NIAC The President's National Infrastructure Advisory Council

Securing Cyber Assets

Addressing Urgent Cyber Threats to Critical Infrastructure

August 2017

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

Executive Summary: Imperative Takeaways

Our review of hundreds of studies and interviews with 38 cyber and industry experts revealed an echo chamber, loudly reverberating what needs to be done to secure critical U.S. infrastructure against aggressive and targeted cyber attacks. Cyber is the sole arena where private companies are the front line of defense in a nation-state attack on U.S. infrastructure. When a cyber attack can deliver the same damage or consequences as a kinetic attack, it requires national leadership and close coordination of our collective resources, capabilities, and authorities.

Our Assessment

The National Security Council (NSC) tasked the President's National Infrastructure Advisory Council (NIAC) with examining how federal authorities and capabilities can best be applied to support cybersecurity of high-risk assets. We reviewed a comprehensive dataset of more than 140 federal capabilities and authorities, demonstrating impressive depth and complexity of federal resources.

We believe the U.S. government and private sector collectively have the tremendous cyber capabilities and resources needed to defend critical private systems from aggressive cyber attacks—provided they are properly organized, harnessed, and focused. Today, we are falling short.

Recommendations

The challenges the NIAC identified are well-known and reflected in study after study. There is a narrow and fleeting window of opportunity before a watershed, 9/11-level cyber attack to organize effectively and take bold action. **We call on the Administration to use this moment of foresight to take bold, decisive actions**:

1. Establish **SEPARATE, SECURE COMMUNICATIONS NETWORKS** specifically designated for the most critical cyber networks, including "dark fiber" networks for critical control system traffic and reserved spectrum for backup communications during emergencies.

   ACTION REQUIRED BY: U.S. Department of Energy (DOE), U.S. Department of Homeland Security (DHS), Office of the Director of National Intelligence (ODNI), U.S. Department of Defense (DOD), NSC, and the Strategic Infrastructure Coordinating Council (SICC) (Electricity, Financial Services, and Communications)

2. **FACILITATE A PRIVATE-SECTOR-LED PILOT OF MACHINE-TO-MACHINE INFORMATION SHARING TECHNOLOGIES**, led by the Electricity and Financial Services Sectors, to test public-private and company-to-company information sharing of cyber threats at network speed.

   ACTION REQUIRED BY: DOE, DHS, ODNI, NSC, and the SICC

3. Identify best-in-class **SCANNING TOOLS AND ASSESSMENT PRACTICES**, and work with owners and operators of the most critical networks to scan and sanitize their systems on a voluntary basis.

   ACTION REQUIRED BY: NSC and DHS

4. Strengthen the capabilities of **TODAY'S CYBER WORKFORCE** by sponsoring a public-private expert exchange program.

   ACTION REQUIRED BY: NSC, DHS, and Congress

5 Establish a set of **LIMITED TIME, OUTCOME-BASED MARKET INCENTIVES** that encourage owners and operators to upgrade cyber infrastructure, invest in state-of-the-art technologies, and meet industry standards or best practices.

ACTION REQUIRED BY: DOE, DHS, ODNI, NSC, Congress, and the SICC

6 Streamline and significantly expedite the **SECURITY CLEARANCE PROCESS** for owners of the nation's most critical cyber assets, and expedite the siting, availability, and access of Sensitive Compartmented Information Facilities (SCIFs) to ensure cleared owners and operators can access secure facilities within one hour of a major threat or incident.

ACTION REQUIRED BY: DHS, ODNI, NSC, Federal Bureau of Investigation (FBI), U.S. Office of Personnel Management (OPM), and all agencies that issue/sponsor clearances

7 Establish clear protocols to **RAPIDLY DECLASSIFY CYBER THREAT INFORMATION** and proactively share it with owners and operators of critical infrastructure, whose actions may provide the nation's front line of defense against major cyber attacks.

ACTION REQUIRED BY: NSC, DHS, ODNI, FBI, and the Intelligence Community

8 **PILOT AN OPERATIONAL TASK FORCE OF EXPERTS IN GOVERNMENT AND IN THE ELECTRICITY, FINANCE, AND COMMUNICATIONS INDUSTRIES**—led by the executives who can direct priorities and marshal resources—to take decisive action on the nation's top cyber needs with the speed and agility required by escalating cyber threats. (See explanatory chart on page 16.)

ACTION REQUIRED BY: DOE, DHS, ODNI, NSC, the SICC, DOD, U.S. Department of the Treasury (Treasury), and U.S. Department of Justice (DOJ)

9 **USE THE NATIONAL-LEVEL GRIDEX IV EXERCISE (NOVEMBER 2017) TO TEST** the detailed execution of federal authorities and capabilities during a cyber incident, and identify and assign agency-specific recommendations to coordinate and clarify the federal government's response actions where they are unclear.

ACTION REQUIRED BY: DOE, DHS, ODNI, NSC, and the SICC

10 Establish an **OPTIMUM CYBERSECURITY GOVERNANCE APPROACH** to direct and coordinate the cyber defense of the nation, aligning resources and marshaling expertise from across federal agencies.

ACTION REQUIRED BY: DHS, ODNI, NSC, DOJ, DOD, and Congress

11 Task the Homeland Security Advisor to review the recommendations included in this report and within six months **CONVENE A MEETING OF SENIOR GOVERNMENT OFFICIALS** to address barriers to implementation and identify immediate next steps to move forward.

ACTION REQUIRED BY: Homeland Security Advisor

The time to act is now. As a nation, we need to move past simply studying our cybersecurity challenges and begin taking meaningful steps to improve our cybersecurity to prevent a major debilitating cyber attack.

Our nation needs direction and leadership to dramatically reduce cyber risks. The NIAC stands ready to continue to support the President in this area.

Introduction

Today's cyber attacks are increasingly dangerous and targeted, designed by advanced actors to damage or disrupt critical U.S. infrastructure that deliver vital services—particularly electricity and financial services. Attackers can inflict damage on physical infrastructure by infiltrating the digital systems that control physical processes, damaging specialized equipment and disrupting vital services without a physical attack. As a nation-state cyber attack on U.S. infrastructure places private companies on the front line, this presents a national security challenge unlike any other. It is imperative that federal and private roles in defending these systems are aligned and mutually supportive.

The President's National Infrastructure Advisory Council (NIAC) believes that the federal government and private sector collectively have the tremendous cyber capabilities and resources needed to defend critical private systems from aggressive cyber attacks—provided they are properly organized, harnessed, and focused. Today, we are falling short. Cyber capabilities and oversight are fragmented while roles and responsibilities remain unclear. We are simply not organized to keep up with the threat.

Fortunately, we find ourselves in a pre-9/11-level cyber moment, with a narrow and fleeting window of opportunity to coordinate our resources effectively. Our recommendations call on the Administration to use this moment of foresight to take bold, decisive actions—requiring the federal government to apply its collective authorities and capabilities in concert with the private sector.

Our Task

In support of Presidential Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,* issued in May 2017, the National Security Council (NSC) tasked the NIAC to **assess how existing federal authorities and capabilities could be employed to assist and better support the cybersecurity of critical infrastructure assets that are at greatest risk of a cyber attack that could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security**. The NIAC formed a Working Group of nine members to complete this tasking.

Our Assessment

The Working Group was presented with a comprehensive dataset of more than 140 different federal capabilities and related authorities, encompassing multiple programs and stand-alone activities. While this dataset demonstrates the impressive depth of available federal capabilities, it also underscores the complexity of the federal structure and mechanisms that house these capabilities. We examined the top needs of high-risk industries today, then examined how existing federal authorities and capabilities can be best applied to address them.

We found that many outstanding federal capabilities play crucial roles in cyber defense and resilience today. However, their effectiveness is constrained in the following ways:

- Private sector knowledge of these capabilities and incentives to use them is limited.
- Access is hindered by multiple legal and administrative constraints.
- Government capabilities are scattered across a wide swath of agencies, departments, and their sub-units—a complicated labyrinth comparatively few can effectively navigate.
- Classification of essential threat information can delay and hinder coordinated response.

Recommendations and Supporting Findings

Our review of hundreds of studies and interviews with 38 cyber and industry experts revealed an echo chamber, loudly reverberating the enormity of the challenge and *what* needs to be done. (See our expert contributors in Appendix B.) **The challenges the NIAC identifies here are well-known** and reflected in study after study, including past NIAC studies, and recently in great detail by the Commission on Enhancing National Cybersecurity (CENC).

In this crowded space, the NIAC's distinct value lies in its ability to provide **insights from senior-level private sector owners and operators into *how* the government can best work with the private sector** to secure the most critical infrastructure assets. Achieving the level of coordination required to act on these recommendations will not be easy. That is why several of our recommendations involve piloting innovative solutions with the most critical sectors, where urgency is high and senior leadership are already being engaged.

We have studied the cybersecurity challenge in detail and are ready to take action. Our 11 recommendations reflect a strong consensus on what must be done next. (Appendices C and D provide additional background, and Appendix E lists references.)

Recommendation 1

Establish **SEPARATE, SECURE COMMUNICATIONS NETWORKS** specifically designated for the most critical cyber networks, including "dark fiber" networks for critical control system traffic and reserved spectrum for backup communications during emergencies.

A **Launch a pilot project to identify existing but unused/underused fiber networks** ("dark fiber") that could be used to create a dedicated communication network for critical infrastructure sectors. Demonstrate the ability for pilot organizations to operate critical control systems in isolation from public networks, making them more difficult to access.

B **Identify and dedicate a secure backup communication system to enable real-time communication during a major, cross-sector cyber attack.** This communication system may reserve a portion of the electromagnetic spectrum to separate it from any Internet or cyber-based communication network. It should enable, for example, electric utilities to communicate with utility crews working in the field to manually restore power after an attack.

ACTION REQUIRED BY: U.S. Department of Energy (DOE), U.S. Department of Homeland Security (DHS), Office of the Director of National Intelligence (ODNI), U.S. Department of Defense (DOD), National Security Council (NSC), and the Strategic Infrastructure Coordinating Council (SICC) (Electricity, Financial Services, and Communications Sectors)

Supporting Findings

- **The scale, scope, and frequency of cyber attacks on digital and physical infrastructure systems is growing rapidly.** Threats are escalating as more sophisticated and organized attackers are designing targeted attacks to damage or disrupt vital services and critical physical systems.
    - Cyber threats today are two-fold: attacks targeting information technology (IT), which includes the software and networks that underpin business functions in critical sectors like Financial Services, and attacks targeting operational technology (OT), which includes control systems designed to operate physical processes like power flows in the electric grid.
- **Industrial control systems connected to business IT systems and the Internet constitute a systemic cyber risk among critical infrastructure.** Cyber-connected OT systems improve automation and efficiency in the control of critical processes—such as generation, processing, and delivery of power, water, fuel, and chemicals—but also introduce new cyber risks.
- **Several power companies are moving their operational systems to dedicated, closed networks they own**, rather than shared lines they lease from communication providers. Isolating these networks can significantly limit access points, giving operators fewer digital gates to guard.
- **Backup networks will quickly become flooded and unreliable in a major cyber attack that disrupts primary communications (Internet, email, phone, and cell communications).** The government can dedicate spectrum for critical infrastructure communications to hasten response and recovery.

Recommendation 2

FACILITATE A PRIVATE-SECTOR-LED PILOT OF MACHINE-TO-MACHINE INFORMATION SHARING TECHNOLOGIES, led by the Electricity and Financial Services Sectors, to test public-private and company-to-company information sharing of cyber threats at network speed.

A **Use the pilot to identify and evaluate state-of-the-art technologies** and software platforms, resolve interoperability issues, address privacy concerns, and work through legal and liability barriers that hamper or limit company-to-company and government-to-company sharing today.

B **Leverage, build upon, and coordinate across existing platforms** designed for rapid public-private sharing of cyber threats and attack indicators, including:

- The Cybersecurity Risk Information Sharing Program (CRISP), operated by the Electricity Information Sharing and Analysis Center (E-ISAC), which uses classified analysis of network traffic to identify attacks.
- The Financial Services Information Sharing and Analysis Center's (FS-ISAC) machine-to-machine information sharing programs, now also used by some in the Energy Sector.
- DHS's Automated Indicator Sharing (AIS) platform, which releases attack indicators from multiple sources.

C Use lessons learned to **identify platforms, protocols, and best practices that Information Sharing and Analysis Centers (ISACs) can use** to expand the pilot to other critical sectors, and guide machine-to-machine research and development (R&D) as appropriate.

ACTION REQUIRED BY: DOE, DHS, ODNI, NSC, and the SICC

Supporting Findings:

- **The public and private sectors remain unable to move actionable information to the right people at the speed required** by cyber threats. Threat information and mitigations must move at network speed. Advances in machine-to-machine information sharing and automated mitigations show great promise.
- **Machine-to-machine information sharing technology and processes are still immature, and must grapple with significant legal, liability, technology, trust, and cost challenges.** A pilot offers the opportunity to coordinate on key issues:
  - Securely sharing real-time system data with the federal government requires significant trust regarding how the information will be protected, shared, and used. Leaked data creates significant business risks and liability protections are not court-tested.
  - Machine-to-machine sharing requires consensus on common technologies, data formats, protocols, and policies.
  - Automatically implementing mitigations can create unpredictable outcomes in operational control environments.

  - Automated indicator sharing can overwhelm operators with data, making it difficult to parse and prioritize.

- **The most effective, value-added platforms will incorporate public-private and business-to-business information exchange.**
  - The private sector has more raw, real-time network data of value, and sharing information between companies is often faster.
  - Government analysis adds value by connecting the dots across companies to reveal potential threats, add intelligence insights, understand intent, and provide warnings. Today, the time required to vet, analyze, and obtain permission to share threats creates significant delays.
  - Businesses can best lead the development of trusted solutions that meet their needs.
- **ISACs vary dramatically in effectiveness** across sectors based on their organization, industry trust and buy-in, member retention and growth, and level of resources. But ISACs serve as a critical conduit for threat information from the Intelligence Community and for company-to-company exchange. Highly functioning ISACs should be used as a model for other sectors.

Recommendation 3

Identify best-in-class **SCANNING TOOLS AND ASSESSMENT PRACTICES**, and work with owners and operators of the most critical networks to scan and sanitize their systems on a voluntary basis.

A **Develop a voluntary, cost-shared scanning and assessment program** that provides onsite tools and expertise to help organizations: 1) test their systems for malware using best-in-class tools, 2) sanitize their systems, and 3) identify government and industry tools and service providers to upgrade and maintain system security.

B **Establish a Center of Excellence to showcase best-in-class tools across government and industry** and provide a test bed environment for companies to test and evaluate new software, particularly for use by small and medium-sized companies; and recognize, use, and expand cybersecurity programs at existing educational institutions.

ACTION REQUIRED BY: NSC and DHS

Supporting Findings

- **Managers often do not fully understand the magnitude or complexity of the risks** they face, or to what extent their systems may be compromised.
    - Security researchers report that **more than 30 percent of computers worldwide likely have some malicious code or malware**, but few companies understand the extent of potential breaches.
    - As a result, many companies are not practicing basic cyber hygiene despite the availability of effective tools and practices. There is a broad lack of awareness of the federal tools available to help scan, detect, mitigate, and defend against cyber threats.
- **The owners of critical systems can range from Fortune 100 companies to small businesses, with diverse risks, resources, and cybersecurity needs.** Customizable solutions are needed, and one-size-fits-all tools are rarely effective.
    - Government tools or capabilities are often most useful to entities with lower levels of cybersecurity maturity or during widespread cyber attack.
- **Supply chain risks remain a struggle for system operators, who lack a trusted method to verify the provenance and custody of digital components** from design and manufacture to integration and use.
    - There is no way to test for embedded threats or verify the security of devices for critical OT systems. DOE, the National Labs, and DHS could work with the electricity industry and component manufacturers to develop an industry-driven method to verify and certify supply chain security for OT system devices.

Recommendation 4

Strengthen the capabilities of **TODAY'S CYBER WORKFORCE** by sponsoring a public-private expert exchange program.

A **Implement a public-private sector employee exchange program** to provide federal employees with a better understanding of the day-to-day operations of critical infrastructure and the role of cyber systems. This could help the federal government better identify and design programs, tools, and resources that can assist private sector organizations and overcome barriers to their use. For private sector employees, the program would provide a better awareness of the programs, tools, and resources available from the federal government. In addition, cross-training federal contractors who have appropriate clearances on industry control systems can also enable a stronger response to cyber attack.

B **Prioritize federal and congressional action to expand cyber workforce programs**, using the findings of the review required in EO 13800 to build a sustainable pipeline and address the expected shortfall in qualified cyber personnel.

- Congress should also consider expanding scholarship-for-service programs focused on attracting the next-generation cyber workforce.
- Sponsor clearances for students in college-level cybersecurity programs to speed access to qualified cyber personnel and encourage valuable internship programs.

ACTION REQUIRED BY: NSC, DHS, and Congress

Supporting Findings

- **The public and private sectors must compete for a limited pool of highly trained cyber experts**, creating a shortage of cybersecurity leadership and expertise**.** The shortfall of qualified cyber experts is forecasted to reach 1.8 million unfilled positions by 2022.[1]
    - The federal government's numerous cyber workforce development programs are now being reviewed under EO 13800, and near-term action on the recommendations should be a priority of the Administration. (See Appendix C for detail.)
- **Federal cyber experts have a limited understanding of unique private sector systems, which limits their ability to provide technical assistance**, particularly in response to a cyber attack. A focused effort is needed to develop both cyber expertise and operational system expertise across industry and government.

[1] Center for Cyber Safety and Education. *Global Information Security Workforce Study*. 2017.

Recommendation 5

Establish a set of **LIMITED TIME, OUTCOME-BASED MARKET INCENTIVES** that encourage owners and operators to upgrade cyber infrastructure, invest in state-of-the-art technologies, and meet industry standards or best practices.

A **Incentives could include regulatory relief** from frequent audits, reporting, and self-reports when industry standards are routinely met; a **limited-time tax credit** to incentivize security system upgrades; or **grant and investment programs** to fund upgrades or security investments without requiring a rate-based modification.

B **Require implementation of the National Institute of Standards and Technology (NIST) Cybersecurity Framework** to qualify for incentives for the most critical assets, and recognize that small and medium-sized businesses will need additional support to meet the requirements.

ACTION REQUIRED BY: DOE, DHS, ODNI, NSC, Congress, and the SICC

Supporting Findings

- **Cyber regulations are often blunt tools** that are unable to keep up with dynamic risks in an arena where attack and defense capabilities change rapidly over months and years, not decades.
    - Prescriptive requirements result in a focus on compliance rather than maintaining best-in-class security. However, many experts noted that regulations are an effective government tool to drive a minimum level of cyber hygiene.
    - Outcome-based requirements give companies the flexibility to best achieve or exceed objectives, while allowing for variations in company structure, size, and resources.
- **Outcome-based market incentives can encourage large-scale infrastructure upgrades**, directing company resources toward exceptional security rather than demonstrated compliance with minimum standards.
- **The NIST Cybersecurity Framework is viewed as a foundational document** for providing guidance and identifying the minimum best practices for cybersecurity.

Recommendation 6

Streamline and significantly expedite the **SECURITY CLEARANCE PROCESS** for owners of the nation's most critical cyber assets, and expedite the siting, availability, and access of Sensitive Compartmented Information Facilities (SCIFs) to ensure cleared owners and operators can access secure facilities within one hour of a major threat or incident.

A Direct agencies to facilitate and **prioritize Top Secret/Sensitive Compartmented Information (TS-SCI) clearances for at least two key personnel** at every organization operating the nation's most critical cyber assets (for which an attack could result in catastrophic effects to public safety, economic, or national security).

B **Improve the transfer of clearances**: require clearances sponsored by any agency to be accepted by all other agencies, and facilitate the transfer of clearance sponsorship as individuals move among agencies and to the private sector.

C **Expand the number of SCIFs** nationwide, and ensure secure information can be shared simultaneously between SCIFs maintained by different agencies.

ACTION REQUIRED BY: DHS, ODNI, NSC, Federal Bureau of Investigation (FBI), U.S. Office of Personnel Management (OPM), and all agencies that issue/sponsor clearances

Supporting Findings

- Despite dedicated private sector clearance programs, **too few of the right individuals in private companies have clearances at the right level** to receive timely cyber threat information and act on it. Critical businesses need, at minimum, two cleared individuals to respond to potential threats.
- **The federal clearance process is time-consuming, inefficient, and difficult for the private sector to navigate**. Clearances can take more than a year to process.
- **Federal agencies do not easily transfer clearances or universally reciprocate clearances issued by other agencies**. Individuals must frequently restart the lengthy clearance process.
    - Clearances appear to be position-specific and do not move with the individual. Individuals who hold a clearance with one agency and move to another role, or move from the federal government to private sector employment, often cannot transfer their clearance to the new agency that must sponsor it, and must often restart the entire clearance process from the beginning.
    - This is inefficient, duplicative, and prevents previously cleared employees from acting to improve the cybersecurity of critical companies.
- **Clearances have limited value if private sector individuals cannot rapidly access secure facilities to receive sensitive intelligence on cyber threats.** Private sector personnel may have to travel more than an hour away to access SCIFs, or even fly to DC to attend in-person briefings. A fast-moving cyber incident will not allow time to share information at this speed.

Recommendation 7

Establish clear protocols to **RAPIDLY DECLASSIFY CYBER THREAT INFORMATION** and proactively share it with owners and operators of critical infrastructure, whose actions may provide the nation's front line of defense against major cyber attacks.

A **Engage and embed cleared private sector representatives** from the most critical infrastructure assets in government intelligence and information sharing centers to help inform and prioritize information declassification. Industry generally needs to know when, how, and what to protect from attack—not who might launch an attack or why.

- Examine the Kansas Intelligence Fusion Center as a model for co-location and information sharing. This fusion center has private sector representatives cleared to the TS-SCI level who are actively working on cyber issues side-by-side with the National Guard and other agency representatives.
- Consider significantly expanding the National Cybersecurity and Communications Integration Center (NCCIC), which provides a central location to coordinate public-private information sharing and response, and increasing ISAC integration.

B **Expand the mission of intelligence agencies** to proactively share intelligence with private sector owners and operators to support the defense of critical civilian infrastructure. Establish protocols that require intelligence analysts and federal response officials to rapidly share threat vectors and attack indicators—either with cleared individuals or through declassification—as early as possible.

ACTION REQUIRED BY: NSC, DHS, ODNI, FBI, and the Intelligence Community

Supporting Findings

- **The inability to rapidly declassify and share the less-sensitive elements of a potential threat**, like threat indicators or vulnerabilities, leaves private companies in the dark for too long.
  - Those with a high need to know—businesses who could immediately act to secure critical systems—are often some of the last to know.
  - Our processes to share classified intelligence were designed for slower-paced threats and are insufficient as cyber threats escalate.
- **Intelligence agencies do not have the clear mission or processes to proactively declassify information as a threat unfolds, as they have not historically needed to treat private businesses as primary customers of threat data.**
  - Intelligence agencies have the authority to declassify and share information, but often lack the clear mission. While DHS has a clear mission to share with the private sector, it often does not "own" the information and must work through other agencies to declassify and share.
- **Building trusted relationships is at the core of effective information sharing**. Agencies and businesses must work as trusted partners in securing the nation from cyber threats and work proactively to understand operational and information needs.

Recommendation 8

PILOT AN OPERATIONAL TASK FORCE OF EXPERTS IN GOVERNMENT AND THE ELECTRICITY, FINANCE, AND COMMUNICATIONS INDUSTRIES—led by the executives who can direct priorities and marshal resources—to take decisive action on the nation's top cyber needs with the speed and agility required by escalating cyber threats.

A **Establish a three-tiered task force** that includes: 1) senior executives in industry and government with the authority to set priorities and direct resources, 2) operational leaders who work the issues and implement strategic direction, and 3) dedicated full-time operational staff from both industry and government that dig in and solve complex issues. This operational component is crucial if the task force is to be successful.

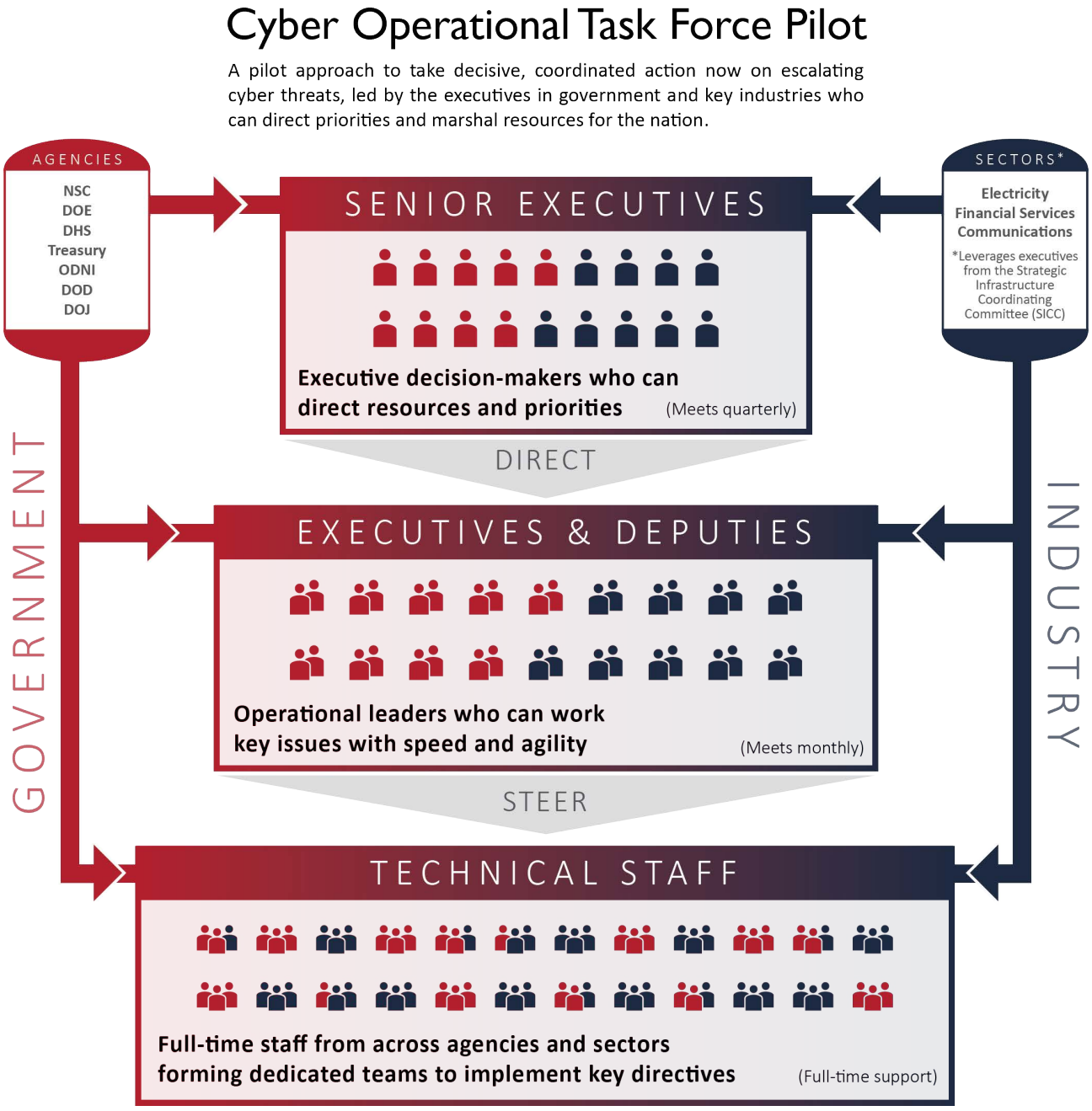
B **Leverage the SICC to identify executives** in the Electricity, Financial Services, and Communications sectors willing to participate in the pilot task force.

C **Use the NIAC's recommendations and findings as a starter agenda** to provide critical areas for focus. The task force should tackle persistent barriers to cyber coordination and information sharing, such as legal and liability issues, data privacy concerns, fragmentation of authorities, and cost allocation for improving the security of private networks.

D Use lessons learned and best practices from this pilot to **expand the task force coordination approach** to other sectors and assets.

ACTION REQUIRED BY: DOE, DHS, ODNI, NSC, the SICC, DOD, U.S. Department of the Treasury (Treasury), and U.S. Department of Justice (DOJ)

Recommendation 8 pilots an approach for agile, integrated action that we believe will be pivotal to achieving the level of coordination required to act on all recommendations. The graphic below illustrates how this pilot could be implemented.



Supporting Findings

- **Today's fragmentation of federal cybersecurity capabilities, authorities, missions, roles, and oversight is inefficient and precarious**. A bold new approach is needed.
- **Solutions to intractable cyber issues cannot be designed or led by any one agency.** The NIAC identified persistent, foundational coordination issues that will require a challenging reexamination of how agency missions are aligned and authorities are applied. Executive leadership and direction is required.
- **Key stakeholders in the Administration must champion cybersecurity with the private sector**. We need senior leaders to converge on national priorities, establish a clear agenda, and direct an operational team of cross-agency, public-private staff to triage and make headway on the biggest needs.
    - The operational task force would not be another advisory council or other passive coordination group. It is intended to design and *implement* solutions.
- **Senior-executives are crucial to driving action** because of their ability to set strategic direction and priorities, apply resources, and exercise accountability.
- **A pilot task force with the sectors facing the most urgent threats** and that have high executive engagement (i.e., Electricity, Financial Services, and Communications Sectors) will be able to mobilize quickly, tackle the most pressing issues, and allow the format to be tested to determine if it can be applied more broadly across sectors.
    - Senior executives in the Electricity, Financial Services, and Communications Sectors have formed the SICC to serve as a focal point for government engagement and cross-sector coordination.

Recommendation 9

USE THE NATIONAL-LEVEL GRIDEX IV EXERCISE (NOVEMBER 2017) TO TEST the detailed execution of federal authorities and capabilities during a cyber incident, and identify and assign agency-specific recommendations to coordinate and clarify the federal government's response actions where they are unclear.

A Invite executives and **representatives from the Financial Services and Communications** sectors to participate in exercise planning, ownership, and execution.

B **Require key agencies to develop white papers in advance of the exercise** that outline specifically how federal authorities will be executed in extreme situations to support response. Use the National Cyber Incident Response Plan (NCIRP), which outlines roles and responsibilities, and identify potential gaps in processes and protocols.

C **Test federal decision-making, protocols, and procedures** as it exercises specific authorities and capabilities during the exercise. For example, DHS has conducted extensive research into how to apply the Defense Production Act during an incident to prioritize resource allocation.

D Use the exercise to **further validate and refine the results of the DOE, DHS, and ODNI assessment**—called for in EO 13800—of the nation's readiness for a prolonged power outage associated with a significant cyber incident.

E **Direct specific recommendations from the GridEx after-action report to specific agencies** for implementation. The Administration should support and provide resources for agencies to implement the recommendations.

ACTION REQUIRED BY: DOE, DHS, ODNI, NSC, and the SICC

Supporting Findings

- **Our response to a large-scale, cyber attack with physical consequences on critical infrastructure today is likely to be insufficient**. High-level federal cyber incident response authorities are clear, but the specific timing, processes, and coordination of resources is not well understood by federal personnel or industry owners and operators.
    - Several agencies have substantial emergency authorities during a major cyber attack, but it remains unclear what triggers those authorities, how they are applied, who authorizes them, and when.
    - High-level cyber incident response roles are defined in the NCIRP, but it remains unclear what triggers federal assistance and what it will look like in practice.
- **The timing and resource needs for a cyber incident will be largely different than for physical disaster response.** Detailed policies, procedures, and federal technical assistance, and mutual assistance agreements must be developed and exercised. Gaps and issues must be addressed in coordination.

Recommendation 10

Establish an **OPTIMUM CYBERSECURITY GOVERNANCE APPROACH** to direct and coordinate the cyber defense of the nation, aligning resources and marshaling expertise from across federal agencies.

A **Use the cyber task force (see Recommendation #8) to evaluate effective cyber governance models** from other nations and recommend the best approach to centralize and elevate cyber governance and enable national-level coordination for public-private cyber defense. Although the circumstances in the United States are different than in those nations, we believe that better coordination at the senior levels of the U.S. government would improve operational control over individual federal elements and help ensure an effective response to the cyber threat.

B **Consider establishing a senior-level position or similar unit** that can effectively coordinate and exercise operational control over individual federal organizations. This may require congressional action and broad public recognition of the urgency of the cyber threat—which experience shows may not come until after a catastrophic cyber incident occurs.

ACTION REQUIRED BY: DHS, ODNI, NSC, DOJ, DOD, and Congress

Supporting Findings

- **The substantial capabilities among federal agencies are collectively insufficient to address sophisticated cyber threats because they are divided, uncoordinated, and often duplicative**.
    - There is a large amount of dedicated, mission-oriented work being done by individual agencies. There are 6 federal cybersecurity centers, 140 cyber authorities and capabilities across 20 agencies, 4 tools, and 8 assessment programs.
    - This is indicative of both the enormous complexity of the problem and the fact that there are not and cannot be silver-bullet solutions.
- **Existing structures and legislative authorities result in numerous agencies and dozens of Congressional committees with cybersecurity oversight**, yet limited national-level consensus on priorities for focused action.
- **Innovative national governance models for cybersecurity** show that effective coordination, at speed, is driven by a central authority that can coordinate cyber priorities for the nation, align industry and government resources, and provide national leadership for cyber defense. (Appendix D summarizes new governance models recently unveiled by Israel and the United Kingdom.)

Recommendation 11

Task the Homeland Security Advisor to review the recommendations included in this report and within six months **CONVENE A MEETING OF SENIOR GOVERNMENT OFFICIALS** to address barriers to implementation and identify immediate next steps to move forward.

A In 12 months, **task the NIAC with tracking the status of implementing these recommendations** to create a focused and planned opportunity to measure our progress to improving cybersecurity of the nation's most critical infrastructure assets.

ACTION REQUIRED BY: Homeland Security Advisor

Supporting Findings

- **There is an urgent need to act**. Major attacks and watershed incidents—like the 9/11 attacks—have historically triggered a new level of strategic, coordinated action driven by public demand and strong political will. We have an opportunity to demonstrate foresight and leadership before a cyber attack severely disrupts critical services.
- We believe a senior Administration official like the Homeland Security Advisor can provide the authority and leadership to convene heads of government agencies and **lead a rapid advancement in the nation's cyber capabilities with industry leaders**.

Moving Forward: Fundamental Change

The time to act is now. As a nation, we need to move past simply studying our cybersecurity challenges and begin taking meaningful steps to improve our cybersecurity to prevent a major debilitating cyber attack.

The Working Group appreciates the Administration's attention on key issues that were continuously reiterated during this study, including the need to build and sustain a cyber workforce, identify strategies to deter adversaries, and to examine our readiness to respond to a major cyber attack on our electric grid.

National Vision and Leadership

We envision a national strategy—championed by senior leaders—that will allow government and industry to harness capabilities to successfully deter and withstand aggressive cyber attacks. Achieving a shared vision will require significant near-term and long-term commitments to ultimately achieve:

- Strong **public support and political will** to act in support of cybersecurity as a national priority.
- Strong **leadership** from the most senior levels of government and the private sector.
- Federal cyber authorities and capabilities are **aligned, coordinated, and easily accessible** across government and the private sector.
- Businesses receive **incentives and technical assistance** to meet basic standards for cybersecurity.
- The nation is positioned to **effectively protect and defend against cyber attacks**, mitigate the impact of cyber attacks, and quickly respond and recover following an incident.
- The United States is a **world leader in cybersecurity.** USA, Inc.—the concept of the public and private sector working seamlessly together like a unified business unit—has cemented its position as a world leader in cyber technology and cyber workforce.

Our nation needs direction and leadership to dramatically reduce cyber risks. The NIAC stands ready to continue to support the President in this area.

Appendix A. Study Methodology

The private sector and federal government are extensively examining cyber risks in both individual and coordinated efforts. Over the past few years, a robust body of good work has been completed that has outlined the current cyber risk landscape, the need to take action, and *what* needs to be done. In this crowded space, the NIAC's distinct value lies in its ability to provide insights from senior-level, private sector owners and operators into *how* the government can best work with the private sector to secure the most critical infrastructure assets.

Charge to the NIAC

The May 11, 2017, *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (EO 13800) called for improving the cybersecurity of critical infrastructure at greatest risk by applying existing federal authorities and capabilities. On May 15, 2017, the White House through the NSC tasked the NIAC to review existing federal authorities and capabilities, and examine how they could be employed to assist and better support the cybersecurity of critical infrastructure assets that are at greatest risk of an attack that could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.

Study Approach

To conduct this study, the Council formed the Cyber Study Working Group made up of nine NIAC members, to examine how existing federal authorities and capabilities could be applied in the private sector. To complete the study, the Working Group:

- **Built on the *NIAC Cyber Scoping Study*** completed in February 2017. For that study, the Working Group interviewed more than 20 past and present senior leaders in government and the private sector, received four classified and four unclassified briefings, and reviewed many of the recent U.S. strategies and expert reports on how to address cyber risk. The scoping study identified three urgent cyber priorities that were affirmed by this current study:

  1. Triage today's problems.

  - Implement immediate and urgent fixes to address the most serious cyber risks to critical infrastructure. Focus on the sectors and set of assets, that if compromised, would result in major economic, safety, and security consequences to the United States.
  - Improve cyber hygiene across all critical infrastructure and consider some form of compliance.
  - Improve information sharing mechanisms, leading to machine-to-machine exchanges.

  2. Develop novel approaches for cyber resilience.

  - Design next-generation cyber systems that are inherently secure, resilient, and self-healing, particularly those that control critical functions. Develop solutions that make it extremely difficult and economically unattractive to extract value.

  3. Strengthen public-private partnership and leadership.

  - Develop effective executive-level, public-private mechanisms to strengthen leadership and efficient decision-making concerning critical cyber incidents and policy actions.
  - Streamline, reconfigure, and clarify roles and responsibilities within the federal government.

- **Focused on the leading-edge, highly critical sectors** of Electricity and Financial Services, which have been cited by the NIAC and other entities, such as the Homeland Security Advisory Council as vital because they underpin the operations of other critical infrastructure sectors. As a result, focusing on these sectors provided broad insights that can be applied in other critical sectors. (See Appendix C for more information).
- **Leveraged the wealth of existing information and built on the body of extensive work examining the nation's cybersecurity**. For example, the most recent and most comprehensive of which was the Commission on Enhancing National Cybersecurity (CENC) *Report on Securing and Growing the Digital Economy*, published in December 2016. The CENC—comprised of 12 representatives from industry, academia, and former government officials—identified six imperatives, 16 recommendations, and 52 specific actions to move forward. The recommendations address many of the challenges identified in this and other studies, including cyber workforce development, increasing research and development, and better aligning and understanding federal and private sector roles and responsibilities.
- **Identified industry cyber needs** and started with the assumption that federal authorities and capabilities exist and could be applied to the private sector.
- **Conducted interviews** with 22 senior leaders and experts in government and the private sector, including five individuals who were also interviewed during the *NIAC Cyber Scoping Study.* (See Appendix B for a list of interviewees and report contributors). In total, the Working Group built on information from interviews with 38 senior leaders and experts between the two closely-linked studies.
- **Reviewed list of more than 140 different federal capabilities and related authorities provided to the Working Group in July 2017** to identify capabilities that aligned with industry needs and existing capabilities highlighted in interviews and research.

Appendix B. Acknowledgements

Working Group Members

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

Robert Carr (Co-Chair), Founder and Chairman, Give Something Back Foundation; and Founder and former CEO, Heartland Payment Systems

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

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

Margaret E. Grayson, Consultant, E2M, LLC; former President MTN Communications Government Services; former President and CEO, V-ONE Security Services

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

Tom Noonan, Former General Manager, Cisco Energy Services

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

Beverly Scott, Ph.D., CEO, Beverly Scott Associates, LLC; former General Manager, Massachusetts Bay Transportation and Rail, and Transit Administrator for the Commonwealth of Massachusetts (NIAC Vice Chair)

Working Group Support

Saba Long, Owner, Obelisk Strategies

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

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

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

Rivka Tadjer, Chief of Staff, Give Something Back Foundation

Interviewees

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

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

John Bear, President and CEO, Midcontinent Independent System Operator (MISO)

William Terry Boston, former President and CEO, PJM; and current NIAC member

Michael Daniel, former Special Assistant to the President, and former Cybersecurity Coordinator

Lt. Gen. Albert J. Edmonds, Chairman and CEO, Edmonds Enterprise Services, Inc.; CEO, Logistics Applications, Inc.; former Director, Defense Information Systems Agency (DISA); and current NIAC member

Daniel Ennis, Center for International and Security Studies Fellow, University of Maryland; former Chief, Tailored Access Operations, NSA; former Director, Threat Operations Center, NSA

Nate Fick, CEO, Endgame

Lt. Gen. Reynold Hoover, Deputy Commander, U.S. Northern Command

Interagency Working Group with representatives from more than a dozen federal agencies

Rob Joyce, Assistant to the President for Homeland Security and Counterterrorism

James Katavolos, Senior Vice President, Citigroup

Henry Kenchington, Deputy Assistant Secretary, Cybersecurity and Emerging Threats Research and Development Division, Office of Electricity Delivery and Reliability (OE), U.S. Department of Energy (DOE)

Bob Kolasky, Acting Deputy Under Secretary for the National Protection and Programs Directorate (NPPD) and Deputy Assistant Secretary for the Office of Infrastructure Protection (IP), U.S. Department of Homeland Security (DHS)

Richard Ledgett, former Deputy Director, NSA

Kristin Lovejoy, CEO, BluVector

Kevin Mandia, CEO, FireEye

Jeanette Manfra, Assistant Secretary for Cybersecurity and Communications, NPPD, DHS

Tom McDermott, Deputy Assistant Secretary for Cyber Policy, Office of Policy, DHS

Bill Nelson, President and CEO, Financial Services Information Sharing and Analysis Center (FS-ISAC)

Edward Reiskin, Director of Transportation, San Francisco Municipal Transit Authority (SFMTA)

Lisa Walton, Chief Technology Officer, SFMTA

Errol Weiss, Senior Vice President, Threat Analytics and Information Sharing, Bank of America

Lucia Ziobro, Chief for Cyber Operational Engagement, Federal Bureau of Investigation (FBI)

NIAC Cyber Scoping Study Interviews (Oct. 2016-Feb.2017)

Scott Aaronson, Executive Director, Security and Business Continuity, EEI

Michael Assante, Lead, Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) Security, SANS Institute; and Co-founder of NexDefense

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

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

John Carlson, Chief of Staff, FS-ISAC; Vice Chair, FSSCC

R. James Caverly, Adjunct Research Staff Member, Institute for Defense Analyses; and former Director, Partnership and Outreach Division, IP, 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 Associates; and former Assistant Secretary, IP, DHS

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

Glenn Gerstell, General Counsel, NSA; and former NIAC member

Eric Goldstein, Branch Chief, Partnership and Engagement, Office of Cybersecurity and Communications, DHS; former Senior Counselor to the Undersecretary, NPPD, DHS

Patricia A. Hoffman, Principal Deputy Assistant Secretary and Acting Assistant Secretary, OE, DOE

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

Monica Maher, Director for Cybersecurity, NSC

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

Stephanie Morrison, former Director, Critical Infrastructure Policy, NSC

Bill Nelson, President and CEO, FS-ISAC

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

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

Paul Stockton, Managing Director, Sonecon; Senior Fellow, Johns Hopkins Applied Physics Lab; former Assistant Secretary for Homeland Defense, U.S. Department of Defense (DOD)

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

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

NIAC Cyber Scoping Study Briefings

Classified

- National Security Agency (NSA)
- U.S. Cyber Command
- Office of the Director of National Intelligence (ODNI)
- U.S. Cybersecurity and Emergency Response Team (US-CERT)

Unclassified

- NSA and U.S. Cyber Command
- Federal Bureau of Investigation (FBI)
- Mike Assante, SANS Institute
- Draper Lab

Department of Homeland Security Study Support Resources

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

Deirdre Gallop-Anderson, Alternate Designated Federal Officer, NIAC, IP, DHS

Beth Ward, Nexight Group, LLC

Lindsay Kishter, Nexight Group, LLC

Jack Eisenhauer, Nexight Group, LLC

Jim Carey, Nexight Group, LLC

Jennifer Ganss, Nexight Group, LLC

Megan Wester, BayFirst Solutions, LLC

Appendix C. Urgency of Cyber Threats to Critical Sectors

Given the short-time frame for this study, the Working Group focused on sectors facing urgent threats that exemplify the complexity and scale of the cyber challenge for the nation's critical infrastructure. The Electricity and Financial Services Sectors are not only interconnected, but also underpin all other sectors. The Homeland Security Advisory Council (HSAC) Cybersecurity Subcommittee stated in its 2016 report that these sectors along with the Communications Sector face rapidly growing cyber threats, and because of other sectors' reliance on them, could be attractive targets for a cyber attack.[2] A large-scale cyber attack on one of these sectors could cause cascading effects across multiple sectors, threatening public health and safety, as well as economic and national security.

1. Increasing Sophistication and Intent of Cyber attacks

Over the past 25 years, the technical knowledge needed to launch an attack has decreased. Malicious cyber tools and exploits can be easily found on the Internet and may be used by lone actors, organized criminal and terrorist groups, or nation-states. At the same time, the sophistication of cyber attacks has increased. For example, the Stuxnet attack, first discovered in 2010, disrupted Iranian nuclear facilities through a series of events: the malware infiltrated Windows systems through USB drives, then autonomously spread to programmable logic controllers that ultimately destroyed 984 uranium enrichment centrifuges.[3] Stuxnet showcases an early case of successfully targeting industrial control systems (ICS), and illustrates how a cyber attack can have very serious physical consequences.

> *"Experts agree that the [cyber] threat is so grave because barriers to entry are extremely low while potential rewards are great." - NSA General Counsel Glenn Gerstell, Keynote address at Duke Law's Center on Law, Ethics and National Security 2017 Conference*

Not only are attacks more sophisticated: attributing attacks to specific actors is difficult, if the cyber intrusion is even detected. As more devices become Web-enabled or connected to a network, the number of cyber intrusions increases. The U.S. Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) reported 290 cyber attacks on critical infrastructure control systems in fiscal year 2016.[4]

In the second installment of its Quadrennial Energy Review, published in January 2017, the U.S. Department of Energy (DOE) stated:

"In the current environment, the U.S. [electric] grid faces imminent danger from cyber attacks, absent a discrete set of actions and clear authorities to inform both responses and threats. Widespread disruption of electric service because of a transmission failure initiated by a cyber attack at various points of entry could undermine U.S. lifeline networks, critical defense infrastructure, and much of the economy; it could also endanger the health and safety of millions of citizens."[5]

[2] HSAC. *Final Report of the Cybersecurity Subcommittee: Part I-Incident Response*. 2016.
[3] Zetter. "An unprecedented look at Stuxnet, the world's first digital weapon." 2014.
[4] NCCIC. *ICS-CERT: Year in Review 2016*.
[5] DOE. *The Second Installment of the QER*. January 2017.

2. Ability to Attack Physical Systems through Cyber Means

All businesses face the threat of cyber attacks on their business networks, customer accounts, communication systems, Websites, and proprietary data. Many critical infrastructure companies, however, face additional threats to their operational technology (OT) systems—often called ICS or supervisory control and data acquisition (SCADA)—which operate physical processes such as the generation, processing, and delivery of power, water, fuels, and chemicals; and the controls for communication and transportation. Cyber attacks on OT can potentially disrupt vital services, damage critical equipment, threaten human health and safety, and trigger disruptions in other sectors.

Cyber-connected OT devices have significantly improved automation and efficiency in the monitoring and measurement of critical functions, but these new efficiencies also introduce vulnerabilities. Traditionally, OT security—particularly in the Electricity Sector—has relied on obscurity and specialization in keeping threat actors from disrupting ongoing operations.[6] An individual utility's system was highly customized to meet the needs of its customers and might only be compatible with components from a specific vendor; these characteristics limited an attacker's ability to find and execute exploits against grid components.

Unlike the central SCADA or information technology (IT) systems, OT systems are not automatically updated with service packs, new releases, and bug fixes. In reality, the OT devices are often running the same software as when they were installed 10-15 years ago at a time when physical separation form the network IT systems was considered secure.[7]

Operational Technology ≠ Information Technology

Web-enabled sensing and measuring technologies have enabled the critical systems to become more reliable and automated, but have also created more vulnerabilities that differentiate OT from IT:

- *Compromise of OT can disable operations, disrupt critical services to customers, and damage highly specialized equipment.*
- *OT must be able to survive a cyber incident while sustaining critical functions.*
- *Many OT systems must operate in real-time with 24/7 availability and are unable to go offline for patching or upgrades.*
- *OT components may be very simple devices and may not have enough computing resources to support additional cybersecurity capabilities.*
- *OT components may be widely dispersed and located in publicly accessible areas where they are subject to physical tampering.*

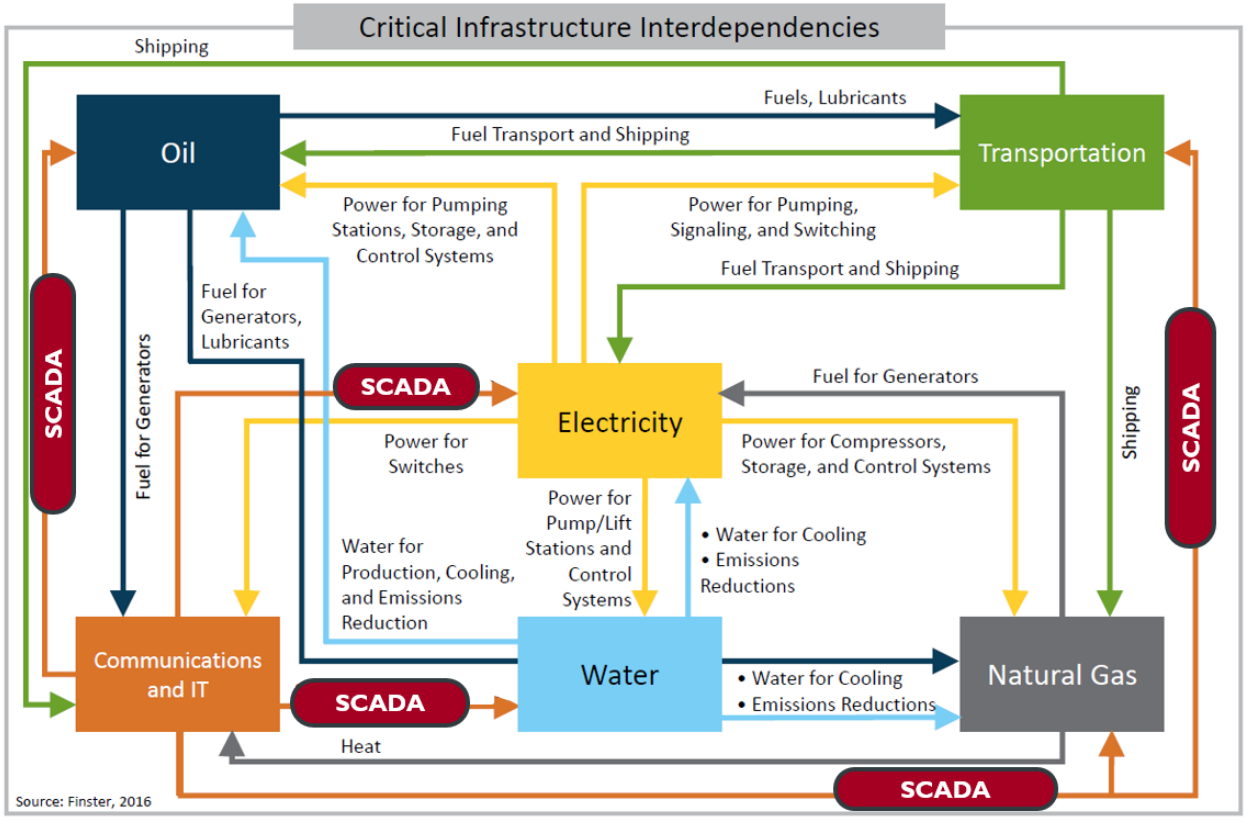
Upgrading, replacing, or patching network components could result in an interruption of service, and even a brief interruption can have cascading effects on how other sectors function. These systems also cannot simply be turned off when an attack is detected. OT security technologies require not only focusing on detecting attacks, but maintaining functionality during them.

Figure 1 is a schematic that highlights the interdependencies between sectors and the SCADA controls that are integral to the operations of electricity, fuels, water, and transportation. If one sector fails, the products and services they provide to other sectors may be disrupted as well.

[6] DOE. *Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats.* 2016.

[7] Fowke. "Testimony before the U.S. Senate Committee on Energy and Natural Resources Subcommittee on Energy." 2017.

Figure 1. Interdependencies Compound Cyber Risks[8]



The U.S. Electricity Sector consists of over 3,300 electricity providers[9]—a mix of publicly- and privately-owned businesses or municipalities—responsible for the generation, transmission, and distribution of electricity throughout the country. These systems are all interconnected, and a disruption in one small utility can potentially cascade into a widespread and long-term outage.

In 2015, a major cyber attack caused widespread disruption to power services throughout Ukraine, resulting in 225,000 customers without power. In this attack, three electric distribution companies and several substations in Ukraine were targeted by readily available malware tools.[10] Long-term planning and coordination contributed to the success of this extensive cyber attack; investigations determined that the affected entities were breached about nine months prior through spear-phishing emails.[11]

This was one of the first examples of a targeted and sophisticated cyber attack that disrupted electricity delivery. In addition to causing power disruptions, cyber attacks on the Electricity Sector can damage highly specialized and costly equipment. Recovering from system or equipment failure—particularly in the bulk power system—requires a careful and time-consuming restoration process, which potentially keeps customers stranded in the dark for a long period.

The Financial Services Sector consists of investment institutions, insurance companies, credit and financing organizations, and the infrastructure that enables these businesses to function.[12] These organizations,

[8] DOE. *The Second Installment of the QER*. 2017.
[9] APPA. *2016-2017 Statistical Report*. 2017.
[10] DOE. *The Second Installment of the Quadrennial Energy Review*. 2017.
[11] DOE. *Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats.* 2016.
[12] DHS. "Financial Services Sector" Webpage. Last updated July 6, 2017.

ranging in size from small businesses to multinational corporations, are responsible for millions of dollars in assets.

In 2016, the chair of the Securities and Exchange Commission (SEC) cited cybersecurity as the biggest risk to the sector.[13] Later that year, the Bangladesh Central Bank's network was infiltrated by hackers who were able to obtain log-in credentials to the Society for Worldwide Interbank Financial Telecommunications Network (SWIFT). Access to the network, which allows financial institutions to share information, enabled the hackers to steal over $80 million.[14]

While the SWIFT attack shows the inherent risks to individual financial entities, future sophisticated attacks could result in larger-scale and longer-term disruptions to the economy. Such compromises to the data of major financial institutions can erode consumer confidence. Financial Services Sector disruptions can also have cascading impacts on other sectors that require financial data systems for day-to-day operations. For example, in 2012, several financial institutions large and small withstood coordinated distributed denial-of-service (DDoS attacks).[15]

3. Defining and Unifying Public and Private Sector Roles

Throughout our nation's history we have developed well-established roles for government and the private sector to manage various kinds of physical risks. For example, if there is a threat of an attack through a missile or bomb, the federal government has a clearly defined role to step in for the common defense of the nation. For cyber threats of a similar scale, the private sector is the first line of defense and the role of the government to defend critical systems it does not own is unclear.

"Even though the Internet is now ubiquitous in our lives, cyber remains the only domain where we ask private companies to defend themselves against Russia, China, Iran, and other nation-states."— Penny Pritzker, former Secretary of Commerce, September 27, 2016, Keynote address at the U.S. Chamber of Commerce Cybersecurity Summit

It is widely agreed that the federal government bears the responsibility of protecing the United States from a major nation-state attack or an attack that could have major public safety, economic, or national security implications. But the traditional roles and responsibilities become less clear in the cyber realm, particularly the shared responsibility between government and industry as cyber attacks become more sophisticated and the potential consequences increase. As it becomes harder and more expensive to protect systems from cyber attacks attacks begin to outpace the capabilities of any individual company, and the government has more of a role to play. How these roles are shared remains a challenge.

Repeatedly throughout the study, the Working Group heard that the federal government should exercise its authority to deter adversaries. The United States has deterrence power as part of its diplomatic tools. It must find a way to extend deterrence capabilities into the cyber domain to make it clear to nation-states and other adversaries that there are consequences for attacks, in the same way there would be in a traditionally physical attack.

[13] Lambert. "SEC says cyber security biggest risk to financial system." 2016.
[14] Security Scorecard. *Financial Industry Cybersecurity Research Report.* 2016.
[15] DHS. *Financial Services Sector-Specific Plan.* 2015.

Shared Need for Cyber Workforce

The federal government and the private sector have both identified the shared need for a larger and more skilled cyber workforce. This talent shortage is expected to grow over the next few years. The Center for Cyber Safety forecasted the workforce shortage will reach 1.8 million unfilled cyber positions by 2022.[16]

In 2016, the Federal Cybersecurity Workforce Strategy included a four-pronged government-wide approach to increasing cyber jobs by expanding the workforce through education and training; increasing recruitment and outreach; improving employee retention through developmental opportunities; and identifying specific cybersecurity workforce gaps.[17] The Working Group learned from interviews that there are numerous programs already in place tackling this issue, including the National Science Foundation's CyberCorps: Scholarship for Service, Defense Information Systems Agency Pathways Program, and the National Initiative for Cybersecurity Careers and Study.

An assessment of the scope and sufficiency of the nation's cybersecurity workforce and education efforts is already underway to meet requirements of EO 13800.[18] The results of the assessment are expected later this year, and the Working Group has great interest in learning more about the recommendations for growing and sustaining the nation's cybersecurity workforce.[19]

4. Examples of Success

As the comprehensive dataset of more than 140 different federal capabilities and related authorities illustrates, there is an impressive depth of available federal capabilities available today, including capabilities that play a crucial role in cyber defense and information sharing.

National Cybersecurity and Communications Integration Center

The National Cybersecurity and Communications Integration Center (NCCIC) serves as a federal civilian interface for multi-directional and cross-sector information sharing. The NCCIC includes four branches: NCCIC Operations and Integration (NO&I), United States Computer Emergency Readiness Team (US-CERT), Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), and National Coordinating Center for Communications (NCC).[20]

The Electricity Information Sharing and Analysis Center (E-ISAC) and Financial Servives Information Sharing Analysis Center (FS-ISAC) both have representatives at the NCCIC, allowing for better collaboration and coordination of information sharing. Information Sharing and Analysis Centers (ISACs) were frequently identified as successful mechanisms for sharing threat information and working collaboratively within sectors and with government partners.

Electricity Information Sharing and Analysis Center

The E-ISAC is a division of the North American Electric Reliability Corporation (NERC) that gathers and analyzes security information, coordinates incident management, and communicates mitigation strategies with stakeholders within the electricity industry, across interdependent sectors, and with government partners.[21] The E-ISAC works in collaboration with DOE and the Electricity Subsector Coordinating Council

[16] Center for Cyber Safety and Education. *Global Information Security Workforce Study*. 2017.
[17] The White House. "Strengthening the Federal Cybersecurity Workforce." Press release. 2016.
[18] The White House. Executive Order—Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. 2017.
[19] NICE. NICE Webinar Series. 2017.
[20] NCCIC. "NCCIC." 2017.
[21] E-ISAC. "About." 2017.

(ESCC) to serve as the primary security communications channel for the Electricity Sector and enhances its ability to prepare for, and respond to cyber and physical threats, vulnerabilities, and incidents.[22] The E-ISAC's success is built on trusted relationships. All information shared with the E-ISAC is protected from the Federal Energy Regulatory Commission (FERC), NERC, and the Compliance and Enforcement Program via signed legal agreements, NERC corporate policy, and physical and logical separation from NERC.[23]

Financial Services Information Sharing and Analysis Center

The FS-ISAC is often cited as a successful model that provides member-to-member information sharing, as well as providing various levels of information to arm companies with the information they need to take action. It has almost 7,000 members in more than 30 countries, including banks, credit unions, payment processors, broker-dealers, third party service providers, and insurance companies. The FS-ISAC uses a traffic-light protocol to share different levels of information based on classification. It is also working to establish the Energy Analytic Security Exchange (EASE). This new intelligence sharing community for utilities and energy grid companies is intended to provide members with real-time and "near real-time intelligence, the ability to monitor risks to extended supply chains, and access to cross-industry intelligence."[24]

The FS-ISAC is also working to form a more targeted, special interest group for the financial institutions deemed most critical for national and economic security. By taking the lead in this area, the Financial Services Sector is working to improve the cyber capabilities and reduce costs for these entities, and provide a forum for them to engage more intensely with U.S. government agencies. Ultimately, this group could be expanded beyond the Financial Services Sector to include participation of all assets deemed most critical to national and economic security.

Cybersecurity Risk Information Sharing Program

The Cybersecurity Risk Information Sharing Program (CRISP) was also cited as a successful example of an information sharing initiative for rapidly collecting, analyzing, and disseminating threat information among participating utilities. The hardware for capturing network data was first developed by DOE in partnership with its National Labs with the intent of automating data collection and analysis. The data collection is fully automated and analyzed, incorporating input from DOE and the Intelligence Community. The analyses are then distributed as alerts or mitigation measures to participating utilities. While the hardware and analytical capabilities were first developed in the public sphere, CRISP is managed and operated by the E-ISAC. The program's success is underlined by the fact that it initially faced a number of barriers and resistance from both the private and public sectors (e.g., compliance with privacy laws, classification levels). Utilities participating in CRISP serve over 75 percent of U.S. electricity customers. CRISP's machine-to-machine threat information sharing platform can also be adapted to enable company-to-company information sharing.

[22] E-ISAC. "About" Webpage. July 2017.
[23] E-ISAC. "E-ISAC Brochure." June 2017.
[24] FS-ISAC. "FS-ISAC Launches New Energy Sector Sharing Community" Press Release, February 15, 2017.

Appendix D. National Cyber Governance: United Kingdom and Israeli Models

The Working Group repeatedly heard in interviews that the federal government is not organized to effectively deploy existing cyber capabilities and authorities. The United Kingdom (UK) and Israel were cited as models of nations that faced major cyber threats and challenges, which triggered a reorganization of how these governments approached cybersecurity. Below is a brief overview of what those countries have in place, should the United States decide to move forward with a fundamental restructuring of cyber authorities.

Overall there are three key takeaways:

1. The national government has established one central point of federal cyber authority.
2. Cyber offense, including attribution and strike-back capabilities, is identified as a clear responsibility that government plays in deterring cyber adversaries.
3. Cyber defense and cyber technology leadership are inextricably linked.

1. Cyber Efforts in the United Kingdom

National Cyber Security Strategy 2016-2022

In November 2016, the UK published its plan to make the UK more secure and resilient in cyberspace. The strategy includes three main objectives: 1) defend against evolving cyber threats and effectively respond to incidents, 2) deter and disrupt hostile action, and take offensive actions if needed, and 3) develop the cybersecurity industry, research and development (R&D), and talent needed.[25] It also included a £1.9 billion investment.

The strategy established that the government is ultimately responsible for assuring the country's cyber resilience, and that the UK would not accept the risks created by businesses not taking the necessary steps to manage cyber threats.[26]

National Cyber Security Centre

The National Cyber Security Centre (NCSC) was launched in October 2016 and officially opened in February 2017 "to be the authority on the UK's cyber security environment, sharing knowledge, addressing systemic vulnerabilities, and providing leadership on key national security issues." The NCSC is a public-facing organization with reach back to the Government Communications Headquarters (GCHQ), the UK equivalent of the National Security Agency (NSA), and is intended to provide a unified source of threat intelligence.[27]

The NCSC replaced three cyber organizations—the Centre for Cyber Assessment (CCA), Computer Emergency Response Team UK (CERT UK), and CESG (the GCHQ's information security arm). Cyber-related responsibilities were also shifted from the Centre for the Protection of National Infrastructure (CPNI).[28]

[25] HM Government. *National Cyber Security Strategy 2016-2022*. 2016.
[26] Ibid.
[27] HM Government, "National Cyber Security Centre."
[28] Ibid.

Office of Cyber Security and Information Assurance

The Office of Cyber Security and Information Assurance (OCSIA) helps determine cybersecurity priorities, provides strategic direction, and coordinates the government cybersecurity program. OCSIA also supports education and awareness initiatives for the country, works with the private sector to exchange information and promote best practices in cybersecurity, ensures that cyber capabilities are maintained and improved as needed. The office coordinates with the NCSC.[29]

Existing Regulations

General Data Protection Regulation: A European Union (EU) regulation intended to strengthen and unify personal data protection (including the export of personal data outside the EU). This replaces the data protection directive from 1995, and will become effective in May 2018. It requires business to have capabilities to protect personal data and requires personal data breaches be reported (with fines resulting from breaches an additional possibility). The Information Commissioner's Office (ICO) and NCSC are working to ensure UK organizations can thrive under the directive.[30]

The Directive on security of network and information systems (NIS Directive): An EU directive that establishes minimum requirements that high-risk organizations and digital service providers should have for cyber protection to ensure these groups build comprehensive cyber risk management programs. It aims to improve cooperation among EU countries in cyber incidents.[31]

2. Cyber Efforts in Israel

The **National Cyber Bureau** was created to advance the capabilities outlined in Government Resolution No. 3611 of 2011. The Bureau reports to the Prime Minister (PM) and provides guidance and policy coordination to the PM and across the government. Resolution 3611 also established a national Computer Emergency Response Team (CERT). The Bureau is also charged with encouraging cooperation among academia, industry, and government entities to improve cyber defense of national critical infrastructures.[32]

Below are the four main functions of the Bureau:[33]

1. **Defending against Cyber Threats:** Develop a national defense strategy and establish cross industry or industry-specific regulation; develop a national cyber situation assessment and cyber threat reference.
2. **Promoting the Cyber Defense Industry:** Establish cyber R&D programs and encourage international companies to invest in Israel.
3. **Developing Academia and Human Capital:** In Israel, the civilian cybersecurity presence extends from a number of private companies to education and training that encourages young people to pursue work in cybersecurity. This builds upon a national culture that is focused on security and a nearly universal recognition that cyber threats are both imminent and a high priority.

[29] HM Government. "Office of Cyber Security and Information Assurance."
[30] HM Government Information Commissioner's Office. "Overview of the General Data Protection Regulation."
[31] European Commission. "Digital Single Market."
[32] Israeli Prime Minister's Office. "Mission of the Bureau."
[33] Israeli Government. *Resolution No. 3611 of the Government of August 7. 2011*.

4. **International Cooperation:** Develop relationships with state partners with similar cyber goals – promote information sharing, R&D, etc.

In 2015, Resolution 2444 was approved, which established a **National Cyber Defense Authority**, allowing the National Cyber Bureau to focus on strategy, whereas the Authority would focus on operational objectives to improving cyber protection.[34]

- The purpose of the Authority is to "direct, operate, and execute as needed all defensive and operational efforts at the national level in cyberspace, based on a systemic approach, to allow a full and constant defensive response to cyber attacks, including the handling of cyberspace threats and cyber events in real time, formulation of a current situation assessment, gathering and research of intelligence, and work with the special institutions."[35]

Challenges

One of the major criticisms of these recent organizational changes is that the roles and responsibilities of the resulting organizations have not been clear.[36] These criticisms have primarily come from heads of other Israeli security agencies, but are also highlighted in a report from the Knesset's (Israel's version of Congress) Foreign Affairs and Defense Committee.[37]

Since the National Cyber Defense Authority is subordinate to the National Cyber Bureau, there are concerns this structure could hamper the Authority's work with improving cybersecurity for civilian groups.

Other conclusions cited in the report are that the Authority should avoid becoming yet another intelligence gathering agency; any regulations put forth by the Authority must take into account and involve all relevant defense and civilian parties; and that the structure of cyber leadership should be reexamined periodically over the next five years.[38]

[34] Chachko, Elena. "Cyber Reform in Israel at an Impasse: A Primer." 2017.
[35] Even, Shmuel. "Structuring Israel's Cyber Defense." 2016.
[36] Chachko, Elena. "Cyber Reform in Israel at an Impasse: A Primer." 2017.
[37] The Knesset. "Foreign Affairs and Defense Committee." 2016.
[38] Even, Shmuel. "Structuring Israel's Cyber Defense." 2016.

Appendix E. References

Adamsky, Dmitry. "The Israeli Odyssey toward its National Cyber Security Strategy," *The Washington Quarterly,* 40, no. 2:113-127. June 14, 2017. https://twq.elliott.gwu.edu/sites/twq.elliott.gwu.edu/files/downloads/TWQ_Summer2017_Adamsky.pdf.

Alkhalisi, Zahraa. "Saudi Arabia warns of new crippling cyber attack," *CNN*, January 26, 2017. http://money.cnn.com/2017/01/25/technology/saudi-arabia-cyberattack-warning/index.html.

American Public Power Association (APPA). *2016-2017 Statistical Report*. 2017. http://www.publicpower.org/Programs/Landing.cfm?ItemNumber=38710&&navItemNumber=3.

Atlantic Council. *Overcome by cyber risks? Economic benefits and costs of alternate cyber futures.* September 2015. http://publications.atlanticcouncil.org/cyberrisks/.

Behr, Peter and Blake Sobczak. "White House-New cyber order draft keeps focus on critical grid companies," *E&E News,* May 4, 2017. https://www.eenews.net/energywire/2017/05/04/stories/1060054017.

Bell, Greg, Tony Buffomante, Ken Dunbar, and Cliff Justice. "Technology: Al Adds a New Layer to Cyber Risk," *Harvard Business Review,* April 13, 2017. https://hbr.org/2017/04/ai-adds-a-new-layer-to-cyber-risk.

Boyd, Aaron. "Civilian Cybersecurity Strategy coming this summer," *Federal Times,* July 14, 2015. http://www.federaltimes.com/story/government/cybersecurity/2015/07/14/civilian-cybersecurity-strategy/30138103/.

Boyd, Aaron. "Initial meeting lays out how commission will enhance cybersecurity," *Federal Times,* April 15, 2016. http://www.federaltimes.com/story/government/cybersecurity/2016/04/15/cyber-commission-first-meeting/83080592/.

Brown, Jared T. *Presidential Policy Directive 8 and the National Preparedness System: Background and Issues for Congress.* Congressional Research Service. October 21, 2011. https://fas.org/sgp/crs/homesec/R42073.pdf.

Burley, Diana L. "Testimony Before the United States of Representatives Committee on Science, Space, & Technology, Subcommittee on Research and Technology Hearing on Strengthening U.S. Cybersecurity Capabilities." February 14, 2017. http://docs.house.gov/meetings/SY/SY15/20170214/105554/HHRG-115-SY15-Wstate-BurleyD-20170214.pdf.

Carberry, Sean D. "Fate of Trump cyber order still unclear," *FCW: The Business of Federal Technology,* April 11, 2017. https://fcw.com/articles/2017/04/11/trump-cyber-order-murky.

Center for Cyber Safety and Education. *Global Information Security Workforce Study*. 2017. https://iamcybersafe.org/research_millennials/.

Center for Strategic and International Studies (CSIS). "CSIS Cyber Policy Task Force." Accessed January 13, 2017. https://www.csis.org/programs/technology-policy-program/cybersecurity/csis-cyber-policy-task-force.

Center for Strategic and International Studies (CSIS). *From Awareness to Action. A Cybersecurity Agenda for the 45th President.* Accessed July 18, 2017. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170110_Lewis_CyberRecommendationsNextAdministration_Web.pdf.

Center for Strategic and International Studies (CSIS). "Significant Cyber Incidents List." Accessed July 18, 2017. https://csis-prod.s3.amazonaws.com/s3fs-public/170519_Significant_Cyber_Events_List.pdf?HJ4k1Bt7x.zleLsdr9m6SQbkWHtuNJ39.

Center for Strategic and International Studies (CSIS) Cyber Policy Task Force. Testimony of Iain Mulholland. *Strengthening U.S. Cybersecurity Capabilities.* February 14, 2017. http://docs.house.gov/meetings/SY/SY15/20170214/105554/HHRG-115-SY15-Wstate-MulhollandI-20170214.pdf.

Center for Strategic and International Studies (CSIS) Cybersecurity Commission. *A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters.* November 2010. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/101111_Evans_HumanCapital_Web.pdf.

Center for Strategic and International Studies (CSIS) Cybersecurity Commission. *Cybersecurity Two Years Later.* 2011. https://www.csis.org/analysis/cybersecurity-two-years-later.

Center for Strategic and International Studies (CSIS) Cybersecurity Commission. *Securing Cyberspace for the 44th Presidency.* 2008. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

Center for Strategic and International Studies (CSIS) Cybersecurity Commission. *Twenty Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines.* 2009. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/Twenty_Critical_Controls_for_Effective_Cyber_Defense_CAG.pdf.

Chachko, Elena. "Cyber Reform in Israel at an Impasse: A Primer," *Lawfare*, April 27, 2017. https://www.lawfareblog.com/cyber-reform-israel-impasse-primer.

Chappell, Bill. "We're No. 3: U.S. Infrastructure, Education Faulted In Global Competitiveness Index," *NPR,* September 28, 2016. http://www.npr.org/sections/thetwo-way/2016/09/28/495796271/were-no-3-u-s-infrastructure-education-faulted-in-global-competitiveness-index.

Columbus, Louis. "Roundup of Internet of Things Forecasts and Market Estimates," *Forbes,* November 27, 2016. https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#6c7f7dc2292d.

Commission on Enhancing National Cybersecurity (CENC). "Briefing on Current Federal Initiatives for the Federal Governance Sub-Committee." Washington, D.C. August 3, 2016. https://www.nist.gov/sites/default/files/documents/2017/01/19/commission_preparatory_working_group_meeting_august_3_2016_clean_final.pdf.

Commission on Enhancing National Cybersecurity (CENC). "Meeting Minutes." American University Washington College of Law, Washington, D.C. September 19, 2016. https://www.nist.gov/sites/default/files/documents/2016/11/15/sept_19_2016_amer_univ_meeting_minutes.pdf.

Commission on Enhancing National Cybersecurity (CENC). "Meeting Minutes." Conference Calls. July 7, 2016 – November 21, 2016.

Commission on Enhancing National Cybersecurity (CENC). "Meeting Minutes." New York University School of Law-Vanderbilt Hall, New York, NY. May 16, 2016. https://www.nist.gov/sites/default/files/may_16_2016_nyc_meeting_minutes.pdf.

Commission on Enhancing National Cybersecurity (CENC). "Meeting Minutes." University of California, Berkeley, Berkeley, CA. June 21, 2016. https://www.nist.gov/sites/default/files/june_21_2016_ucb_meeting_minutes.pdf.

Commission on Enhancing National Cybersecurity (CENC). "Meeting Minutes." University of Houston, Houston, TX. July 14, 2016. https://www.nist.gov/sites/default/files/commission_on_enhancing_national_cybersecurity_mn_09072016.pdf.

Commission on Enhancing National Cybersecurity (CENC). "Meeting Minutes." University of Minnesota, Minneapolis, MN. August 23, 2016. https://www.nist.gov/sites/default/files/documents/2016/11/15/aug_23_2016_univ_minnesota_meeting_minutes.pdf.

Commission on Enhancing National Cybersecurity (CENC). "Meeting Minutes." U.S. Department of Commerce-Commerce Research Library, Washington, D.C. April 14, 2016. https://www.nist.gov/sites/default/files/documents/cybercommission/Meeting_Minutes_April_14.pdf.

Commission on Enhancing National Cybersecurity (CENC). "Panelist Statements." New York University—School of Law, New York, NY. May 16, 2016. https://www.nist.gov/sites/default/files/may_16_panelist_statements.pdf.

Commission on Enhancing National Cybersecurity (CENC). "Panelist Statements." University of California, Berkeley, Berkeley, CA. June 21, 2016. https://www.nist.gov/sites/default/files/documents/2016/09/12/june21_panelist_statements.pdf.

Commission on Enhancing National Cybersecurity (CENC). "Panelist and Speaker Statements." University of Houston, Houston, TX. July 14, 2016. https://www.nist.gov/sites/default/files/july14_panelist_statements.pdf.

Commission on Enhancing National Cybersecurity (CENC). "Panelist and Speaker Statements." University of Minnesota, Minneapolis, MN. August 23, 2016. https://www.nist.gov/sites/default/files/documents/2016/08/25/august23_panelist_statements.pdf.

Commission on Enhancing National Cybersecurity (CENC). "Panelist and Speaker Statements." American University, Washington, D.C. September 19, 2016. https://www.nist.gov/sites/default/files/documents/2016/09/23/dc_commission_panelist_and_speaker_statements.pdf.

Commission on Enhancing National Cybersecurity (CENC). "Preparatory Working Group Meeting." Washington D.C. October 19, 2016. https://www.nist.gov/sites/default/files/documents/2017/01/19/commission_preparatory_working_group_meeting_october_19_2016_clean_final.pdf.

Commission on Enhancing National Cybersecurity (CENC). "Recommendations Working Group Discussion." Washington, D.C. November 8, 2016. https://www.nist.gov/sites/default/files/documents/2017/01/19/commission_preparatory_working_group_meeting_november_8_2016_clean_final.pdf.

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

Dahan, Maha El, Jim Finkle, Andrew Hay, Mark Potter, and Reem Shamseddine. "Saudi Arabia warns on cyber defense as Shamoon resurfaces," *Reuters,* January 23, 2017. http://www.reuters.com/article/us-saudi-cyber-idUSKBN1571ZR.

Defense Information Systems Agency (DISA). "Pathways Program." Accessed July 31, 2017. http://www.disa.mil/careers/pathways-program.

Deloitte. *Quantum Dawn 2: A simulation to exercise cyber resilience and crisis management capabilities*. October 21, 2013. https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Financial-Services/gx-fsi-us-Quantum-Dawn-2-2013-10.pdf.

Deloitte. *Standing Together for Financial Industry Resilience: Quantum Dawn 3 After-Action Report.* November 19, 2015. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-quantum-dawn-3-after-action-report.pdf.

Electricity Information Sharing and Analysis Center (E-ISAC). "About E-ISAC." Accessed July 28, 2017. https://www.eisac.com/#about.

Electricity Information Sharing and Analysis Center (E-ISAC). *Analysis of the Cyber Attack on the Ukrainian Power Grid.* March 18, 2016. http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.

Electricity Information Sharing and Analysis Center (E-ISAC). "E-ISAC Brochure." Public Document Library. June 2017. https://www.eisac.com/api/documents/6436/publicdownload.

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

European Commission. "Digital Single Market: The Directive on security of network and information systems (NIS Directive)." Accessed July 17, 2017. https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.

Even, Shmuel, David Siman-Tov, and Gabi Siboni. "Structuring Israel's Cyber Defense." Institute for National Security Studies with Tel Aviv University. *INSS Insight* No. 856. September 21, 2016. http://www.inss.org.il/publication/structuring-israels-cyber-defense/.

Executive Office of the President. *Federal Cybersecurity Research and Development Strategic Plan. Cybersecurity National Action Plan.* 2016. https://www.cerias.purdue.edu/assets/symposium/2016/docs/shannon_slides.pdf.

Executive Office of the President. National Science and Technology Council. *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program*. December 2011. https://www.nitrd.gov/SUBCOMMITTEE/csia/Fed_Cybersecurity_RD_Strategic_Plan_2011.pdf.

Executive Office of the President. Office of Management and Budget. *Memorandum for the Heads of Executive Departments and Agencies: Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.* May 19, 2017. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/M-17-25.pdf.

Executive Office of the President. President's Council of Advisors on Science and Technology. *Report to the President Immediate Opportunities For Strengthening the Nation's Cybersecurity.* November 2013. https://www.broadinstitute.org/files/sections/about/PCAST/2013%20pcast-cybersecurity.pdf.

Fattah, Zainab. "Cyber Attacks Target Saudi Arabia's State Agencies, Companies," *Bloomberg*, January 24, 2017. https://www.bloomberg.com/news/articles/2017-01-24/cyber-attacks-target-saudi-arabia-s-state-agencies-companies.

Federal Energy Regulatory Commission (FERC). "Commission Will Approve Applications For Prudent Cost Recovery Tied To Security Needs." Press release, September 14, 2001. https://www.ferc.gov/media/news-releases/2001/2001-3/nr01-38.PDF.

Financial Services Information Sharing and Analysis Center (FS-ISAC). "2017 FS-ISAC Annual Summit." Agenda. May 1, 2017. https://www.fsisac-summit.com/files/galleries/2017annual-web-descriptions.pdf.

Financial Services Information Sharing and Analysis Center (FS-ISAC). "FS-ISAC Launches New Energy Sector Sharing Community." Press release, February 15, 2017. https://www.fsisac.com/sites/default/files/news/FS-ISAC_Sector_EASE_Press_Release_FINAL_2-15-17.pdf.

Financial Services Information Sharing and Analysis Center (FS-ISAC). *Strength In Sharing: 2017 FS-ISAC Annual Summit Brochure.* 2017. https://www.fsisac-summit.com/files/galleries/2017annual-brochure.pdf.

Flournoy, Michele and Amy Schafer. "Building a cyber ROTC," *Boston Globe*, July 13, 2017. https://www.bostonglobe.com/opinion/2017/07/12/flournoy/RZJgYqcmIScy51HyUiopII/story.html.

Fowke, Benjamin G.S. III. "Testimony before the U.S. Senate Committee on Energy and Natural Resources Subcommittee on Energy hearing to Examine Cybersecurity Threats to the U.S. Electrical Grid and Technology Advancements to Minimize the Threat." March 28, 2017. https://www.energy.senate.gov/public/index.cfm/files/serve?File_id=40A50EA7-75FA-4CEB-9A5A-3FE9074F4B77.

Franzetti, Andres. "In the Lame Duck, How Congress Makes Cybersecurity A Non-Partisan Priority," *Forbes*. November 14, 2016. https://www.forbes.com/sites/realspin/2016/11/14/in-the-lame-duck-how-congress-makes-cybersecurity-a-non-partisan-priority/#246e39351469.

Friedman, Sam and Adam Thomas. "Demystifying cyber insurance coverage," *Deloitte University Press,* February 23, 2017. https://dupress.deloitte.com/dup-us-en/industry/financial-services/demystifying-cybersecurity-insurance.html.

Gambrell, Jon. "Saudi Arabia warns destructive computer virus has returned (Updated)," *Phys Org News,* January 24, 2017. https://phys.org/news/2017-01-saudi-arabia-destructive-virus.html.

Gerstell, Glenn. "Confronting the Cybersecurity Challenge—Keynote Address by Glenn S. Gerstell, NSA General Counsel." 2017 Law, Ethics and National Security Conference at Duke Law School. February 25, 2017. https://www.nsa.gov/news-features/speeches-testimonies/speeches/20170225-gerstell-duke-keynote.shtml.

Gregory-Brown, Bengt. *Securing Industrial Control Systems—2017.* SANS Institute. June 2017. https://www.sans.org/reading-room/whitepapers/analyst/securing-industrial-control-systems-2017-37860.

HM Government. *Cyber Security Regulation and Incentives Review.* December 2016. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/579442/Cyber_Security_Regulation_and_Incentives_Review.pdf.

HM Government. "Office of Cyber Security and Information Assurance." Accessed July 7, 2017. https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance.

HM Government. "National Cyber Security Centre." Accessed July 7, 2017. https://www.ncsc.gov.uk/about-us.

HM Government. *National Cyber Security Strategy 2016-2022.* 2016. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

HM Government Information Commissioner's Office. "Overview of the General Data Protection Regulation." Accessed July 17, 2017. https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/.

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

House of Representatives. *National Defense Authorization Act for Fiscal Year 2017*. November 2016. http://docs.house.gov/billsthisweek/20161128/CRPT-114HRPT-S2943.pdf.

Idaho National Laboratory. *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector.* August 2016. https://energy.gov/epsa/downloads/cyber-threat-and-vulnerability-analysis-us-electric-sector.

IBM Global Technology Services. *IBM Security Services 2014 Cyber Security Intelligence Index.* 2014. https://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf.

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). "About the Industrial Control Systems Cyber Emergency Response Team." Accessed July 24, 2017. https://ics-cert.us-cert.gov/About-Industrial-Control-Systems-Cyber-Emergency-Response-Team.

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). *ICS-CERT Annual Assessment Report FY 2016.* Accessed July 19, 2017. https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/FY2016_Industrial_Control_Systems_Assessment_Summary_Report_S508C.pdf.

Clinton, Larry, and David Perera, eds. *The Cybersecurity Social Contract: Implementing a Market-Based Model for Cybersecurity.* Internet Security Alliance. September 2016.

Israeli Government. *Resolution No. 3611 of the Government of August 7, 2011: Advancing National Cyberspace Capabilities*. Accessed July 17, 2017. http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Documents/Advancing%20National%20Cyberspace%20Capabilities.pdf.

Israeli Prime Minister's Office. "Mission of the Bureau." Accessed July 17, 2017. http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Pages/default.aspx.

Intelligence and National Security Alliance (INSA). *FINnet: A Proposal to Enhance the Financial Sector's Participation in Classified Cyber Threat Information Sharing.* June 2017. https://www.insaonline.org/wp-content/uploads/2017/06/INSA-FINnet-Proposal-June-2017.pdf.

The Knesset. "Foreign Affairs and Defense Committee: National Cyber Defense Authority should be in charge of Israel's cyber defense." Press release, August 1, 2016. https://knesset.gov.il/spokesman/eng/PR_eng.asp?PRID=12198.

Lambert, Lisa, and Suzanne Barlyn. "SEC says cyber security biggest risk to financial system," *Reuters*, May 17, 2016. http://www.reuters.com/article/us-finance-summit-sec-idUSKCN0Y82K4.

Lloyd's. *Business Blackout*. July 2015. https://www.lloyds.com/news-and-insight/risk-insight/library/society-and-security/business-blackout.

Madnick, Stuart. "Preparing for the Cyber attack That Will Knock Out U.S. Power Grids," *Harvard Business Review,* May 10, 2017. https://hbr.org/2017/05/preparing-for-the-cyber attack-that-will-knock-out-u-s-power-grids.

Mandiant Consulting. "Threat Landscape: By The Numbers," *Infographic*, August 10, 2016. https://www.slideshare.net/FireEyeInc/infographic-mtrends-2016.

National Cybersecurity and Communications Integration Center (NCCIC). "NCCIC." Accessed July 28, 2017. https://www.us-cert.gov/nccic.

National Cybersecurity and Communications Integration Center (NCCIC). "Preparing for Cyber Incident Analysis." Accessed July 18, 2017. https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_Cyber_Incident_Analysis_S508C.pdf.

National Cybersecurity and Communications Integration Center (NCCIC). "ICS-CERT Fact Sheet." Accessed July 19, 2017. https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_IR_Pie_Chart_FY2016_S508C.pdf.

National Cybersecurity and Communications Integration Center (NCCIC). *ICS-CERT: Year in Review 2016.* Accessed July 18, 2017. https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_Final_S508C.pdf.

National Cybersecurity Center of Excellence (NCCoE). "Fact Sheet: About the National Cybersecurity Center of Excellence." Accessed July 18, 2017. https://nccoe.nist.gov/sites/default/files/library/fact-sheets/nccoe-fact-sheet.pdf.

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). *Best Practices for Government to Enhance the Security of National Critical Infrastructure.* 2004. 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. 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. 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. 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. 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.* 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). *Critical Infrastructure Security Resilience National Research and Development Plan*. 2014. https://www.dhs.gov/sites/default/files/publications/NIAC-CISR-RD-Plan-Report-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). Cyber Scoping Study Working Group Quarterly Business Meeting Presentation. February 16, 2017.

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). *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). *The Prioritization of Critical Infrastructure for a Pandemic Outbreak in the United States*. 2007. https://www.dhs.gov/sites/default/files/publications/niac-pandemic-outbreak-final-report-01-17-07-508.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). *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). *Transportation Sector Resilience*. 2015. 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. 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. 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. https://www.dhs.gov/sites/default/files/publications/niac-workforce-education-final-report-04-11-06-508.pdf.

National Initiative for Cybersecurity Careers and Studies (NICCS). "NICCS Workforce Development." Accessed July 31, 2017. https://niccs.us-cert.gov/.

National Initiative for Cybersecurity Education (NICE). NICE Webinar Series. "The President's Executive Order on Cybersecurity Workforce: Next Steps and How to Engage." June 5, 2017. https://www.nist.gov/sites/default/files/documents/2017/07/05/cybersecurity_eo_webinar_slides.pdf.

National Institute of Standards and Technology (NIST). *Framework for Improving Critical Infrastructure Cybersecurity.* 2014. https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

National Institute of Standards and Technology (NIST). "National Initiative for Cybersecurity Education (NICE), About." Accessed July 31, 2017. https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework.

National Institute of Standards and Technology (NIST). "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework." Accessed July 31, 2017. https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework.

National Institute of Standards and Technology (NIST). Testimony of Charles H Romine, Ph.D. *Strengthening U.S. Cybersecurity Capabilities.* 2017. https://www.nist.gov/speech-testimony/strengthening-us-cybersecurity-capabilities.

National Institute of Standards and Technology (NIST). "Notice, Request for Information—Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Workforce Development." *Federal Register*. July 12, 2017. https://www.federalregister.gov/documents/2017/07/12/2017-14553/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure-workforce.

National Science and Technology Council. Networking and Information Technology Research and Development. *Federal Cybersecurity Research and Development Strategic Plan.* February 2016. https://www.nitrd.gov/cybersecurity/publications/2016_Federal_Cybersecurity_Research_and_Development_Strategic_Plan.pdf.

National Security Agency (NSA). "Frequently Asked Questions." Accessed July 18, 2017. https://www.nsa.gov/about/faqs/about-nsa-faqs.shtml.

National Security Agency (NSA). "Mission and Strategy." Accessed July 18, 2017. https://www.nsa.gov/about/mission-strategy/.

National Security Telecommunications Advisory Committee (NSTAC). *Cybersecurity Collaboration Report.* 2009. https://www.dhs.gov/sites/default/files/publications/NSTAC%20CCTF%20Report.pdf.

National Security Telecommunications Advisory Committee (NSTAC). *Industrial Internet Scoping Report.* 2014. https://www.dhs.gov/sites/default/files/publications/Final%20NSTAC%20Industrial%20Internet%20Scoping%20Report_0.pdf.

National Security Telecommunications Advisory Committee (NSTAC). *2009-2010 NSTAC Issue Review.* 2010. https://www.dhs.gov/sites/default/files/publications/2009%20-%202010%20Issue%20Review%20%28FINAL%29_0.pdf.

National Security Telecommunications Advisory Committee (NSTAC). *NSTAC Report to the President on Communications Resiliency.* 2011. https://www.dhs.gov/sites/default/files/publications/NSTAC-Report-to-the-President-on-Communications-Resiliency-2011-04-19.pdf.

National Security Telecommunications Advisory Committee (NSTAC). *NSTAC Report to the President on Information and Communications Technology Mobilization.* 2014. https://www.dhs.gov/sites/default/files/publications/NSTAC%20-%20Information%20and%20Communications%20Technology%20Mobilization%20Report%2011-19-2014.pdf.

National Security Telecommunications Advisory Committee (NSTAC). *NSTAC Report to the President on the Internet of Things.* 2014. https://www.dhs.gov/sites/default/files/publications/IoT%20Final%20Draft%20Report%2011-2014.pdf.

National Security Telecommunications Advisory Committee (NSTAC). *Telecommunications and Electric Power Interdependency Task Force (TEPITF).* 2006. https://transition.fcc.gov/pshs/docs/advisory/hkip/GSpeakers060418/ACT1070.pdf.

North American Electric Reliability Corporation (NERC). *Grid Security Exercise (GridEx II) After-Action Report.* March 2014. http://www.nerc.com/pa/CI/CIPOutreach/GridEX/GridEx%20II%20Public%20Report.pdf.

North American Electric Reliability Corporation (NERC). *Grid Security Exercise GridEx III Report.* March 2016. http://www.nerc.com/pa/CI/CIPOutreach/GridEX/NERC%20GridEx%20III%20Report.pdf.

Office of the Director of National Intelligence (ODNI). "Mission, Vision, & Goals." Accessed July 24, 2017. https://www.odni.gov/index.php/who-we-are/mission-vision.

Office of the Director of National Intelligence (ODNI). "What We Do." Accessed July 24, 2017. https://www.odni.gov/index.php/what-we-do.

Office of Electricity Delivery & Energy Reliability (OE). "Energy Sector Cybersecurity Framework Implementation Guidance." January 2015. https://energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf.

Office of Personnel Management (OPM). "CyberCorps: Scholarship for Service, Students: Frequently Asked Questions." Accessed July 31, 2017. https://www.sfs.opm.gov/StudFAQ.aspx#num8.

Paganini, Pierluigi. "Symantec speculates Shamoon 2 attacks aided by Greenbug hackers," *Security Affairs,* January 24, 2017. http://securityaffairs.co/wordpress/55634/cyber-crime/shamoon-2-greenbug.html.

Pagliery, Jose. "Hackers destroy computers at Saudi aviation agency," *CNN*, December 2, 2016. http://money.cnn.com/2016/12/01/technology/saudi-arabia-hack-shamoon/?iid=EL.

Pritzker, Penny. "U.S. Secretary of Commerce Penny Pritzker Delivers Key Note Address at U.S. Change of Commerce's Cybersecurity Summit." Written remarks, September 27, 2016. https://www.commerce.gov/news/secretary-speeches/2016/09/us-secretary-commerce-penny-pritzker-delivers-keynote-address-us.

PwC. "Industry findings: Telecommunications." Excerpt from the *Global State of Information Security Survey*. Accessed July 19, 2017. https://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/telecommunications-industry.html.

Sabillon, Regner, Victor Cavaller, and Jeimy Cano. "National Cyber Security Strategies: Global Trends in Cyberspace." *International Journal of Computer Science and Software Engineering,* No. 5. 5:67-81. May 2016. http://ijcsse.org/published/volume5/issue5/p1-V5I5.pdf.

Security Scorecard. *2016 Financial Industry Cybersecurity Report.* August 2016. https://cdn2.hubspot.net/hubfs/533449/SecurityScorecard_2016_Financial_Report.pdf.

Siboni, Gabi and Ofer Assaf. *Guidelines for a National Cyber Strategy.* The Institute for National Security Studies. March 2016. http://www.inss.org.il/publication/guidelines-for-a-national-cyber-strategy/.

Swartz, Scott D. and Michael J. Assante. *Industrial Control System Cybersecurity Response to Physical Breaches of Unmanned Critical Infrastructure Sites.* SANS Institute. January 2014. https://www.sans.org/reading-room/whitepapers/analyst/industrial-control-system-ics-cybersecurity-response-physical-breaches-unmanned-critical-infrastructure-sites-35282.

Thomas, Will. "Congress Passes National Defense Authorization Act," FYI: Science Policy News from AIP, American Institute of Physics, December 9, 2016. https://www.aip.org/fyi/2016/congress-passes-national-defense-authorization-act.

Trump for America. "President-Elect Trump Announces Former Mayor Rudolph Giuliani to Lend Expertise in Cyber Security Efforts." GreatAgain Website. Accessed January 17, 2017. https://greatagain.gov/giuliani-681188f84cb5#.6ka6242fx.

United States Computer Emergency Readiness Team (US-CERT). "Alert (TA17-163A) CrashOverride Malware." Accessed July 19, 2017. https://www.us-cert.gov/ncas/alerts/TA17-163A.

The Honorable James R. Clapper, Director of National Intelligence, the Honorable Marcel Lettre, Undersecretary of Defense for Intelligence, and Admiral Michael S. Rogers, USN Commander, U.S. Cyber Command Director, National Security Agency. "Joint Statement for the Record to the Senate Armed Services Committee: Foreign Cyber Threats to the United States." January 5, 2017. https://www.armed-services.senate.gov/imo/media/doc/Clapper-Lettre-Rogers_01-05-16.pdf.

U.S. Department of Defense, U.S. Cyber Command. *Beyond the Build: Delivering Outcomes through Cyberspace*. June 3, 2015. https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/docs/US-Cyber-Command-Commanders-Vision.pdf.

U.S. Department of Energy (DOE). *Transforming the Nation's Electricity System: The Second Installment of the Quadrennial Energy Review.* January 2017. Accessed July 18, 2017. https://energy.gov/epsa/downloads/quadrennial-energy-review-second-installment.

U.S. Department of Energy (DOE). *Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats.* June 2016. https://energy.gov/sites/prod/files/2017/01/f34/Electric%20Grid%20Security%20and%20Resilience--Establishing%20a%20Baseline%20for%20Adversarial%20Threats.pdf.

U.S. Department of Homeland Security (DHS). *Cyber Storm V: After Action Report.* July 2016. https://www.dhs.gov/sites/default/files/publications/CyberStormV_AfterActionReport_2016vFinal-%20508%20Compliant%20v2.pdf.

U.S. Department of Homeland Security (DHS). *Cyber Storm III Final Report.* July 2011. https://www.dhs.gov/sites/default/files/publications/CyberStorm%20III%20FINAL%20Report.pdf.

U.S. Department of Homeland Security (DHS). *Emergency Services Sector-Specific Plan*. 2015. https://www.dhs.gov/sites/default/files/publications/nipp-ssp-emergency-services-2015-508.pdf.

U.S. Department of Homeland Security (DHS). *Energy Sector-Specific Plan.* 2015. https://www.dhs.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf.

U.S. Department of Homeland Security (DHS). "Financial Services Sector." Last updated July 6, 2017. https://www.dhs.gov/financial-services-sector.

U.S. Department of Homeland Security (DHS). *Financial Services Sector-Specific Plan.* 2015. https://www.dhs.gov/sites/default/files/publications/nipp-ssp-financial-services-2015-508.pdf.

U.S. Department of Homeland Security (DHS). "Industrial Control Systems Cyber Emergency Response Team." Accessed July 19, 2017. https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_ICS-CERT_S508C.pdf.

U.S. Department of Homeland Security (DHS). *Healthcare and Public Health Sector-Specific Plan.* 2016. Accessed July 20, 2017. https://www.phe.gov/Preparedness/planning/cip/Documents/2016-hph-ssp.pdf.

U.S. Department of Homeland Security (DHS). *Informing Cyber Storm V: Lessons Learned from Cyber Storm IV.* 2015. https://www.dhs.gov/cyber-storm-v.

U.S. Department of Homeland Security (DHS). "National Cybersecurity and Communications Integration Center." Last updated June 22, 2017. https://www.dhs.gov/national-cybersecurity-and-communications-integration-center.

U.S. Department of Homeland Security (DHS). *National Cyber Incident Response Plan.* December 2016. Accessed July 18, 2017. https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf.

U.S. Department of Homeland Security (DHS). *NCCIC/ICS-CERT Year in Review FY 2015*. Accessed July 17, 2017. https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf.

U.S. Department of Homeland Security (DHS). "National Protection and Programs Directorate Cybersecurity Legal Authorities Overview." Accessed July 31, 2017. https://www.dhs.gov/national-protection-and-programs-directorate.

U.S. Department of Homeland Security (DHS). "U.S. Government Support for Critical Infrastructure Cybersecurity Risk Management Authorities and Capabilities Matrix." Accessed July 31, 2017.

U.S. Government Accountability Office (GAO). *Cybersecurity: Actions Needed to Strengthen U.S. Capabilities.* February 14, 2017. https://www.gao.gov/assets/690/682757.pdf.

U.S. Government Accountability Office (GAO). *Federal Information Security: Actions Needed to Address Challenges.* September 19, 2016. http://www.gao.gov/assets/680/679877.pdf.

The White House. *Executive Order--Commission on Enhancing National Cybersecurity*. February 9, 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity.

The White House. *Executive Order—Improving Critical Infrastructure Cybersecurity*. February 12, 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

The White House. *Executive Order—Promoting Private Sector Cybersecurity Information Sharing*. February 13, 2015. https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.

The White House. *Executive Order—Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. May 11, 2017. https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal.

The White House. "Fact Sheet: Cybersecurity National Action Plan." February 9, 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

The White House. "Fact Sheet: Cyber Threat Intelligence Integration Center." February 25, 2016. https://obamawhitehouse.archives.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center.

The White House. *Presidential Policy Directive – Critical Infrastructure Security and Resilience.* February 12, 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

The White House. "Statement by the President on Signing the National Defense Authorization Act for Fiscal Year 2017." Press release, December 23, 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/12/23/statement-president-signing-national-defense-authorization-act-fiscal.

The White House. "Strengthening the Federal Cybersecurity Workforce." Press release, July 12, 2016. https://obamawhitehouse.archives.gov/blog/2016/07/12/strengthening-federal-cybersecurity-workforce.

Whitehouse, Sen. Sheldon. "Whitehouse Delivers Cybersecurity Recommendations For Trump Administration" Press release, January 5, 2017. https://www.whitehouse.senate.gov/news/release/whitehouse-delivers-cybersecurity-recommendations-for-trump-administration.

World Economic Forum. *The Global Competitiveness Report 2016-2017*. 2016. http://www3.weforum.org/docs/GCR2016-2017/05FullReport/TheGlobalCompetitivenessReport2016-2017_FINAL.pdf.

World Economic Forum. *Recommendations for Public-Private Partnership against Cybercrime*. January 2016. http://www3.weforum.org/docs/WEF_Cybercrime_Principles.pdf.

Zetter, Kim. "An unprecedented look at Stuxnet, the world's first digital weapon," *WIRED*, November 3, 2014. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

Zetter, Kim. "NSA Hacker Chief Explains How to Keep Him Out of Your System," *WIRED,* January 27, 2016. https://www.wired.com/2016/01/nsa-hacker-chief-explains-how-to-keep-him-out-of-your-system/.