TheChertoffGroup

Enabling A More Secure World

A SECURE AND RESILIENT U.S. ELECTRIC GRID

JULY 2019

EXECUTIVE SUMMARY »

The protection and reliability of the U.S. electric grid is a consistent national security priority, with responsibilities for security and resilience falling on the U.S. Departments of Energy and Homeland Security (DHS), as well as a number of supporting regulatory and standards-producing organizations. However, as DHS operationalizes the National Protection and Programs Directorate (NPPD) into the new Cybersecurity and Infrastructure Security Agency (CISA) and applies a new focus on infrastructure systems and critical functions, many are wondering how CISA will differ from NPPD to establish itself as the coordinating authority on infrastructure protection and national critical functions, how critical systems like the electric grid will be prioritized, and how CISA will work with the private sector to understand and reduce risk?

The number of vulnerabilities facing electric utility owners and operators only continues to grow, as does the number of sophisticated threat actors, including nation-states like Russia and China. The private sector is eager to be a meaningful and collaborative partner, but DHS needs to ensure CISA is prepared to lead a whole-of-government approach to work with infrastructure owners and operators to better understand and reduce the risks to our infrastructure systems and national critical functions.

To make meaningful, near-term progress toward building resilience across critical infrastructure sectors, and to empower and legitimize CISA—as well as the newly created National Risk Management Center—DHS should consider:

- Expanding information sharing pathways and transparency directly from CISA and the National Risk Management Center to private sector partners to improve coordination and develop a common operating picture.
- Investing in the research, development, and deployment of tools to make secure-by-design capabilities more accessible to grid owners and operators and easier to integrate into standard business processes.
- Working with the U.S. Congress to incentivize secure-by-design systems by considering additional liability protection for the private sector and critical infrastructure, such as extending Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act coverage to include disruptive cyber events attributed by the U.S. Government to a foreign state actor.
- Legitimizing the recommendations produced by the National Risk Management Center through national best practices and standards.
- Working with State Homeland Security Advisors to improve information sharing, coordination, and programmatic support between state and local governments and the private sector.

CRITICAL INFRASTRUCTURE: THE U.S. ELECTRIC GRID

INTRODUCTION »

The U.S. electric grid is one of the most relied upon infrastructures in the country. It is a complex system of substations, transformers, and power lines that is required to move power and connect electricity producers and consumers.[1] Of the 16 critical infrastructure sectors, the Energy Sector is considered one of several lifeline sectors and is depended upon by all other sectors to maintain their operability. The electric grid supplies a function that is critical to the daily way of life in the United States. It perfectly fits the DHS definition of critical infrastructure, as an asset "so vital to the United States that [its] incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination of those matters."[2]

The necessity of a resilient electric grid is without question. It is the criticality of services, such as electric power, that led DHS to create the Cybersecurity and Infrastructure Security Agency (CISA). This organization has the potential to shift how DHS will approach working with the private sector and critical infrastructure owners and operators—not just grid owners and operators—to manage risk and build resilience. CISA is the first federal cybersecurity agency with operational capabilities whose mission is to protect critical infrastructure through collaboration with the private sector. The National Risk Management Center (NRMC) is managed within CISA. Designed to represent a permanent public-private partnership between critical infrastructure and the U.S. Government, this Center "will identify and defend against today's threats, while securing against the evolving risks of tomorrow."[4]

It is unclear if this is an evolutionary step in the way DHS will collaborate with the private sector to identify and support national critical functions, or if it is just a rebranding of preexisting capabilities.

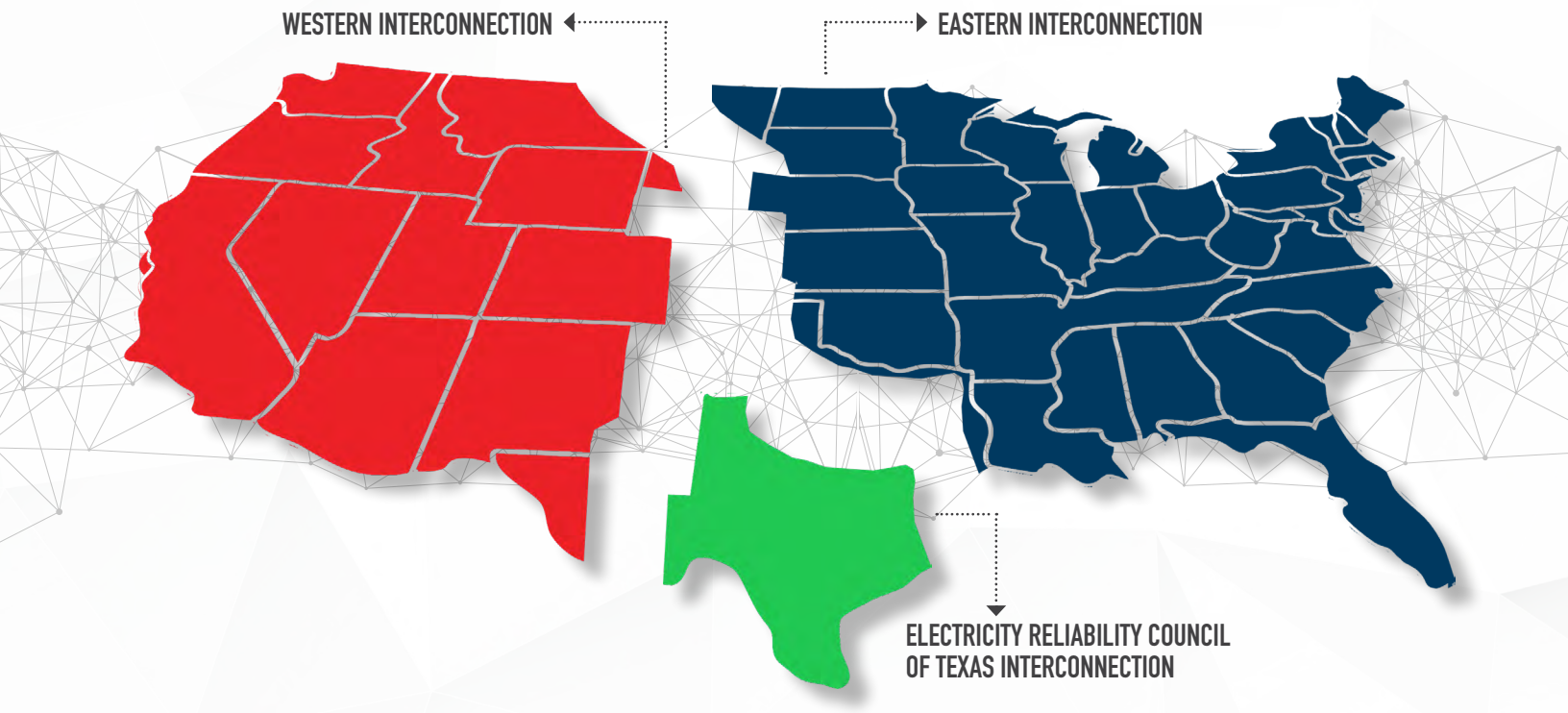
To be successful and make meaningful improvements toward a new level of cross-sector collaboration, the missions and authorities of CISA and the NRMC must be clearly defined, consistent across government agencies, and championed by the private sector.

In an effort to encourage and improve effective coordination and collaboration with the private sector, this white paper examines current DHS initiatives and the known goals and activities of CISA and the NRMC, while exploring the current threat environment facing the electric grid. It makes recommendations to strengthen relationships and capabilities through cross-sector collaboration around national critical functions, with a particular focus on the security and resilience of the electric grid supply chain. Concentrating on the electric grid supply chain is an opportunity to articulate how something once considered a sector-specific concern is critical to all sectors while also providing a focal point for the U.S. Government to ground its new efforts and produce meaningful results through CISA and the NRMC.

THE ELECTRIC GRID »

According to *Presidential Policy Directive/PPD 21: Critical Infrastructure Security and Resilience*, resilience is defined as "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents."[5] America's public safety and economic strength depends on reliable and consistent electrical power. The U.S. electric grid is a complex system composed of millions of interconnected components spread across the country. Furthermore, the reliability of the grid depends on raw energy sources and technologies that are procured through non-domestic supply chains.

REGIONS OF U.S. ELECTRIC GRID



These interconnections make up the physical system of the grid, including infrastructure from generation through distribution, whereas balancing authorities are responsible for the management and operation of the grid. These authorities ensure that power system demand and supply are appropriately balanced in order to maintain the safe and reliable operation of the power system. The grid must always be in balance, with generation matching the load, otherwise an unbalanced system can result in local and even regional power blackouts.[6] The advent of utility-scale battery storage could offset some of the reliability risk—increasing resilience—but the technology is not ubiquitous (most large-scale battery storage installations are in California and the northeastern United States), and its application has mostly been driven by state and federal regulators.[7]

To manage this complexity in a consumer-affordable manner, the U.S. employs a strategy whereby the energy infrastructure is owned and operated by thousands of different private-sector entities and is regulated through a network of public-sector agencies. The energy enterprise understands the critical service they provide and works hard to ensure that the electric grid is secured against damage and disruptions.

It is widely recognized, however, that there is no single solution that can completely eliminate each and every possible disruption scenario.[8] Rather, it is more effective to identify and invest in layered capabilities that can prevent, protect against, mitigate, respond to, and recover from all types of hazards.[9]

In addition to DHS, to help electric grid infrastructure owners and operators understand and manage risk, a whole of government approach is taken with support provided by the U.S. Department of Energy—the assigned Sector-Specific Agency responsible for developing the Energy Sector-Specific Plan and providing subject-matter expertise—as well as regulatory bodies like the Federal Energy Regulatory Commission (FERC) and the North American Reliability Corporation (NERC), and standards-producing organizations like the National Institute for Standards and Technology (NIST) and the International Organization for Standardization (ISO). These agencies and organizations work together and with grid owners and operators to build resilience into individual systems and interconnections collectively.[10]

Grid Reliability and the Cyber Threat

The reliability of the electric grid has been a longstanding concern for many reasons, largely because it is critical to every aspect of modern life. The good news is that the grid has a lot of built-in redundancy through system-specific capabilities and the benefits of regional interconnections. While certain incidents can have local impacts resulting in a set of substations being taken offline, such an incident would not pose a catastrophe-level risk. The bad news is that threat actors are increasingly motivated to target the energy sector and are becoming more sophisticated, while the number of threat vectors and vulnerabilities are only growing.

The evolution of the threat environment has made it increasingly challenging to account for all potential threat vectors and to mitigate all vulnerabilities. Just as threat vectors and vulnerabilities continue to grow, cyber capabilities are becoming more readily available, and threat actors will continue to adopt and develop new tactics, techniques, and procedures to use against targets in the United States.[11] In Dragos' 2017 in Review report, for example, Dragos discovered 163 new security vulnerabilities in Industrial Control Systems, 61 percent of which would cause "severe operational impact" if exploited in a cyber attack.[12]

The agencies responsible for regulating and assisting electric utilities to build and maintain security and resilience capabilities continue to develop new guidelines and requirements. NERC, for example, maintains 11 critical infrastructure protection standards subject to enforcement, 10 of which are related to cybersecurity,[13] and is planning to release cybersecurity supply chain risk management standards that will be subject to enforcement as well.[14] But the rate of expansion in threat pathways and the sophistication of actors now conducting cyber operations has changed the risk surface for critical infrastructure, especially electric utility owners and operators and the electric grid at large.

While individual actors and non-state actor groups still conduct a significant number of cyber operations globally, the advent of state actors using cyber operations to collect intelligence, and potentially manipulate critical systems and functions, makes the ability to defend against cyber-attacks much more challenging. According to the U.S. Department of Homeland Security, a primary target of these operations has been electricity systems.[15]

In April 2018, Jeanette Manfra, Assistant Secretary of the Office of Cybersecurity and Communications for the Department of Homeland Security (now Assistant Director of CISA), testified before the Senate Committee on Homeland Security and Governmental Affairs that Russian government actors continue to target government entities and businesses in the energy, nuclear, water, aviation, and critical manufacturing sectors.[16] DHS and the Federal Bureau of Investigation (FBI) assess Russia's objective to be to collect information on industrial control systems and ultimately gain access to industrial control system environments. In July 2018, the Department of Homeland Security told representatives of the energy sector that Russian actors had successfully gained access to the industrial control systems of an electric utility in the United States.[17]

According to DHS, these intrusion attempts have targeted two distinct categories of victims: staging and intended targets.[18] Specifically, DHS has observed Russia target certain entities that become pivot points (staging targets), leveraging existing relationships between the initial victim and the intended targets to hide their activity, as part of a multi-stage intrusion campaign to gain access to networks of major, high-value assets that operate components of U.S. critical infrastructure. A vulnerability in common corporate network software, such as enterprise resource planning applications, could ultimately provide access to operational technology like industrial control systems. A joint Technical Alert (TA18-074A) issued by DHS and the FBI outlines indicators of compromise and technical details on the tactics, techniques, and procedures of these intrusions.[19]

Through active information sharing forums and strong industry and government coordination—managed and facilitated by organizations like the Electricity Information Sharing and Analysis Center (E-ISAC) that look to reduce physical and cybersecurity risk to the electricity industry—electricity utilities at large have created layered defenses to either prevent access to critical functions or at least limit the consequences of a successful intrusion. However, as the number of skilled and motivated threat actors continues to grow, along with exploitable vulnerabilities and potential cascading impacts, it will become more challenging for utilities to effectively manage risk.

THE ELECTRIC GRID SUPPLY CHAIN »

Because both industry and government recognize these growing risks, there is increasing focus and intention by the U.S. Government on understanding interdependencies and their importance to, and impact on, national critical functions such as the generation, transmission, and distribution of electricity. Supply chains are a foundational aspect of interdependency analysis. So, what is a supply chain, and what are the risks?

Risks to the Electric Grid Supply Chain

A supply chain is the sequence of processes involved in the production and distribution of a commodity. Within the context of the electric grid, supply chains include the physical infrastructure to generate, transmit, and distribute electricity, but also the technology systems used to monitor and govern operations, as well as the third-party vendors utilized throughout the process. This makes the electric grid supply chain risk surface dynamic and complex, with exposure across hardware, software, and vendors.

Hardware can be shipped with built-in backdoors—whether known or unknown to the hardware developer—which has long been a concern of the U.S. Department of Homeland Security in sourcing information and communications technology (ICT) vendors, effectively leading to a ban of providers such as ZTE and Huawei on U.S. Government systems.[20] It can also be exploited by threat actors who leverage common misconfigurations.[21]

Similarly, **software can be directly compromised during the development or update phases, as was seen with the 2017 NotPetya attack when the NotPetya virus was delivered through compromised accounting software—ultimately becoming one of the most destructive and costly cyber attacks in history.**[22] Software can also be exploited by threat actors who leverage known vulnerabilities that haven't been remediated. This was the cause of the Equifax breach, which resulted in the theft of personal data of nearly 150 million people.[23] Finally, software can be exploited by threat actors who understand how to take advantage of software that was incorrectly implemented, especially those with widespread implications, such as enterprise resource planning applications, which support multiple functions including supply chain management.[24]

These and other vendors can be leveraged as stepping stones, or staging targets as previously discussed, to reach an actor's primary target. Examples of other vendor types include managed services providers, which remotely manage information technology infrastructure and have been repeatedly targeted to gain the confidential information of the businesses they support,[25] or sector-specific vendors, which are being actively targeted by nation-state actors, such as Russia, to gain access to critical functions and processes, such as industrial control systems.[26]

Finally, people continue to pose a risk—intentionally or not—that is a consistent challenge to overcome. According to Verizon's 2018 Data Breach Investigations Report, 17 percent of the 2,216 data breaches analyzed in the report were the result of avoidable human error. Further, the report estimated that 4 percent of individuals targeted in a phishing campaign will click on a malicious link or file.[27]

The Vulnerabilities are Only Increasing

As technologies advance and grow in complexity, along with the growing number of devices that can be connected to the internet, so do the vulnerabilities owners and operators are forced to mitigate. There are more than 20 billion "Internet of Things" (IoT) devices—any object or device that sends and receives data automatically through the internet[28]—estimated to be connected to the internet. Many of these IoT devices, which are only growing in number, are built with poor security design and present additional threat pathways for owners and operators to defend against.[29]

As grid owners and operators continue to rely on connected devices to monitor and automate system functions, the number of opportunities for threat actors to gain access to the system will increase as well.

The convergence of information technology (IT) and operational technology (OT) systems creates a potentially unmitigated vector directly into grid operations. IT systems integrated with OT systems—without sufficient controls to prevent access and movement between the two systems—are a pathway to attack core energy-related industrial control systems. The 2015 cyber attack against Ukraine's Kyivoblenergo, a regional electricity distribution company, demonstrates this tactic and was the first publicly acknowledged cyber attack to result in power outages.[30] Alternative goals may even go beyond manipulating outputs and operability, as seen in a cyber attack against a petrochemical plant in Saudi Arabia, in which many experts believe the attackers' objective, while unsuccessful, was to cause an explosion.[31]

Finally, software in general is only getting more complex with more lines of code, more open source software, and more frequent changes increasing the number of vectors for threat actors to take advantage of, and for critical infrastructure owners and operators to protect against. This requires high levels of awareness of a system's software applications, lifecycle and patches, and the security controls required to prevent access to and movement throughout the system.

All of these examples and vectors highlight the threat not only to the electric grid, but to critical infrastructure across all sectors, and the numerous opportunities along the supply chain to infiltrate and manipulate critical systems. Consequently, this makes the electric grid supply chain an excellent area of focus for DHS, by elevating a sector-specific concern to a national critical function, and dedicating resources to fully understanding the risks and developing solutions.

OPPORTUNITIES TO REDUCE RISK »

Prioritizing the security and resilience of the electric grid, specifically supply chain risk, is an opportunity for the Cybersecurity and Infrastructure Security Agency and the National Risk Management Center to support a national critical function, but also use it as a springboard to better understand critical operational interdependencies, and to work collaboratively—and effectively—with the private sector.

Over the past 16 years, DHS and other supporting and/or regulatory federal government agencies have largely been successful in national efforts to build resilience across critical infrastructure. However, these efforts also created a challenge that hinders effective coordination and collaboration today. Specifically, the segregation of information sharing between sectors. Creating a methodology to codify and organize programmatic priorities was extremely effective to begin building resilience within each sector, but the result of this structuring has created information stove pipes. While each sector has plenty of knowledge to share and lessons to learn from other sectors, there has historically been little cross-over between them.

The creation of CISA and the NRMC represents a potential change in this way of thinking on behalf of DHS. CISA has explicitly stated that its mission "requires effective coordination and collaboration among a broad spectrum of government and private sector organizations." Though promising, limited details on how CISA or the NRMC plan to incorporate the private sector in its planning, operations, and decision-making have been shared.

CISA was formally established in November 2018, but has, as a practical matter, existed for years as the former National Protection and Programs Directorate within DHS. It also includes the National Cybersecurity and Communications Integration Center, which provides 24/7 cyber situational awareness, analysis, incident response, and cyber defense capabilities. In this new structure, CISA is now responsible for protecting the nation's critical infrastructure from physical and cyber threats. In information made available since CISA's creation, it is clear a primary focus will be on coordinating critical infrastructure security and resilience efforts with the private sector, but how that will be implemented long-term, along with the incentives for and results from private sector participation are uncertain.

Managing risk through collaboration is a hallmark of DHS and clearly a guiding mantra for CISA and the NRMC. But how does that translate to effectiveness? The NRMC is a planning, analysis, and collaboration center tasked to identify and address the most significant risks to the nation's critical infrastructure. When the NRMC was announced, it was tied to this key focus area: "By understanding what is truly critical, where key dependencies and interdependencies lie, and the potential cascading impacts of threats, we can identify pockets of risk we deem to be unacceptable for the nation."[32] Similarly, the *Joint National Priorities for Critical Infrastructure Security and Resilience* developed in conjunction between the DHS and the critical infrastructure community list "reduce risk to national critical functions" as its first priority.[33]

The question surrounding the NRMC and CISA is: how do they move forward to have the most meaningful impact? To accomplish that, CISA and the NRMC need to make concerted efforts to avoid information sharing and capability silos, thwarting private sector participation due to a lack of incentives, and diminishing the value of working groups and task forces due to a lack of authority or impact. A clear directive to collaborate with the private sector is excellent progress, but without pre-determined authorities or known capabilities, both organizations run the risk of being just another "coordination" center, rather than producing meaningful risk reduction through active collaboration with the private sector.

RECOMMENDATIONS »

To avoid setbacks and make meaningful, near-term progress toward building resiliency across critical infrastructure sectors, the following are recommendations DHS should consider to empower CISA and the NRMC to effectively identify and build capabilities that support national critical functions, using the electric grid and supply chain resilience as a key starting point. In addition, opportunities for the private sector to reduce risk, as well as state-level collaboration, are included throughout these recommendations.

1. **Information Sharing and Transparency.** The focus on supply chain security across critical infrastructure has led many owners and operators to examine the different layers of their supply chain, but too often this examination is linear, preventing questions like: "Who are my suppliers' suppliers?" CISA and the NRMC should consider a roadmap for local and regional electricity systems to holistically evaluate their supply chain to identify capability gaps, weakness, or single points of failure that may otherwise go unnoticed. This empowers owners and operators to better understand the risks to their systems, but also act to mitigate them.

   Further, as CISA and the NRMC continue to better understand the interconnectivity and subsequent interdependencies of critical infrastructure and national critical functions, they should build capabilities to foster a shared situational awareness following incidents with interdependency implications. **Knowledge of an incident and its implications cannot be limited to a single sector or even geographic region but should be evaluated by potential cascading impacts along interdependent connections. This will not only increase the awareness of interdependencies at large but improve response and recovery times and potentially prevent cascading impacts from occurring.**

   Additionally, system owners and operators should take action and work together to understand threat vectors and vulnerabilities as much as possible in order to effectively and efficiently mitigate potential risks. Industry managed organizations like the E-ISAC rapidly share information on new vulnerabilities or known threats, providing its members the opportunity to patch vulnerabilities before being impacted or reduce the consequences of an ongoing event. Many state government agencies as well, beyond just regulators, offer opportunities to collaborate, express challenges and needs, and identify solutions in a risk-free environment.

   Finally, there needs to be a strategic vision for what information sharing and operational coordination looks like in the future. Where do government and the private sector want to be in ten years? What capabilities are needed? These are questions that CISA and the NRMC should look to answer through collaboration with the private sector, and develop a long-term strategy to achieve that vision together.

2. **Secure-by-Design Tools.** Secure-by-design is a concept in which security capabilities are considered and implemented during the system design process and the development of system architecture. Identifying solutions after the fact can come at a higher cost, and potentially be less effective than when incorporated during initial design,[34] and the security capabilities of the system at large may be less able to adapt and grow over time.

Through the NRMC, CISA should invest in the research, development, and deployment of tools to make secure-by-design capabilities more accessible to grid owners and operators, and easier to integrate into standard business processes. This would be a direct partnership between the NRMC and system owners and operators to build a shared awareness of the infrastructure design process and methods to incorporate security controls from the outset and foster a cycle of continuous improvement. This will reduce the inherent risk of individual systems and regional interconnections, but also improve the ability of owners and operators to adapt to new risks and make changes over security technology lifecycles.

3. **Incentivize Secure-by-Design.** To incentivize secure-by-design systems, the U.S. Congress should consider developing additional liability protection for the private sector and critical infrastructure, such as extending Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act coverage to include disruptive cyber events attributed by the U.S. Government to a foreign state actor. The SAFETY Act was originally passed to encourage the development of anti-terrorism products, services, and programs by limiting liability related to the deployment of capabilities that could pass a thorough government vetting process. Coverage is currently limited to terrorism events, and while a number of proposals have been made to extend coverage to cyber incidents, none have passed.[35]

While it is unrealistic to provide coverage for all cyber incidents—companies should take reasonable steps to mitigate risks of reasonably foreseeable harms—providing coverage for cyber events that could be catastrophic is a logical evolution of the SAFETY Act. This status would not be easy to achieve—the vetting process established by the Office of SAFETY Act Implementation is substantial and requires the applicant to prove the utility, effectiveness, and immediate availability of its security capabilities. Nonetheless, investment to build those capabilities and achieve SAFETY Act status will not only help a system owner improve the system's capabilities and reduce liability, but it can also bolster the resilience of local and regional components of the grid.

This may not be unanimously supported, but without a viable alternative to both incentivize and reduce the liability of critical infrastructure owners and operators, the SAFETY Act is currently the best vehicle to accomplish these goals. However, DHS should also consider investing in new opportunities to incentivize the private sector and reduce liability.

4. **Legitimize the Recommendations of the National Risk Management Center.** The NRMC needs to take advantage of early opportunities to both solidify its role and legitimize its value within CISA and DHS. The Executive Order on Coordinating National Resilience to Electromagnetic Pulses is an excellent chance to capitalize one of these opportunities. Electromagnetic pulses (EMPs) have long been a hot-button issue for some government leaders and legislators who want to see immediate action to reduce the likelihood and impacts of what they perceive to be a catastrophic-level risk, but the executive order takes a more considered and measured approach to improve our collective understanding of the risks before developing and implementing new mitigation measures. The NRMC is well positioned to take the lead on a number of the directives within the executive order and would benefit from working with owners and operators and taking a risk-based approach to find the best solutions.

   Further, to ensure the results produced by the NRMC's new working groups and task forces—such as the Information and Communication Technologies (ICT) Supply Chain Task Force—have an impact, DHS should empower the NRMC to adjudicate the Task Force's recommendations and develop national best practices. These should be shared directly from the NRMC to critical infrastructure owners and operators to socialize any new capabilities and begin a dialogue between the critical infrastructure community at large and the NRMC as a new authority and leader in managing risk to national critical functions.

   Additionally, the NRMC should consider further empowering the recommendations of established groups within DHS, such as the President's National Infrastructure Advisory Council (NIAC), whose 2018 report, Surviving a Catastrophic Power Outage: How to Strengthen the Capabilities of the Nation, includes recommendations echoed in this white paper—including, design standards, state and local integration, and developing "a portfolio of incentives." Groups like NIAC—which was chartered to advise the President of the United States through the Secretary of Homeland Security on the security and resilience of critical infrastructure—have positions and insights that should be acted upon and considered as national standards or best practices.

   This would not only begin to solidify the NRMC's role outside DHS to the critical infrastructure community—as well as state and local government communities—but simultaneously add weight to the best practices and recommendations it provides. The products of these early opportunities need to be legitimized by creating actionable results that are recommended and socialized nationally in order to effectively establish the NRMC and its role within CISA and DHS.

5. **State and Local Government Coordination.** DHS already works closely with state and local governments—specifically Homeland Security Advisors, fusion centers, and public safety agencies—but state and local government approaches to supporting critical infrastructure are not consistent. DHS should work with Homeland Security Advisors in each state and territory to establish advisory councils between government officials and critical infrastructure that exist outside of state sunshine laws, giving owners and operators the opportunity to discuss sensitive, homeland security related information outside of a regulatory environment in order to meaningfully discuss challenges and identify potential solutions.

CONCLUSION »

The Department of Homeland Security is making a clear effort to improve the way the United States Government works with the private sector to assess, mitigate, and monitor risk through the creation of the Cybersecurity and Infrastructure Security Agency and the National Risk Management Center. But there needs to be clear definitions, roles, and responsibilities for what that coordination and collaboration looks like in both the short- and long-term. The recommendations outlined herein are an opportunity to not only address risk and build resilience in the electric grid, but to take advantage of an opportunity to build awareness and understanding of national critical functions and interdependencies, work collaboratively and effectively with the private sector, and develop new capabilities that critical infrastructure owners and operators can be incentivized to utilize.

The private sector is eager to be a meaningful, collaborative partner, understand their role with CISA and the NRMC, and want to apply effective risk management practices to prepare for, respond, and recover from incidents of all kinds. DHS should capitalize on this opportunity to reduce the risk to a national critical function through collaborative cross-sector engagement and move forward with a strategy to make a meaningful and timely impact in this unique environment.

ABOUT THE CHERTOFF GROUP »

The Chertoff Group is a global advisory services firm exclusively focused on security and risk management. The Chertoff Group applies security expertise, technology insights and policy intelligence to help clients build resilient organizations, gain competitive advantage and accelerate growth. With a particular focus around security and technology, The Chertoff Group provides a broad array of professional services to help our clients at every stage of the business lifecycle. We leverage our deep subject matter knowledge around important policy matters and security operations to build and execute effective strategies that enable companies to capture new opportunities and create lasting competitive advantage. For those organizations that require tactical security support, we work hand-in-hand with clients to better understand today's threats and assess, mitigate and monitor potential dangers and evolving risks in order to create more secure environments for their business operations. For more information about The Chertoff Group, visit **www.chertoffgroup.com**

FOOTNOTES »

[1] U.S. Energy Information Agency. 2018. *Electricity Explained: How Electricity is Delivered to Consumers.* **https://www.eia.gov/energyexplained/index.php?page=electricity_delivery**

[2] The White House. 2013. *Presidential Policy Directive/PPD-21: Critical Infrastructure Security and Resilience.* **https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil**

[3] U.S. Congress, House, *To Amend the Homeland Security Act of 2002 to authorize the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, and for other purposes*, HR 3359, 115th Congress, 2nd sess. **https://www.congress.gov/115/bills/hr3359/BILLS-115hr3359enr.pdf**

[4] U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency. Last Published Date: November 16, 2018. **https://www.dhs.gov/cybersecurity-and-infrastructure-security-agency**

[5] The White House. 2013. *Presidential Policy Directive/PPD 21: Critical Infrastructure Security and Resilience.* **https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil**

[6] U.S. Energy Information Administration. 2016. *U.S. Electric System is Made Up of Interconnections and Balancing Authorities.* **https://www.eia.gov/todayinenergy/detail.php?id=27152**

[7] U.S. Energy Information Administration. 2018. *The Design and Applicability of Utility—Scale Battery Storage Varies by Region.* **https://www.eia.gov/todayinenergy/detail.php?id=35132**

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

[9] The White House. 2013. *Presidential Policy Directive/PPD 21: Critical Infrastructure Security and Resilience.* **https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil**

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

[11] The White House. 2017. *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.* **https://www.energy.gov/sites/prod/files/2018/05/f51/EO13800%20electricity%20subsector%20report.pdf**

[12] DRAGOS. 2018. *Industrial Control Vulnerabilities: 2017 in Review.* **https://dragos.com/media/2017-ReviewIndustrialControl-Vulnerabilities.pdf**

[13] North American Electric Reliability Corporation. *Critical Infrastructure Protection Standards.* **https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx**

[14] North America Electric Reliability Corporation. CIP-013-1 – *Cyber Security Supply Chain Risk Management.* **https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=CIP-013-1&title=Cyber%20Security%20-%20Supply%20Chain%20Risk%20Management&jurisdiction=null**

[15] U.S. Department of Homeland Security, U.S. Computer Emergency Readiness Team and the U.S. Federal Bureau of Investigation. *Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors* (March 2018), **https://www.us-cert.gov/ncas/alerts/TA18-074A**.

[16] U.S. Congress, Senate, Committee on Homeland Security and Government Affairs. Testimony before a United States Senate Committee on Homeland Security and Government Affairs Hearing on Mitigating America's Cybersecurity Risk by Assistant Secretary Jeanette Manfra (April 2018), **https://www.hsgac.senate.gov/imo/media/doc/Testimony-Manfra-2018-04-24.pdf**

[17] Smith, Rebecca. "Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say." The Wall Street Journal, July 2018. **https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110**.

[18] U.S. Department of Homeland Security, U.S. Computer Emergency Readiness Team and the U.S. Federal Bureau of Investigation. Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors (March 2018), **https://www.us-cert.gov/ncas/alerts/TA18-074A**.

[19] U.S. Department of Homeland Security, U.S. Computer Emergency Readiness Team and the U.S. Federal Bureau of Investigation. Alert (TA18-074A): *Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors* (March 2018), **https://www.us-cert.gov/ncas/alerts/TA18-074A**.

[20] U.S. Congress, House, *John S. McCain National Defense Authorization Act for Fiscal Year 2019*. HR 5515. 115th Congress, 2nd Session. **https://www.congress.gov/bill/115th-congress/house-bill/5515/text**

[21] U.S. Department of Homeland Security, U.S. Computer Emergency Readiness Team and the U.S. Federal Bureau of Investigation. Alert (TA18-106A): *Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices* (April 2018), **https://www.us-cert.gov/ncas/alerts/TA18-106A**

[22] United States, Office of the Press Secretary. "Statement of the Press Secretary." *The White House*, February 15, 2018. **https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/**

[23] U.S. Government Accountability Office. 2018. *Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach.* **https://www.gao.gov/assets/700/694158.pdf**

[24] **Onapsis. 2018. ERP** *Applications Under Fire: How Cyberattackers Target the Crown Jewels.* **https://www.onapsis.com/research/reports/erp-security-threat-report**

[25] U.S. Department of Justice. 2018. *Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information.* **https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion**

[26] U.S. Department of Homeland Security, U.S. Computer Emergency Readiness Team and the U.S. Federal Bureau of Investigation. Alert (TA18-074A): *Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors* (March 2018), **https://www.us-cert.gov/ncas/alerts/TA18-074A**

[27] Verizon Communications. 2018. *2018 Data Breach Investigations Report.* **https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf**

[28] U.S. Computer Emergency Readiness Team. 2017. Security Tips (ST17-001): *Securing the Internet of Things.* **https://www.us-cert.gov/ncas/tips/ST17-001**

[29] U.S. Department of Commerce, National Telecommunications and Information Administration. 2018. *U.S. Department of Commerce, Homeland Security Release Report to President on Promoting Action Against Botnets and Other Automated Threats.* **https://www.ntia.doc.gov/press-release/2018/us-departments-commerce-homeland-security-release-report-president-promoting**

[30] Electricity Information Sharing and Analysis Center. 2016. *Analysis of the Cyber Attack on the Ukrainian Power Grid.* **https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf**

[31] Perlroth, Nicole, and Clifford Krauss. 2018. *A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try*. The New York Times. **https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html**

[32] U.S. Cybersecurity and Infrastructure Security Agency. 2018. *National Risk Management Center*. **https://www.dhs.gov/sites/default/files/publications/NRMC%20100%20Days%20Fact%20Sheet%2020181115_CISA.pdf**

[33] U.S. Department of Homeland Security. 2018. *Joint National Priorities for Critical Infrastructure Security and Resilience.* **https://www.dhs.gov/sites/default/files/publications/Joint-National-Priorities-Fact-Sheet-20180928-508.pdf**

[34] The White House. 2017. *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.* **https://www.energy.gov/sites/prod/files/2018/05/f51/EO13800%20electricity%20subsector%20report.pdf**

[35] Isles, Adam. 2018. *Amend the SAFETY Act to Cover State Actor Cyberattacks.* The Hill. **https://thehill.com/opinion/cybersecurity/382642-amend-the-safety-act-to-cover-state-actor-cyber-attacks**

[36] The President's National Infrastructure Advisory Council. 2018. Surviving a Catastrophic Power Outage: How to Strengthen the Capabilities of the Nation. **https://www.dhs.gov/sites/default/files/publications/NIAC%20Catastrophic%20Power%20Outage%20Study_FINAL.pdf**