.
- Develop particularly close working relationships with key U.S. government entities, including the Intelligence Community, DOD, relevant sector agencies (e.g., DOE), law enforcement, and others in order to assure a timely and complete understanding of the threat environment.

FCSC Staff

The Staff will be headed by an Executive Director who will lead, manage, and direct the activities of a full-time legal, technical, policy, and administrative staff that executes the direction and decisions of the Commission. The staff should also include rotating detailees—experienced junior executives/senior managers drawn from both the private sector and from key government agencies—who bring sector-specific expertise or represent the cybersecurity, intelligence, and law enforcement communities. Such individuals could be detailed for a limited period of time (e.g., less than two years).

Responsibilities:

- Receive input from the CICC and from government and private sector leaders on all matters, including vulnerabilities, threats, potential impacts, risks of actions by adversaries, or risks inherent in the critical infrastructure.
- Analyze developments and risks potentially impacting the private sector infrastructure.
- Recommend policy measures, regulatory actions, and guidelines to the Commission in situations where no existing federal authorities or mechanisms exist to ensure the security of critical cyber systems.
- Carry out directions, promulgate regulations, exercise regulatory authority, and enforce actions and decisions, as directed by the Commission.

Executive-Driven Public-Private Partnership

FCSC Executives

The FCSC Commissioners will represent the perspectives of the FCSC in the executive partnership.

Private Sector Executives

Senior executives (CEO or immediately below) will represent their sector (energy, communications, or financial services) in the executive partnership.

Federal Senior Executives

Senior executives (S-1 or immediately below) will represent the departments, agencies, and regulatory bodies that have direct oversight of the affected sectors, plus principals from the Intelligence Community and law enforcement, in the executive partnership.

Leveraging the CICC to Counter Cyber Threats

While the FCSC as the ideal solution will take time to implement, the CICC can be stood up more quickly by leveraging existing authorities and with the support of the identified companies in the three sectors. As the FCSC is established, the CICC will continue to play a vital role. The steps below outline how the FCSC process could work in practice with the CICC.

1. **Major cyber threat to national security identified**: The Intelligence Community—through the collaboration in the CICC—identifies and evaluates threats to critical infrastructure. Private company experts provide valuable technical insights to federal partners regarding the implications of the threats for company operations and validate the threats for private industry. Company representatives also have access to their corporate cyber data and can provide real-time coordination and responses to federal representatives, providing a strong value proposition for both public and private partners. The CICC then produces intelligence products, in collaboration with public and private members, that are informed by private company information and technical input. Validated severe and/or urgent cyber threats to private infrastructure that, a) have the potential to impact national security, and b) are not being effectively mitigated through other means, are then presented to the Commission for potential regulatory action.
2. **Rapid assessment of cyber risk or issue**: Based on the CICC assessments, the Commission works with its staff and the CICC to make an initial determination if an action is required to address the cyber risk or compliance issue. Technical staff evaluate the potential impact and possible remedies. Policy staff review existing authorities to see if other departments or agencies can act to address the risk and determine if the mechanisms already exist to mitigate the threat (e.g., existing agencies). If not, the FCSC determines if it needs to provide directives to mitigate the threat.
3. **Consultation with Executive Public-Private Partnership**: The Commission staff brings their initial assessment to industry and government executives to obtain advice and guidance on proposed actions or remedies. The “three-party” partnership bodies engage expert staff and executives to gather analysis and recommendations for action.
4. **Commission decides on appropriate action**: The Commission makes a final determination on the needed actions to address the issue. This could result in a new rule, a referral to another agency or department with regulatory authority, or a proposed action that requires collaboration with other government entities and/or industry groups.

Core FCSC Functions

The table below describes how the FCSC would implement its core functions, and how near-term urgent actions will support FCSC implementation and be rolled into the FCSC as it is established.

Function	Urgent Action: Near-Term Recommendations	Comprehensive Solution: FCSC Implemented (Rec. 5)
Counter Severe Cyber Threats	• **Rec. 1:** Establish the Critical Infrastructure Command Center (CICC) • **Rec. 4**: Use the NLE 2020 to pilot the CICC	• Provide direction and technical resources to companies for rapid development and deployment of cyber mitigations • Exercise regulatory authority to direct private companies to take specific, enforceable mitigation actions to protect their cyber networks when threats, need for speed, or common direction are essential to meet important national security needs
Accelerate Information Sharing	• **Rec. 1**: Establish the CICC • **Rec. 2**: Prioritize detecting and identifying efforts to attack critical infrastructure • **Rec. 3**: Hold the TS/SCI briefing with the CEOs of identified companies	• Leverage the CICC to optimize bi-directional information sharing and accelerate mitigations • Identify ways to rapidly declassify information with broader sector and government implications and disseminate through existing effective channels (e.g., Information Sharing and Analysis Centers)
Ensure Supply Chain Integrity	• **Rec. 7**: Conduct a legal review of existing authorities that could be applied • **Rec. 9**: Continue and expand existing programs to independently test vendor equipment for vulnerabilities and report the results to private companies	• Set standards, rules, and/or regulations to ensure the security of equipment and services related to the IT and OT supply chain or affected companies. • Provide the regulatory authority to blacklist or whitelist components or services to mitigate severe cyber risks • **Rec. 8**: Liability protection to allow blacklisting and whitelisting of critical cyber products used in private critical infrastructure • Provide an independent evaluation of critical components using national laboratories of other resources

Function	Urgent Action: Near-Term Recommendations	Comprehensive Solution: FCSC Implemented (Rec. 5)
Provide Liability Protection	• **Rec. 7:** Conduct a legal review of existing authorities that could be applied	• Exercise existing or propose new regulatory authorities that limit the liability of private critical infrastructure companies that: ○ Share information with the government; ○ Take mitigation measures at the government's direction; or ○ Respond to the government's specific requests to take actions intended to protect, defend or restore critical cyber systems
Harmonize Regulations	• **Rec. 7**: Conduct a legal review of existing authorities that could be applied	• Serve as a cyber resource for federal agencies, provide cyber expertise and resources, and share insights into regulatory efforts • Identify conflicting and/or duplicative regulations across the federal regulatory framework and propose solutions
Share Best Practices	• **Rec. 6**: Convene a symposium (while the focus of the event will be on building out the FCSC and the path to implementation, part of the discussion will likely involve sharing experiences and knowledge)	• Coordinate with the Executive-Driven Public-Private Partnership to share best practices and mitigations used by targeted companies to increase protection and cyber hygiene across sectors

Operating Philosophy

- **The FCSC commissioners and industry and government executives will work collaboratively in the national interest**, through the "three-party" partnership, to set strategic direction, establish priorities, provide resources, and hold people accountable for results and outcomes. Moreover, the people engaged by the executives must have the authority to act on behalf of their organization, including quickly committing resources and personnel, with no (or minimal) prior approval.
- **Actions and decisions by the Commission must recognize the constraints of competitive market conditions and regulatory requirements** that critical infrastructure companies face, and they must provide solutions that enable the companies to act unimpeded by these constraints. This may include financial, regulatory, or policy remedies.
- **Bi-directional sharing of actionable classified information at the level needed is essential** and must occur with the speed and regularity needed to prompt private sector action. Focus should be on what needs to be done to mitigate the risk, rather than on sources and methods, to avoid the need for highly classified information from the TS/SCI space.
- **Prescriptive regulatory solutions to counter private sector risks should be avoided** unless: a) the private sector is not able to effectively and expeditiously act on its own; b) the government has unique technology solutions that are unavailable to the private sector to counter serious threats; or c) the government has classified information pertaining to impending nation-state threats that cannot be shared publicly. Any proposed regulatory framework should seek to establish the desired outcomes without dictating the specific solution.
- **Existing authorities, models, and capabilities should be leveraged**, where possible, to avoid duplication and accelerate practical solutions.

Appendix B. Acknowledgements

Working Group Members

J. Rich Baich, Chief Information Security Officer, AIG

William J. Fehrman, President and CEO, Berkshire Hathaway Energy

Richard H. Ledgett, Jr., Former Deputy Director, National Security Agency

Michael J. Wallace, Former Vice Chairman and COO, Constellation Energy

Working Group Support

Sam Chanoski, Director, Intelligence, Electricity Information Sharing and Analysis Center (E-ISAC), North American Electric Reliability Corporation (NERC); NIAC Point of Contact

Charles Durant, Director of National Security Policy and Resiliency Policy Adviser, Berkshire Hathaway Energy; NIAC Point of Contact

Gibson, Dunn, & Crutcher LLP, legal analysis

Work Session Participants

Mark Harvey, Senior Director, Resilience Policy, National Security Council (NSC)

Chris Krebs, Director, Cybersecurity and Infrastructure Security Agency (CISA), U.S. Department of Homeland Security (DHS)

Brian Harrell, Assistant Director, Infrastructure Security Division (ISD), CISA, DHS

Steve Harris, Deputy Assistant Director, ISD, CISA, DHS

Sue Armstrong, Associate Director, Strategy and Resources, ISD, CISA, DHS

Ed Canuel, Director, Critical Infrastructure Resilience, NSC

Sara Mroz, Director, Energy Policy, NSC

Working Group Interviewees

Keith Alexander, President and CEO, IronNet; former Commander, U.S. Cyber Command; and former Director, National Security Agency (NSA)

John C. "Chris" Inglis, Former Deputy Director, National Security Agency; Commissioner, Cyberspace Solarium Commission

Mark Montgomery, Executive Director, Cyberspace Solarium Commission

Department of Homeland Security Study Support Resources

Ginger Norris, Designated Federal Officer, NIAC

Jessica Eadie, NIAC Secretariat Support

Jim Carey, Nexight Group, LLC

Jack Eisenhauer, Nexight Group, LLC

Lindsay Kishter, Nexight Group, LLC

Beth Slaninka, Nexight Group, LLC

This study is dedicated to the tireless work of Jim Carey (November 13, 1951 – September 27, 2019), who supported the NIAC for more than a decade.

Appendix C. References

Coats, Daniel R. "Statement for the Record, Worldwide Threat Assessment of the U.S. Intelligence Community." Before the Senate Select Committee on Intelligence. January 29, 2019. https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

Commission on Enhancing National Cybersecurity (CENC). *Report on Securing and Growing the Digital Economy*. December 2016. https://www.nist.gov/system/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf.

Das, Debak. "An Indian nuclear power plant suffered a cyberattack. Here's what you need to know." *The Washington Post,* November 4, 2019. https://www.washingtonpost.com/politics/2019/11/04/an-indian-nuclear-power-plant-suffered-cyberattack-heres-what-you-need-know/.

Executive Office of the President. "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (E.O. 13800)." May 11, 2017. https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

Greenberg, Andy. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *Wired*, August 22, 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

National Infrastructure Advisory Council (NIAC). *A Framework for Establishing Critical Infrastructure Resilience Goals.* 2010. 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). *Clarifications on Executive Collaboration for the Nation's Strategic Infrastructure: Responses to National Security Council Questions.* 2015. https://www.dhs.gov/sites/default/files/publications/niac-ceo-report-response-nsc-final-12-01-15-508.pdf.

National Infrastructure Advisory Council (NIAC). *Convergence of Physical and Cyber Technologies and Related Security Management Challenges*. 2007. 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. 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 Final Report and Recommendations*. 2009. https://www.dhs.gov/sites/default/files/publications/niac-critical-infrastructure-resilience-final-report-09-08-09-508.pdf.

National Infrastructure Advisory Council (NIAC). *Cross Sector Interdependencies and Risk Assessment Guidance*. 2004. https://www.dhs.gov/sites/default/files/publications/niac-interdependencies-risk-assess-transmittal-letter-02-26-04-508.pdf.

National Infrastructure Advisory Council (NIAC). *Evaluation and Enhancement of Information Sharing and Analysis*. 2004. https://www.dhs.gov/sites/default/files/publications/niac-eval-enhance-info-sharing-transmittal-letter-08-21-04-508.pdf.

National Infrastructure Advisory Council (NIAC). *Executive Collaboration for the Nation's Strategic Infrastructure*. 2015. 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. https://www.dhs.gov/sites/default/files/publications/niac-framework-dealing-disasters-final-report-07-14-09-508.pdf.

National Infrastructure Advisory Council (NIAC). *Future Focus Study: Strengthening the NIAC Study Process*. 2017. https://www.dhs.gov/sites/default/files/publications/niac-future-focus-study-strengthening-the-niac-study-process-final-508.PDF.

National Infrastructure Advisory Council (NIAC). *Hardening the Internet*. 2004. 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. https://www.dhs.gov/sites/default/files/publications/niac-eo-ppd-implem-final-report-11-21-13-508.pdf.

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

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

National Infrastructure Advisory Council (NIAC). *Optimization of Resources for Mitigating Infrastructure Disruptions.* 2010. 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. 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. 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. 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. https://www.dhs.gov/sites/default/files/publications/niac-sector-partnership-implem-final-report-10-11-05-508.pdf.

National Infrastructure Advisory Council (NIAC). *Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure*. 2017. https://www.dhs.gov/sites/default/files/publications/niac-cyber-study-draft-report-08-15-17-508.pdf.

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

National Infrastructure Advisory Council (NIAC). *Surviving a Catastrophic Power Outage: How to Strengthen the Capabilities of the Nation*. 2018. https://www.dhs.gov/publication/niac-catastrophic-power-outage-study.

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

National Security Telecommunications Advisory Committee (NSTAC). *NSTAC Report to the President on a Cybersecurity Moonshot*. November 2018. https://www.dhs.gov/sites/default/files/publications/NSTAC_CyberMoonshotReport_508c.pdf/.

President's Commission on Critical Infrastructure Protection. *Critical Foundations: Protecting America's Infrastructures*. October 1997. https://www.hsdl.org/?abstract&did=986.

Sheth, Sonam. "Hackers breached a US nuclear power plant's network, and it could be a 'big danger.'" *Business Insider*, June 29, 2017. https://www.businessinsider.com/nuclear-power-plant-breached-cyberattack-2017-6.

U.S. Government Accountability Office. "Nuclear Supply Chain: NNSA Should Notify Congress of its Recommendations to Improve the Enhanced Procurement Authority." August 8, 2019. https://www.gao.gov/assets/710/700794.pdf.

Walton, Robert. "First cyberattack on solar, wind assets revealed widespread grid weaknesses, analysts say." *Utility Dive,* November 4, 2019. https://www.utilitydive.com/news/first-cyber-attack-on-solar-wind-assets-revealed-widespread-grid-weaknesse/566505/.

Zetter, Kim. "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." *Wired*, March 3, 2016. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.