Atlantic Council
GLOBAL ENERGY CENTER

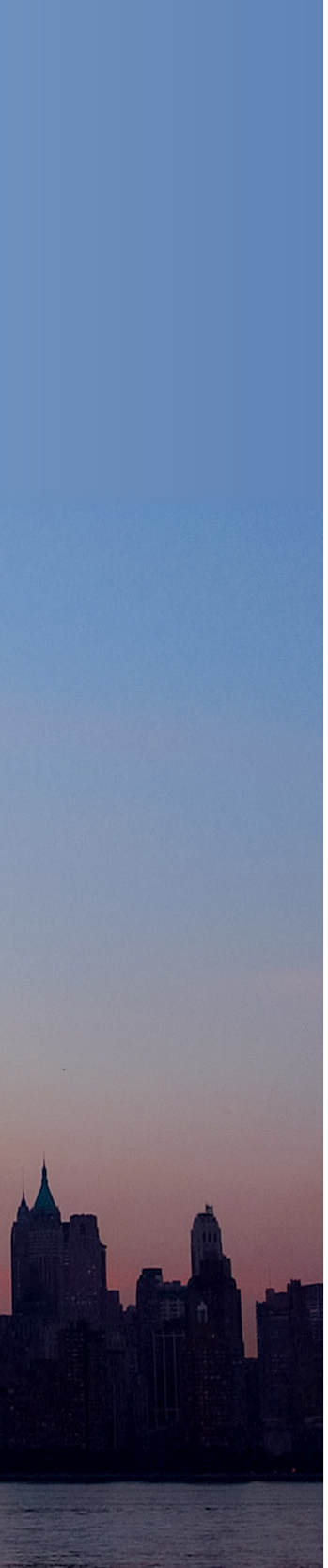
SECURING THE ENERGY TRANSITION AGAINST CYBER THREATS

Report of the Atlantic Council Task Force on Cybersecurity and the Energy Transition

CO-CHAIRMEN
General Wesley Clark
Secretary Michael Chertoff

RAPPORTEURS
Pedro M. Allende
Andrew Gumbiner
John La Rue

CO-DIRECTORS
Randolph Bell
Olga Khakova



Atlantic Council
GLOBAL ENERGY CENTER

The Global Energy Center promotes energy security by working alongside government, industry, civil society, and public stakeholders to devise pragmatic solutions to the geopolitical, sustainability, and economic challenges of the changing global energy landscape.

Atlantic Council
1030 15th Street NW, 12th Floor
Washington, DC 20005

For more information, please visit
www.AtlanticCouncil.org.

The Atlantic Council is grateful to Siemens Energy for its generous support of this project.

ISBN-13: 978-1-61977-240-3

July 2022

Design: Donald Partyka and Anais Gonzalez

Cover: New York City skyline seen at sunrise during a power outage on August 15, 2003. More than twelve hours after the biggest North American power outage in history left huge swaths of the Northeast in sweltering darkness, much of New York and its suburbs were still without electricity. REUTERS/Chip East

Atlantic Council
GLOBAL ENERGY CENTER

SECURING THE ENERGY TRANSITION AGAINST CYBER THREATS

Report of the Atlantic Council Task Force on Cybersecurity and the Energy Transition

Co-Chairmen
General Wesley Clark
Secretary Michael Chertoff

Rapporteurs
Pedro M. Allende
Andrew Gumbiner
John La Rue

Co-Directors
Randolph Bell
Olga Khakova

Table of Contents

Statement by Co-Chairmen

We applaud the Atlantic Council Task Force on Cybersecurity and the Energy Transition for its efforts to craft innovative, rigorous policies that bolster the cybersecurity of the US energy sector. As the energy transition forges on, ensuring the security of the billions of new energy endpoints that will come online is critical. This report is an important step in making sure the private and public sectors are adequately prepared and able to respond to all manner of cyber threats.

The energy sector of the future will rely on digitally native technologies. Increasingly sophisticated systems at the point of generation depend on the Internet of Things, as do energy storage, grid balancing, demand response, and other features of an advanced grid. Each one of these new connections represents a new vulnerability within the energy sector. This makes cybersecurity essential to critical energy infrastructure, and by extension, to national security.

The threat of cyberattacks, which move at the speed of light, must be met with a flexible, resolute response, with the private and public sectors working in concert.

The private sector must provide the requisite investment and training needed to ensure top-to-bottom cyber-secure operations. This includes individual cyber hygiene education, infrastructure investment, real-time monitoring and information sharing, vulnerability assessment across supply chains, and incident reporting protocols.

Government must also work to guarantee preparedness, eliminate duplication, and clarify roles and responsibilities. Federal authorities should look to meld the nimbleness of a streamlined command structure with the robustness of a hierarchy with sector-specific expertise. The goal is to create strong regulatory frameworks that hold the private sector accountable, provide companies with the resources to cultivate in-house cybersecurity, and instill the confidence to engage with public sector bodies and react quickly when cyberattacks strike.

We commend the Task Force on the launch of this report and look forward to future collaboration with the Atlantic Council and other stakeholders on this central issue.

General Wesley Clark

Secretary Michael Chertoff

SECURING THE ENERGY TRANSITION AGAINST CYBER THREATS

Task Force Members & Acknowledgments

The Atlantic Council Task Force on Cybersecurity and the Energy Transition

The Atlantic Council Task Force on Cybersecurity and the Energy Transition comprises civilian and military experts in cybersecurity policy, industrial cybersecurity and control systems, finance, and clean energy. Co-chaired by General Wesley Clark and Secretary Michael Chertoff, the task-force examines the challenges that the energy sector must surmount to attain a secure, reliable future and provides recommendations to establish a more durable cybersecurity framework for the energy transition. The insights, analysis, and recommendations of the Task Force provided the foundation for this study. The conclusions and recommendations of this report do not necessarily reflect all the views of the Co-Chairmen, Task Force members, or other contributors to this project.

- **Jason Bloom**, Head of FICC ETF Strategy, Invesco
- **Andrew Bochman**, Senior Grid Strategist, National and Homeland Security Directorate, Idaho National Laboratory's (INL); Non-Resident Senior Fellow, Atlantic Council Global Energy Center
- **Scott L. Campbell**, Senior Strategic Advisor, Government Relations and Public Policy, Baker Donelson; President, The Howard Baker Forum; Director, The U.S.-Japan Roundtable
- **Helima Croft**, Managing Director, Head of Global Commodity Strategy and MENA Research, RBC Capital Markets
- **Ambassador Paula J. Dobriansky**, Senior Fellow, Harvard University Belfer Center for Science and International Affairs; Vice Chair, Atlantic Council Scowcroft Center for Strategy and Security
- **Justin E. Driscoll**, Interim President and Chief Executive Officer, New York Power Authority
- **Trey Herr**, Director, Cyber Statecraft Initiative, Digital Forensic Research Lab (DFRLab), Atlantic Council
- **Kevin Perkins**, Senior Vice President and Chief Security Officer, Exelon
- **André Pienaar**, Founder, C5 Capital
- **Gil C. Quiniones**, Chief Executive Officer, ComEd; Former President and Chief Executive Officer, New York Power Authority
- **Edward Rhyne**, Executive Principal, Head of Cyber Physical Systems Security, Securonix Inc.
- **Megan Samford**, Vice President, Chief Product Security Officer, Energy Management, Schneider Electric
- **Justin Segall**, Chief Strategy Officer, Uplight
- **Leo Simonovich**, Vice President and Global Head, Industrial Cyber, SIEMENS energy
- **Paul Stockton**, President, Paul N Stockton LLC; Former Assistant Secretary of Defense for Homeland Defense
- **Dave Weinstein**, Chief Information Security Officer, Gro Intelligence; Visiting Fellow, the George Mason University National Security Institute
- **Amit Yoran**, Chairman and Chief Executive Officer, Tenable; Former Director, US-CERT

The Atlantic Council wishes to thank Ameya Hadap, William Loomis, Paddy Ryan, and William Tobin for their work on this project.

Executive Summary

Today, a fleet of digital devices is necessary to balance the power grid and supply electric power to the nation. Energy production and distribution will only increase its reliance on these digital technologies as energy systems continue to shift toward low-emissions and high-efficiency technologies. To deliver reliable, abundant, low-cost, high-efficiency, low-emissions energy, the energy sector must be defended against disruption by cyber threats that range from criminal to geopolitical.

The United States is unprepared to secure this energy transition. Changes in technology, energy sources, and geopolitical considerations have outpaced public policy. Rapid adoption of digitally managed energy assets is transforming the technologies, business models, and policy landscape simultaneously in a matter of years – not decades. These new systems raise the stakes for cybersecurity, even as they strain the regulatory systems designed to ensure reliability in a more centralized, less digitized energy industry.

Cyber exposure of critical infrastructure is a national security risk. Advanced persistent threats attributed to US adversaries have breached American electricity systems in recent years. In 2021, a single ransomware attack prompted the shutdown of the Colonial Pipeline, paralyzing the movement of over half of liquid fuels to the east coast of the United States.

The public and private sectors lack a unified strategic framework to secure energy infrastructure against cyber threats. Existing authorities intended to clarify responsibilities for cybersecurity and assign roles to the Department of Homeland Security, the Department of Energy and other agencies are ambiguous in practice. Ambiguities and gaps in jurisdiction lead to weaker cybersecurity practices, wasted effort by government, confusion for the private sector, and missed opportunities for timely information sharing that would strengthen security.

Aligning government actions can enhance cybersecurity for the energy sector by:

- Clarifying DHS CISA's role as leader of the national unity of effort for critical infrastructure protection
- Reducing duplicative effort and aligning executive and legislative oversight
- Coordinating mandatory and voluntary standards to create a roadmap for future requirements and private sector risk management
- Examining rate-based or tax incentive structures and developing several models to apportion the cost of cybersecurity in the energy sector between owners and operators, consumers, and government

SECURING THE ENERGY TRANSITION AGAINST CYBER THREATS

Because the majority of American energy infrastructure is privately owned, private sector actions are essential to sustaining strong cyber defenses. The private sector must maintain cyber hygiene, and must address supply chain security for physical devices and software used in critical infrastructure. Government can support private sector efforts with clear standards for devices, vulnerability assessment frameworks, and with programs that support testing for physical devices. Government can and should serve as a hub for sharing information on identified threats.

The public and private sector share an interest in recovering quickly when cyber incidents occur. The Infrastructure Investment and Jobs Act, colloquially known as the Bipartisan Infrastructure Bill, included additional investments in cybersecurity for the energy sector, and relatively new programs like the Critical Infrastructure Security Agency's new Cybersecurity State Coordinators and the new Joint Cyber Defense Collaborative show potential for improving incident response. Likewise, technology developments that reduce the cost of cybersecurity monitoring and detection show potential for earlier detection of malicious activity. However, the energy industry would benefit from greater clarity on the thresholds that should prompt government involvement in cyber incident response.

This report's recommendations focus on actions that government can take in support of private sector cybersecurity efforts. These include:

- Recognizing standards organizations that will develop clear guidelines for product and supply-chain security
- Providing penetration testing assistance to certain critical infrastructure assets
- Clarifying and streamlining information sharing practices to foster timely and complete threat information sharing
- Clarifying what constitutes civilian asset response and protection of the kind that DHS CISA can support and what constitutes a more sophisticated matter

The recommendations offered by this Task Force would strengthen American cybersecurity readiness in the energy sector. Aligning federal agencies with the needed authorities for current and future energy markets, would close gaps in uneven regulatory frameworks, and would provide private sector partners with clarity and certainty likely to encourage investment in cybersecurity measures.

1. Introduction: The Energy Transition Depends on Strong Cybersecurity

As the energy transition progresses, renewable and low-emissions energy sources provide an increasing share of US electricity. Renewable sources provided twenty percent of electricity in 2021, comparable to nuclear power's nineteen percent.[1] Electric vehicle sales are growing, and major auto manufacturers have declared their futures are all electric. These technologies are inherently dependent on digital management. Digital controls enable variable power production—such as wind and solar—to sync with the grid. Likewise, distributed generation, battery storage, smart metering, and vehicle charging stations rely on digital management. The energy transition will bring exponential growth to the number of networked devices linked to energy infrastructure—and with it, expanding exposure to cyberattacks.

Existing energy systems provide no haven from cyber threats. In parallel with the energy transition, retrofits are bringing existing critical infrastructure into the digital era. Digital management of critical infrastructure can reduce costs. Among other benefits, digital management optimizes fuel use, enables remote operations, and provides real-time data for monitoring and analysis. Strong return on investment fuels the digitization of existing critical infrastructure in both the public and private sectors.

The future energy sector promises abundant, low-cost, high-efficiency, low-emissions energy—but will be intrinsically dependent on digital technologies.

National security thus requires robust cybersecurity for the energy sector. Modern economies cannot function without reliable fuel and electricity production and distribution; therefore, covertly or overtly disrupting these systems is a desirable capability for any potential adversary. Already, nation-state proxies have been detected deep inside US energy production and distribution networks.[2] Abundant examples both domestically and internationally show that the cyber threat is real. For example, in 2021, a single incidence of ransomware paralyzed the movement of nearly half of transport fuels to the US East Coast in the Colonial Pipeline attack.[3] Industry surveys and statistics indicate the overall number and sophistication of attacks on the energy sector continue to escalate.

Existing efforts to strengthen cybersecurity are insufficient to meet the demands the energy transition will bring. The fragmented, sometimes rivalrous set of institutions regulating and coordinating current cyber defenses leaves many gaps, ambiguities, and weak links, while presenting private-sector actors with overwhelming complexity and uncertainty.

This report examines the challenges that the energy sector must surmount to attain a secure, reliable future and provides recommendations to establish a more durable cybersecurity framework for the energy transition. First, in Section 2 of this report, we provide an overview of the current state of the energy sector in the United States, including the energy transition, its drivers, and the cybersecurity threat environment. Section 3 examines the existing federal policies, laws, and regulations that must be adapted to improve the abilities of both the public and private sector to secure the energy transition. Section 4 examines how both sectors must address key vulnerabilities in existing systems that inhibit industry's ability to scale cybersecurity solutions for a digital energy ecosystem. We believe—with strategic and tactical changes to existing policies, systems, and market drivers—public and private organizations can and must work together to create the conditions that enable the energy sector to achieve and sustain the cybersecurity strength a successful energy transition demands.

1 "Electricity in the United States," US Energy Information Administration, April 19, 2022, https://www.eia.gov/energyexplained/electricity/electricity-in-the-us.php.

2 Rebecca Smith and Rob Barry, "America's Electric Grid Has a Vulnerable Back Door—and Russia Walked through It," *Wall Street Journal*, January 10, 2019, https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112.

3 Michael D. Shear, Nicole Perlroth, and Clifford Krauss, "Colonial Pipeline Paid Roughly $5 Million in Ransom to Hackers," *New York Times*, May 13, 2021, https://www.nytimes.com/2021/05/13/us/politics/biden-colonial-pipeline-ransomware.html.

SECURING THE ENERGY TRANSITION AGAINST CYBER THREATS

2. Energy Transition and Cybersecurity Landscape

The rapid digitalization of the energy sector brings risks. As assets are digitally connected and brought online, each adds a point of exposure for cyberattacks. This presents both technical challenges and business challenges.

No cohesive system secures the energy sector against cyberattacks. Many public and private entities over many decades contributed to creating the complex, interdependent system that delivers energy to consumers today. It is a system in perpetual transition, most recently adapting to the digital revolution.

2.1 The Strategic Importance of the Energy Transition

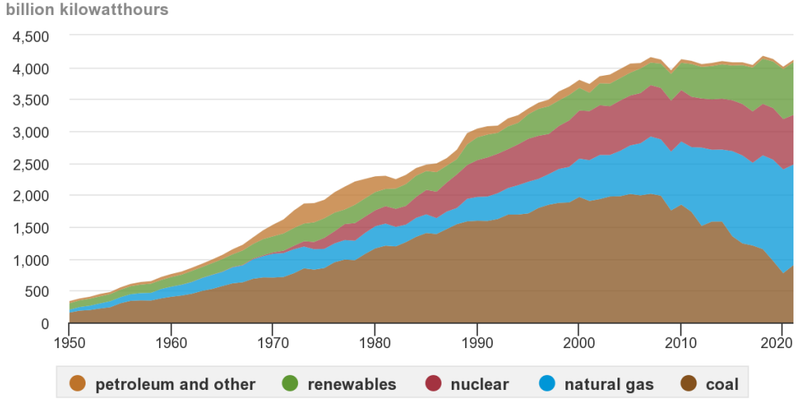
For nearly two centuries, fossil fuels have powered the global economy. Humankind experienced unprecedented levels of prosperity contributing to longer lifespans and economic growth as a direct result of burning oil, gas, coal, and other extracted resources to create electricity, power vehicles, and drive innovation throughout the industrialized world. This prosperity came at a cost—and not all benefited equally from the fossil fuel-based industrial age. Competition over these often-scarce resources fueled domestic and geopolitical conflicts across the globe, financed dictators and human rights abusers, and contributed to climate change.

The Digital Revolution and the Transition from Fossil Fuels

This era of fossil fuels as the backbone of the economy, however, is being disrupted. Technological advances are transforming the production, generation, transmission, and distribution of energy.

While new technologies, including wind turbines and solar power, inherently rely on digital management, digital retrofits also improve the efficiency of existing infrastructure, from thermal generating plants to pipelines and refineries. Policymakers can safely presume that digitalization is per-

US electricity generation by major energy source, 1950-2021



SOURCE: "ELECTRICITY EXPLAINED," US ENERGY INFORMATION ADMINISTRATION, HTTPS://WWW.EIA.GOV/ENERGYEXPLAINED/ELECTRICITY/ELECTRICITY-IN-THE-US.PHP, ACCESSED JULY 5, 2022.

vasive across the future energy sector, regardless of energy source. Advances in the convergence of renewable energy and digital technologies, the volatility of fossil fuel prices, decreasing costs of renewable energy, operational efficiency and lower operating costs are increasingly aligned with the energy transition.[4] The International Energy Agency (IEA) predicts that "potential savings in the electricity sector could total USD 80 billion per year to 2040, or about five percent of total annual power generation costs today."[5] These savings will be felt throughout the industry and will only increase as digitalization expands into transportation markets, smart meters, and other industrial applications.

Improvements in digital and energy technologies make a low- or zero-carbon industry increasingly possible. For example, since 2010, Internet connection speeds have increased exponentially as the costs to enable "Internet of Things" (IoT) business models have dropped, including for sensors, data storage, and analytics platforms. Meanwhile, June 2021 projections from the International Renewable Energy Agency (IRENA) suggest that global renewable power costs will continue to fall in 2022: onshore wind will be between twenty and twenty-seven percent lower the lowest-cost new coal-fired generation option; and seventy-four percent of new solar photovoltaic projects (commissioned in a two-year period through competitive procurement) will have lower award prices than new coal power.[6] In the same way that low costs for natural gas production allowed natural gas to supplant coal as the largest producer of US electricity, renewable sources seem poised to take a major share of electricity production. Related technologies promise to electrify additional sectors, including transportation.

Today, core functions of the energy industry increasingly rely on industrial IoT. These systems digitally connect and control energy assets with operational technology (OT), such as sensors, industrial control systems (ICS), and other physical devices. These devices can then be linked to information technology (IT) and leverage artificial intelligence (AI), machine learning (ML), big-data analytics, and corporate and industrial software. This allows the energy industry—including owners and operators, original equipment manufacturers (OEM), and industrial systems integrators—to reduce costs, improve efficiency, and lower external risk, all while contributing to a greater global good by lowering emissions and reducing pollution. These trends will not only continue but also reshape the energy sector.

Digitalization and the Energy Industry's New Business Model

A post-transition energy sector differs significantly from current infrastructure. Where the historic model for energy distribution relies on large, centralized facilities, such as power plants and refineries, the new wave of technologies enables new business models. Distributed generation and storage, smart metering, and sprawling car-charging networks each rely intrinsically on digitization and network connectivity. Such "prosumer" models, where individuals consume and produce energy, will require millions of networked devices in the hands of consumers, who will be able to sell or purchase electricity from the grid.

These changes are already underway. Significant investments by multinational oil and gas companies in energy assets with low- or zero-emissions are a credible commitment in the direction of decentralization of power generation, greater use of renewables, and the digitally connected ecosystem that enables these shifts.[7] A 2017 report found that investment in digital software for energy and critical infrastructure increased twenty percent annually in the previous four consecutive years.[8] Over a billion industrial devices are expected to connect to critical infrastructure in the very near future.[9]

Regardless of whether a transition is gradual, abrupt, or partial, digital technologies will be a pervasive feature of the energy sector. Economic competition and emissions policies will both contribute to digitization of existing infrastructure and future energy sources. Even in extreme scenarios where new fossil fuel projects cannot compete economically, it is reasonable to expect retrofits aimed at maximizing value extraction from sunk costs of existing infrastructure.

Notably, the enthusiasm for digital technologies, whether renewable or retrofits, is significantly driven by their expected return on investment. In attempting to maximize returns, organizations must balance the uncertain risks of cyberattack against the certain costs of cybersecurity and regulatory compliance. Organizations that underestimate cyber risks will underinvest in prevention. Clear, accurate risk assessments and reduced costs for cybersecurity implementation will tend to strengthen cybersecurity across the sector.

4 Melissa N. Diaz, "U.S. Energy in the 21st Century: A Primer—Congress," Congressional Research Service, *CRS Reports*, March 16, 2021, crsreports.congress.gov/product/pdf/R/R46723.

5 International Energy Agency, *Enhancing Cyber Resilience in Electricity Systems*, IEA Publications, 2021, 13, accessed February 16, 2022, https://www.iea.org/reports/enhancing-cyber-resilience-in-electricity-systems.

6 "Majority of New Renewables Undercut Cheapest Fossil Fuel on Cost," IRENA Press Release, June 22, 2021, https://www.irena.org/newsroom/pressreleases/2021/Jun/Majority-of-New-Renewables-Undercut-Cheapest-Fossil-Fuel-on-Cost.

7 "3 Digital Trends Which Will Transform the Energy Industry: IEF," International Energy Forum, July 28, 2021, www.ief.org/news/3-digital-trends-which-will-transform-the-energy-industry.

8 IEA, *Digitalization and Energy,* IEA Publications, 2017, www.iea.org/reports/digitalisation-and-energy.

9 *Cisco Annual Internet Report (2018–2023) White Paper*, Cisco, Updated March 9, 2020, www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html.

A Jaguar I-Pace electric vehicle is recharged at Waymo's operations center in the Bayview district of San Francisco, California. Such electric car-charging networks rely on digitization and network connectivity. REUTERS/Peter DaSilva

2.2 Cyber Risks of the Energy Transition

According to the IEA, "the number of 'significant' cyber incidents reported globally has risen dramatically in recent years."[10] Utilities were second only to the banking industry in terms of these incidents in 2018, losing an average of "USD 17.8 million per company per year, up eighteen percent from 2017."[11]

Sophisticated attacks have been discovered in American energy infrastructure in recent years. Although most are preventable with straightforward cyber hygiene measures, such cyberattacks rise to the level of national security threats. For example, in 2019, US government investigators made public that Russian intrusions had been discovered in several major electricity generation facilities, including plants holding contracts to supply emergency power to military bases.[12] These intrusions were designed to remain dormant within target systems, allowing foreign agents to tamper with critical infrastructure at the time of their choosing. In 2021, a ransomware attack prompted the Colonial Pipeline operators to halt operations for a week. More recently, in April 2022, the Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (DHS CISA) issued a warning that an advanced persistent threat was targeting specific industrial devices used in natural gas facilities, and once inside a network, would enable attackers to move laterally to other systems.[13]

10 A. M. Jaffe, *Energy's Digital Future: Harnessing Innovation for American Resilience and National Security* (New York: Columbia University Press, 2021), 21. The IEA defines "significant" incidents as those with losses of more than USD one million related to a cyberattack.

11 Jaffe, *Energy's Digital Future*, 21.

12 Smith and Barry, "America's Electric Grid Has a Vulnerable Back Door."

13 "Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," CISA, Released March 15, 2018, Revised March 16, 2018, https://www.cisa.gov/uscert/ncas/alerts/TA18-074A.

This illustration shows a laptop displaying a warning in Ukrainian, Polish, and Russian after a major cyber attack. REUTERS/Valentyn Ogirenko/Illustration

Even temporary disruptions short of significant physical damage could prove catastrophic. Imagine, for example, a federal election day in which electrical outages affect polling locations in a large share of competitive districts. As this report will discuss in later sections, meeting the current threat environment requires both a whole-of-government approach and coordination with the private sector.

Until recently, cybersecurity has been thought of as an information technology (IT) problem. This common paradigm leaves the soft underbelly of operating technology (OT) systems exposed. Current and future cybersecurity challenges bridge IT and OT, requiring strategies that address both. Indeed, the recent Norsk Hydro and Colonial Pipeline attacks show that successful IT attacks can stop production, even when OT is not directly targeted. The differences between attacks on IT and OT infrastructure matter for both prevention and consequence. OT communications protocols are not typically encrypted. Attacks on OT can be embedded in hardware or software supplied by third-party vendors. Attackers may be able to pose as valid users sending commands that are difficult to differentiate from legitimate commands. Only with broader context can defenders distinguish, for example, normal turbine operations from commands that will start and stop a turbine so rapidly it shakes to pieces. Detecting OT attacks requires contextual information and knowledge of the safe parameters for operations. Meanwhile, tools used in IT to prevent attacks are less available in OT. For example, applying software patches typically requires production outages, greatly increasing the cost and decreasing the frequency of updates compared to IT.

Lengthy disruptions to energy infrastructure would have significant consequences for Americans and for the US economy. The Colonial Pipeline's seven-day outage—despite almost immediate payment of the demanded ransom—caused panic buying, raised fuel prices, and required presidential intervention. The incident provides ample warning that longer disruptions in energy production and distribution are highly undesirable.

Timeline of software and malware attacks on ICS since 2009

2009 | Shodan

A search engine built to find Internet-connected devices maps and collects software specifications for over 100 million devices, including industrial control systems.

July 2010 | Stuxnet

An attack targeting Programmable Logic Controllers (PLCs) and SCADA systems disrupts centrifuge operations and causes physical damage at Iranian nuclear facilities.

October 2010 | Metasploit

The first SCADA exploit is added to the open-source penetration testing tool Metasploit, making industrial control systems a viable target for malicious users.

August 2012 | Shamoon

Approximately 35,000 computers owned by Saudi Aramco are infected by a computer virus that uploaded files to the attacker then rewrote master boot records, rendering infected computers unusable.

December 2015 | Ukraine Power Grid 1 (BlackEnergy)

Attackers cut power to 230,000 residents of western Ukraine. Investigations concluded initial compromises allowed reconnaissance and eventual access to SCADA remote operations controls.

December 2016 | Ukraine Power Grid 2 (Industroyer or CrashOverride)

Targeting an electric substation north of the Ukrainian capital, attackers successfully used malware specifically designed to attack energy infrastructure to cause a massive blackout across Kyiv.

January 2017 | Shamoon 2

The same disk-wiping malware used in 2012 was detected on several Saudi Arabian government agencies and linked institutions aimed at disrupting equipment, services, and data at energy and chemical companies.

August 2017 | Triton/Trisis

Malware that had successfully breached industrial safety control systems at a Saudi Arabian petrochemical plant. Triton/Trisis is designed to prevent operators from safely shutting down emergency systems to intentionally cause physical damage and loss of life.

December 2020 | SolarWinds

After more than a year undetected, malicious code injected into a software supply chain is discovered in IT systems used by over 30,000 organizations, including U.S. government agencies.

February 2021 | Oldsmar Wastewater Treatment Facility

Attackers gained access to the industrial control systems at a wastewater treatment facility in Oldsmar, FL, in an attempt to adjust the levels of sodium hydroxide in the city's drinking water.

May 2021 | Colonial Pipeline

In the largest cyberattack against U.S. oil and gas infrastructure, the criminal group DarkSide launched a ransomware attack against Colonial Pipeline's computer systems and IT infrastructure. Colonial Pipeline was forced to shut down operations, which supply approximately 45 percent of the jet fuel and gas to the East Coast.

2.3 The Energy Sector and the Current Cyber Paradigm

How the energy sector handles the coming billions of new connections to its assets will determine whether they continue to reward investment or become a massive liability. Greater reliance on digital technologies in the post-transition energy supply chain will heighten the need for strong cybersecurity in US energy infrastructure. Meanwhile, the organizations responsible for distribution include many small and midsize businesses, co-ops, and municipal utilities with relatively small budgets for cybersecurity.

As owners and operators evaluate this increasing threat landscape, they have increased spending for cybersecurity, but not necessarily for security-related technologies. Estimates from 2020 place global spending on IT and cybersecurity in the energy sector at USD 32 billion in 2028, up from USD 19 billion today, yet only about seven percent of this is expected to be for security-related applications and these are often not for OT-specific technology.[14]

The energy sector, and critical infrastructure sectors more broadly, are highly diverse with countless technical, market, and state and local regulatory differences. The bulk of the US electricity sector is privately owned and operated.[15] The US electricity sector alone has approximately 3,000 utilities that operate under different regulatory authorities depending on utility size, location, and business model.[16] These entities range in size from behemoths like NextEra, Dominion Energy, Duke Energy, and Southern Company,[17] all the way down to small municipal utilities and rural electric cooperatives that represent about a quarter of electricity production in the United States.[18] Some are publicly traded, with a duty to maximize shareholder value. As energy generation and transmission infrastructure becomes more complex, it also requires intensive capital investments.[19] Diverse ownership, inherited complexity, and high costs of capital investment mean there is no one-size-fits-all cybersecurity solution.

Existing regulatory models that oversee today's energy systems, such as centralized power generation, oil and gas distribution through pipelines, and transmission and distribution systems, must be designed to scale cybersecurity solutions to meet the dynamic pace of change in the industry. Meanwhile, new regulatory approaches are required to address oversight gaps like integrating distributed energy resources (DERs) into the electric grid, enabling grid-scale batteries for energy storage, and linking prosumers to the electricity system with at-home EV charging. Addressing energy cybersecurity in the United States, then, is not a matter of revising today's national strategy. It requires reconciling the goals of private-sector energy infrastructure owners for profit through uptime with those of the government for ensuring uptime as a pillar of national security.

To do so, the United States needs these many public and private entities to work together.

14 Jaffe, *Energy's Digital Future*, 17.

15 Federal Emergency Manangement Agency, "Critical Infrastructure Paper," n.d., accessed January 12, 2022, https://www.fema.gov/pdf/about/programs/oppa/critical_infrastructure_paper.pdf.

16 D. Shea, "Cybersecurity and the Electric Grid: The State Role in Protecting Critical Infrastructure," National Conference of State Legislatures, January 2020, https://www.ncsl.org/research/energy/cybersecurity-and-the-electric-grid-the-state-role-in-protecting-critical-infrastructure.aspx.

17 Mark F. Sundback, Bill Rappolt, and Andrew P. Mina, "Electricity Regulation in the United States: Overview," Sheppard Mullin LLP, Thomson Reuters Practical Law (website), law as of July 1, 2020, n.d., https://content.next.westlaw.com/8-525-5799?__lrTS=20210922170104235&transitionType=Default&contextData=(sc.Default)&firstPage=true.

18 "Municipal Cooperative Utilities," Chan Lab, University of Minnesota (website), n.d., accessed February 4, 2022, https://chan-lab.umn.edu/munis-and-co-ops.

19 "Energy," in *2021 Infrastructure Report Card*, American Society of Civil Engineers, March 25, 2021, 43-53 https://www.infrastructurereportcard.org/cat-item/energy/.

3. Preparing Federal Cyber Policy for the Energy Transition

US Department of Homeland Security election security workers monitor screens in the DHS National Cybersecurity and Communications Integration Center (NCCIC) in Arlington, Virginia, US. REUTERS/Jonathan Ernst

Securing the energy transition requires aligning complex federal policies, bureaucracies, and programs to both secure critical infrastructure from cyberattacks and meet the needs of an evolving energy industry. US cyberspace strategy and federal energy policy were designed with vastly different objectives, incentives, and stakeholders in mind. This system was never envisioned to balance connected matters of national or economic security across the government and the private sector. The Cyberspace Solarium Commission summarized this well in 2020: "the United States lacks a clear, comprehensive, publicly declared doctrine that incorporates all of the instruments of power to address less-than-catastrophic attacks on public and private networks in cyberspaces."[20] To contribute effectively to shared cyber defenses, private-sector actors need an improved framework.

The future regulatory model must improve in two overarching areas. First, providing clear, coordinated and consistent rules that apply across the energy sector's various oversight bodies. Second, creating a flexible system focused on risk-based requirements and appropriate incentives—both carrots and sticks. With these requirements met, the energy sector must take ownership over their role in securing critical infrastructure.

20 *Cyberspace Solarium Commission Report*, March 2020, 14, https://www.solarium.gov/report. The commission, per the executive summary, was chartered by the 2019 National Defense Authorization Act and charged with answering two questions: What strategic approach will defend the United States against cyberattacks of significant consequences? And what policies and legislation are required to implement that strategy?

3.1 The Federal Policymakers Shaping Cybersecurity for the Energy Transition

Security policy for the energy transition sits at the nexus of three primary federal bureaucracies: DHS CISA, the Department of Energy (DOE), and the Federal Energy Regulatory Commission (FERC). As the energy transition has changed the cybersecurity landscape, DHS, DOE, and FERC have continued working without greater strategic realignment of their congressional authorizations or appropriations. Reordering this multiplayer environment is essential to aligning regulations, standards, funding, and government programs to meet present and future challenges.

Centralized Cyber Policy for Critical Infrastructure: DHS and CISA

Federal cybersecurity policymaking for the energy sector is organized based on the National Infrastructure Protection Plan (NIPP). Now nearing twenty-five years old, the NIPP divides roles, responsibilities, policy, and operational authorities between a central bureaucratic authority and sixteen critical infrastructure (CI) sectors identified by the government as essential to the national interest. Since the creation of DHS, the department has assumed the lead role for CI protection, which includes the energy sector. DHS works with the Sector Risk Management Agencies (SRMAs)—for example, the Department of Energy—to help the private sector voluntarily "address cyber vulnerabilities, threats, and hazards"[21] in specific sectors.

Congress created CISA in 2018 to centralize the federal government's civilian cybersecurity responsibilities under DHS so it could provide a "complete systemic risk picture" over all critical infrastructure, including cybersecurity for the energy sector.[22] Placing CISA as the federal lead for cyberspace policy has helped focus US operational and coordination capabilities. Its broad mission space allows a wide latitude to act and coordinate across federal policy areas, but also requires CISA to coordinate closely with SRMAs, which provide the relevant industry and technical expertise.

Congress recently created the national cyber director (NCD), following the recommendation of the US Cyberspace Solarium Commission.[23] The NCD serves as the "principal advisor to the President on cybersecurity policy and strategy."[24] Currently helmed by Chris Inglis, the NCD is tasked with "preparing the response by the federal government to cyberattacks and cyber campaigns of significant consequence across federal departments and agencies with responsibilities pertaining to cybersecurity and with the relevant private sector entities."[25] The NCD is new enough that in-depth commentary is premature, but this appears to be a positive development.

Energy Sector Cyber Policy: DOE

DOE serves as the SRMA for the energy sector. Unlike some SRMAs, DOE holds a supporting role, rather than a regulatory role. The department funds research and development (R&D), organizes and participates in training and education events to inform the private sector, and supports private-sector efforts through a series of programs on threat and vulnerability detection, and information sharing.

As a whole, DOE's work to perform its SRMA function has met the challenge placed on it by the executive and legislative branches. Indeed, the department has taken the laboring oar to build relationships and trust, deploy its vast R&D capabilities to address complex problems, develop programs to support robust threat identification and information sharing with the private sector, and stands ready to deploy at a moment's notice to support assessment and recovery efforts after natural and man-made disasters. DOE's work and partnership with the private sector has been critical in protecting assets, but has relied heavily on voluntary participation, and does not always have universal reach.

The Energy Sector's Largest Federal Regulator: FERC

FERC is tasked with regulating the transmission and sale of electricity and natural gas in interstate commerce and the transmission of oil by pipeline in interstate commerce. Under the Energy Policy Act of 2005 (EPAct),[26] FERC received the authority to regulate the reliability of the bulk electric system (BES), which includes the ability to set cybersecurity standards. Under this authority, FERC certified the North American Electric Reliability Corporation (NERC), a voluntary self-regulatory not-for-profit corporation, as the Electric Reliability Organization (ERO) set forth in EPAct, to develop

21 National Association of State Energy Officials, *Enhancing Energy Sector Cybersecurity: Pathways for State and Territory Energy Offices*, 2020, accessed January 11, 2022, 10, https://www.naseo.org/data/sites/1/documents/publications/Final%20NASEO_Cybersecurity%20Report%20(062020).pdf.

22 B. Humphreys, *Critical infrastructure: Emerging Trends and Policy Considerations for Congress*, July 8, 2019, accessed January 17, 2022, https://www.everycrsreport.com/reports/R45809.html.

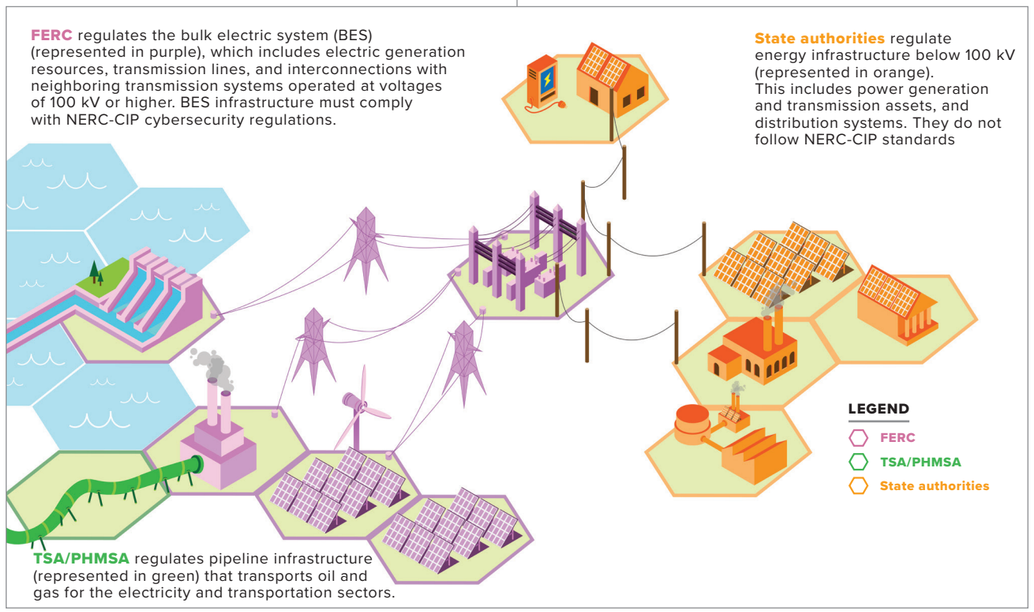
23 6 U.S.C. §1500 (National Cyber Director, enacted as part of the William M. "Mac" Thornberry National Defense Authorization Act for Fiscal Year 2021), https://uscode.house.gov/view.xhtml?path=/prelim@title6/chapter6/subchapter1&edition=prelim.

24 6 U.S.C. § 1500.

25 6 U.S.C. § 1500.

26 Energy Policy Act of 2005, Pub. L. 109-58 (2005).

This graphic provides a simplified diagram of the primary US regulatory authorities mentioned in this report; it does not cover all entities or circumstances.



SOURCE: Authors

critical infrastructure protection (CIP) cybersecurity reliability standards in use today by NERC, FERC, and DOE.

Through NERC and NERC-CIP requirements, the federal government has implemented a regulatory framework for the bulk electric system. Compared to other critical infrastructure sectors, FERC—through NERC—has instituted the most comprehensive requirements, standards, and systems. These include standards and requirements for incident reporting, information protection, systems identification and categorization, supply chain management, and information sharing.[27] To meet NERC-CIP's current regulatory requirements, BES organizations must comply with fourteen cybersecurity and physical security measures, which in turn include more than thirty specific technical and operational standards.[28]

3.2 The Energy Regulatory Landscape

The energy sector's regulatory structure is highly decentralized. Critically, some SRMAs maintain regulatory functions while others do not. As a result, SRMA programs, regulations, and standards apply to certain energy sector owners and operators, but not others.

For the purposes of this report, we primarily focus on the FERC, the largest federal regulatory agency for the electricity sector; DHS's Transportation Security Administration (TSA); and the Pipeline and Hazardous Materials Safety Administration (PHMSA) at the Department of Transportation. TSA and PHMSA share responsibility over pipelines as co-SRMAs. FERC and TSA set up contrasting examples of regulatory approaches and provide key lessons for developing a more consistent regulatory approach.[29]

27 Hearing on Keeping the Lights On: Addressing Cyber Threats to the Grid, Before the House Subcomm. on Energy, 116th Cong. (2019) (statement of James B. Robb, President and Chief Executive Officer, North American Electric Reliability Corporation), https://www.nerc.com/news/testimony/Testimony and Speeches/House Energy and Commerce Cyber Hearing Testimony 7-12-19.pdf.

28 A. Pogorelov, "Achieving Resilience while Fulfilling NERC CIP Requirements," Tripwire (blog), Association for Data and Cyber Governance, June 16, 2021, Accessed April 24, 2022, https://www.adcg.org/resources/achieving-resilience-while-fulfilling-nerc-cip-requirements/.

29 Other federal regulators, such as the Nuclear Regulatory Commission (NRC) or the Environmental Protection Agency (EPA), do not feature prominently in this report, but do play a critical role in establishing an interconnected framework between the federal government and private sector.

DIVERGENCE IN MANDATORY REPORTING REQUIREMENTS

The Colonial Pipeline attack and a cyberattack on a wastewater treatment facility in Oldsmar, Florida, elucidate the need for a consistent set of standards for incident reporting requirements that can be applied across government. The two attacks occurred in separate critical infrastructure sectors and therefore were held to different regulatory requirements based on their assigned SRMA.

Early in 2021, the small wastewater treatment facility in Oldsmar was breached by a cyberattack that altered the levels of lye in the city's water supply. An employee identified the cyber exploitation responsible for tampering with the city's water supply before the attack caused serious damage and contacted authorities.[I] However, this attack could easily have gone unnoticed to the broader critical infrastructure community.

Under EPA requirements, incident reporting for wastewater treatment facilities is voluntary—much like TSA.[II] It is further remarkable because it is an example of an attack on a small-scale critical infrastructure operator, where cybersecurity is typically less sophisticated and federal reporting requirements do not apply. Absent oversight enforcement mechanisms that require investments, many such utilities in resource-starved cities and municipalities will remain weak links in critical infrastructure cybersecurity because they cannot justify investments to customers and state regulators.[III]

The Colonial Pipeline, regulated by TSA, did not face regulatory requirements to report the cyberattack underway. At the time of the attack the pipeline industry was held to "voluntary cyber and physical defense guidelines," without incident reporting requirements.[IV] Even with federal incident-response efforts underway several days into the cyber breach, Colonial Pipeline had not provided full and comprehensive technical details about the attack to authorities.[V] Had Colonial Pipeline been a part of the bulk electric system (BES) regulated under FERC, it would have been penalized more than USD one million per day for this lack of incident reporting.

The lack of uniform incident reporting principles across federal regulatory bodies highlights the inconsistent approach of baseline rules that critical infrastructure industries must follow.

Following the Colonial Pipeline intrusion, TSA issued two successive security directives that required owners and operators of TSA-designated critical pipelines to report confirmed and potential cybersecurity incidents to CISA, and designate a cybersecurity coordinator to be available twenty-four hours a day, seven days a week, in addition to certain protective measures.[VI]

I F. Robles and N. Perlroth, "'Dangerous Stuff': Hackers Tried to Poison Water Supply of Florida Town," *New York Times*, February 9, 2021, https://www.nytimes.com/2021/02/08/us/oldsmar-florida-water-supply-hack.html.

II Environmental Protection Agency, "Supporting Cybersecurity Measures with the Clean Water State Revolving Fund," Fact Sheet, EPA Publication 817F21007, https://www.epa.gov/sites/default/files/2021-05/documents/cwsrf_cybersecurity_fs_final_0.pdf.

III Selena Larson and Lauren Zabierek's study paints a picture of the weakness: "Many critical infrastructure organizations, including those responsible for the distribution and safety of our water systems, are deep in technical debt. That is, computers and other assets often rely on outdated software and firmware that either cannot be upgraded due to restrictions on functionality or financial support. Additionally, many of the organizations are small and underresourced—one or two people might oversee system administration and IT functions as well as the security of everyone's computers in the office and the plant, or the organization might rely heavily on third-party vendors or city staff for security operations." See S. Larson and L. Zabierek, "It's Time to Regulate Water and Wastewater Cybersecurity—Here's How," Harvard Kennedy School's Belfer Center for Science and International Affairs, Analysis & Opinions, November 3, 2021, https://www.belfercenter.org/publication/its-time-regulate-water-and-wastewater-cybersecurity-heres-how.

IV D. Shea, "Cybersecurity and the Electric Grid: The State Role in Protecting Critical Infrastructure," National Conference of State Legislatures, January 2020, https://www.ncsl.org/research/energy/cybersecurity-and-the-electric-grid-the-state-role-in-protecting-critical-infrastructure.aspx.

V Eric Geller and Martin Matishak, "A Federal Government Left 'Completely Blind' on Cyberattacks Looks to Force Reporting," *Politico*, May 15, 2021, https://www.politico.com/news/2021/05/15/congress-colonial-pipeline-disclosure-488406.

VI Transportation Security Administration, "DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners. and Operators," TSA News Release, July 20, 2021, https://www.tsa.gov/news/press/releases/2021/07/20/dhs-announces-new-cybersecurity-requirements-critical-pipeline.

Jurisdiction Gaps in Federal Regulatory Structure

FERC's mandatory NERC-CIP standards contain structural and operational gaps that leave the electricity sector vulnerable to current and future threats because of a lack of jurisdiction beyond the BES. Notably, only between ten percent and twenty percent of the US electricity system falls under mandatory regulations overseen by FERC and issued by NERC—in part because the EPA excluded distribution systems from FERC reliability standards and mandates.[30] As a report from MIT's Energy Initiative, entitled The Utility of the Future, bluntly puts it: the United States currently has "no single central authority for cybersecurity preparedness."[31] In practical terms this means that significant portions of US energy infrastructure is unregulated by the federal government, as is the case in Hawaii and Alaska. The federal government also lacks jurisdiction over large and critically important distribution systems like New York City's.[32]

There are issues of interconnectivity across the energy system as well. While FERC and NERC oversee the bulk power system's cybersecurity standards and compliance measures, regulatory oversight over other parts of the energy sector are either lacking—as is the case with the distribution system—or are regulated under vastly different rules and requirements because they align to another subsector, such as gas pipelines. There is no better example of the divergence in regulatory requirements within the energy sector than the recent Colonial Pipeline attack. At the time of the ransomware attack on Colonial Pipeline, the TSA, the industry's cyber regulator, had no mandatory incident reporting requirements for possible cyberattacks. Instead, it relied on a "voluntary" compliance model for incident reporting. This stands in stark contrast to FERC's mandatory reporting requirements for possible and real cyber breaches, which impose steep financial penalties should companies fail to comply.

Challenges with NERC-CIP's Strategic and Tactical Approach

NERC-CIP standards are often focused on tactical issues, rather than considering the long-term view of the energy transition. The NERC-CIP approach has too often prioritized immediate security needs without considering implementation challenges. Compliance challenges frequently cited by industry include: manual processes required by regulation cannot keep up with the speed of attacks; NERC-CIP requirements tend to increase areas of existing oversight without an abrogation process; requirements and expectations can be overly challenging to decipher; constantly documenting and updating internal compliance protocols is financially and operationally costly; and finally, NERC-CIP's regulatory requirements are challenging to implement across an expanding and decentralized ecosystem.[33]

For an energy sector that increasingly leverages industrial IoT technologies, NERC-CIP standards lack the level of granularity that energy sector owners and operators need to make long-term investments or decisions to connect and integrate decentralized systems and critical infrastructure. The current set of enforceable regulations is woefully behind, as importantly, NERC-CIP offers virtually no guidance for what OT or ICS products are deemed secure. Indeed, NERC CIP does not reference standards with respect to specific products or equipment that an entity may consider investing in and connect to the grid. A baseline standard is much needed; a model developed by the International Society of Automation (ISA) and the International Electrotechnical Commission (IEC), known as ISA/IEC 62443, has shown promise as a standard that can fill the current void. Without mandatory guidance, energy companies often implement in industrial IoT systems the National Institute of Standards and Technology's Cyber Security Framework (NIST CSF), published in 2014 to fill gaps in federal regulation.[34] In an effort to support the energy sector, DOE recently led a collaborative effort to align NIST CSF best practices to IT/OT security practices. This culminated in the July 2021 release of version 2.0 of its Cybersecurity Capability Maturity Model (C2M2), which helps organizations evaluate and improve their cybersecurity programs and strengthen their operational resilience.[35]

30 Glen Andersen et al., *Modernizing the Electric Grid: State Role and Policy Options*, National Conference of State Legislators, November 2019, 17, download available at https://www.ncsl.org/research/energy/modernizing-the-electric-grid-state-role-and-policy-options.aspx.

31 I. Perez-Arriaga and C. Knittel, *Utilty of the Future*, Massachusetts Insitute of Technology, MIT Energy Initiative in collaboration with the Institute for Research in Technology at Comillas Pontifical University, December 2016, 64, 2022, https://energy.mit.edu/wp-content/uploads/2016/12/Utility-of-the-Future-Full-Report.pdf.

32 Richard J. Campbell, *Evolving Electric Power Systems and Cybersecurity,* Congressional Research Service, Report R46959, November 4, 2021, 2, https://crsreports.congress.gov/product/pdf/R/R46959.

33 Robert Walton, "Cybersecurity and the Distributed Grid: A Double-Edged Sword," Utility Dive, May 21, 2018, www.utilitydive.com/news/cybersecurity-and-the-distributed-grid-a-double-edged-sword/523285/. Attackers typically do not target what is protected by NERC-CIP, making it important to ensure new infrastructure can be systematically included. As the build-out of distributed energy resources grows, so will the surface area of entry points and vulnerabilities on the grid.

34 "Managing IOT Risks in Power and Utilities," KPMG, 2019, assets.kpmg/content/dam/kpmg/us/pdf/2019/07/managing-iot-risks-in-power-and-utilities.pdf.

35 "Cybersecurity Capability Maturity Model (C2M2)," US Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response (website), https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2.

State Regulatory Authorities

Because the electricity distribution system falls beyond the authority of FERC, the electricity distribution system in the United States is primarily regulated at the state level. This includes approximately 2,000 public power utilities, 800 cooperatives, and 170 investor-owned utilities,[36] subject to rules from state utility commissions as well as local legislative bodies and oversight boards.

State or local control over energy regulations and standards leaves a significant portion of the United States' electric grid without a unified approach to cybersecurity, and without baseline standards that apply throughout the country. That does not mean that state governments have not focused on the issue. In 2019, sixteen states took up fifty actions to improve cybersecurity for the electricity subsector,[37] and recent years have seen states pass legislation on information sharing, cybersecurity planning, cybercrime, and funding and training for cyber hygiene.[38]

3.3 A Federal Policy Framework for the Energy Transition

To secure the energy transition, the federal government must adjust structurally, reset its relationship with the private sector, and reduce the confusion and turf wars caused by overlapping, unclear authorities. From an interagency perspective, the federal government must embrace the difference in roles between DHS's CISA and SRMAs.

Ambiguity Over Roles and Responsibilities

Ambiguity still exists between CISA's authorities and other SRMAs—in this case DOE—in terms of leading and coordinating broad operational authorities, roles, and responsibilities within the interagency environment and externally with the private sector. DOE and CISA both remain very active in the energy cybersecurity and incident response space, and institutional incentives tend to result in duplicative efforts. The Fiscal Year (FY) 2021 budget, which was enacted, allocated more than USD 18 billion to cybersecurity and related activities (including DOD, USD 9.84 billion; Homeland Security, USD 2.6 billion; DOE, USD 665.6 million), a budgetary incentive to seek a cybersecurity role.

The executive and legislative branches have created duplicative mission sets. For energy sector cyber policy, the mission sets of DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER), CISA, and NSA are inching closer to one another. For example, DOE CESER's Cybersecurity Mission has expanded to closely duplicate the work of CISA's National Risk Management Center and the National Security Agency's Cybersecurity Division. For example, a proposed DOE-run Integrated Security Center (DISC) in Denver would have provided a space for "cybersecurity analysts to develop and provide critical information to the sector and to coordinate with DOE's Office of Intelligence and Counterintelligence."[39] At best, duplicative efforts dilute the impact of spending on cybersecurity; at worst, they generate confusion and delay in moments of crisis. For example, regulated private-sector entities are currently obliged to report cyber incidents to multiple agencies—potentially wasting hours at times when minutes matter.[40]

Focusing Mission Sets for the Energy Transition

The federal government must reenvision the roles and responsibilities between DHS and SRMAs that interface with the energy sector by clarifying conflicting directives and authorities that arise between DHS and the SRMAs.

Regulatory frameworks must be designed for distributed and decentralized business models—and federal oversight cannot stop at the BES system without coordination with state regulators. The federal government is well positioned to craft new regulatory frameworks to match technologies in use, and then work with states and the private sector to implement a baseline approach. DOE can understand both the interdependencies and the differences in operation between electric generation and oil and gas production, but also grasp that pipelines and wind farms have some similarities where common regulation could be helpful. Coordinating with CISA, FERC, EPA, PHMSA, and TSA to reach common ground would mean that entities can look at a single regulation instead of reconciling several regulations.

Each SRMA, in coordination with the broader set of stakeholder departments, could then develop targeted supplemental regulation—building on baseline standards—narrowly tailored to the context of each subindustry or to address a specific issue of concern. Such regulation should be easier to understand and implement across the eighty-five percent of critical infrastructure that is owned by the private sector. DHS

36 Shea, "Cybersecurity and the Electric Grid."

37 Shea, "Cybersecurity and the Electric Grid," 2.

38 Shea, "Cybersecurity and the Electric Grid," 4.

39 US Department of Energy, *Transition 2020 Issue Papers*, 4, https://www.energy.gov/sites/default/files/2021-10/2%20-%20Issue%20Papers.pdf.

40 For example, the digital version of form OE-417, with an estimated time burden of 1.8 hours, includes a mechanism for broader distribution to NERC, the Electricity Information Sharing and Analysis Center (E-ISAC), and CISA—but only if the submitter checks a box for each.

CISA has a role as coordinator of the national unity of effort to protect critical infrastructure. SRMAs such as DOE have roles as the leading experts in their subject matter and must be positioned as the strategic and technical support agency for the energy sector. This is a notional expansion of SRMA's statutory role but a necessary one in our view. DHS CISA should not duplicate or interfere with DOE's deep relationships with the energy sector or its leadership on R&D for the energy ecosystem's cybersecurity. By the same token, the DOE should not duplicate DHS CISA's coordinating role by serving as the hub for energy sector information sharing: for information sharing to address cross-sectoral effects, it must occur at the national level, not the sector level. DOE is a necessary and integral party, but DHS CISA should lead coordinating functions; when DOE duplicates coordination it causes confusion within both government and the private sector.

Pricing Cybersecurity into Utility Rates

Public-sector leaders at all levels seeking to scale industrial cybersecurity solutions and help asset owners secure CI can look to the early days of the energy transition as a model to support innovation. Since the mid-2000s, the public and private sector together have scaled up the development and deployment of renewable energy technologies using market-based approaches. The government has also been instrumental in growing the public-private partnerships (PPPs) that supported the renewable energy industry. This includes everything from establishing test beds, to workforce development and STEM education programs, and even to commercializing technologies with US national laboratories.

The energy sector is an extremely capital-intensive sector. Adding robust industrial cybersecurity technology, personnel, and training is a significant cost. Much of the energy industry's focus is on building new assets, or retrofitting existing assets to meet emissions and efficiency goals. In 2019, the electric power industry invested over USD 120 billion in capital expenditures, encompassing investment in such areas as generation, transmission, distribution, and regulatory compliance.[41] This dwarfs other capital-intensive industries such as telecommunications services, with USD 39.2 billion in capital expenditures, or the automotive industry, with USD 44 billion.[42]

Energy companies of all sizes and business models will need cybersecurity technologies. Yet, under most existing federal and state regulatory frameworks, utilities are limited by statute in their ability to invest in cybersecurity compared to other energy infrastructure investments, such as physical assets.[43] A straightforward but politically challenging proposition would be to use the energy sector's existing business model to put a price on security. According to a recent McKinsey & Company study on the energy sector's vulnerability to cyber threats, a Duke Energy estimate in a 2019 rate-case argument put the cost of upgrading its entire OT network at more than USD 100 million. Investment in OT systems will be essential to securing the energy transition with capabilities to monitor and detect threats and identify weakness and vulnerabilities. Put another way, energy companies build in costs to physically secure critical infrastructure with fencing, cameras, and personnel—so why not do the same for cybersecurity?

In 2021, FERC began to explore narrow approaches to justifying rate-case adjustments for limited investments for enhanced cybersecurity protections. The proposal incentivized utilities to exceed mandatory CIP requirements and implement NIST security protocols that would go beyond minimum standards. [44] In return, FERC proposed that utilities be able to defer cost recovery or wave investment costs for these upgrades. While encouraging, the limited scope of the initial proposal, and its narrow applicability to utilities regulated under FERC, makes evaluating such an approach difficult for more widespread adoption.

A Cyber Loan Program and Investment Bank

Several investment models exist to help energy sector companies, especially those with smaller balance sheets, scale existing cybersecurity technologies. Private lenders can be reluctant to finance technology deployment due to the risk profile or the time horizon of the investment. In certain instances, government could step in to support ventures with direct financing or loan guarantees for proj-

41 Edison Electric Institute, "Delivering America's Resilient Clean Energy: Electric Power Industry Outlook," EEI Wall Street Briefing, PowerPoint Presentation, February 9, 2022, accessed February 16, 2022, https://www.eei.org/issues-and-policy/wall-street-briefing.

42 Aswath Damodaran, "Capital Expenditures by Sector (US)," Data Set Provided by Kerschner Family Chair in Finance Education, Stern School of Business, New York University, last updated January 2022, accessed February 16, 2022, https://pages.stern.nyu.edu/~adamodar/New_Home_Page/datafile/capex.html.

43 A report by the Vermont Law School, commissioned by Protect Our Power, states: "Cybersecurity investments are a different type of utility investment that [sic] a traditional utility investment in infrastructure. Cybersecurity investments have shorter lifespans in the range of 3-7 years instead of the 30 to 40-year lifespan of poles and wires. Investment is needed in a combination of software, hardware, and training which all have different characteristics and rate treatments. A compounding factor is that the risk of redundancy is greater because of the rate of change in technologies and the pace at which threats emerge and are identified. Adding to the risk element is that cybersecurity protections are less likely to produce offsetting revenue increases or expense reductions, although they might be paired with other technology that does." M. James et al., *Improving the Cybersecurity of the Electric Distribution Grid,* Institute for Energy and the Environment, Vermont Law School, November 2019, accessed April 13, 2022, https://www.vermontlaw.edu/sites/default/files/2019-11/VLS%20IEE%20-%20Cybersecurity%20Report%20-%20Phase%202.pdf. Protect Our Power is an independent, nonpartisan, nonprofit organization.

44 Cybersecurity Incentives, Proposed Rule of Federal Energy Regulatory Commission, 86 Fed. Reg. 8309 (February 5, 2021), https://www.federalregister.gov/documents/2021/02/05/2021-01986/cybersecurity-incentives; this notice was first published on the FERC website on December 17, 2020, https://www.ferc.gov/media/e-2-rm21-3-000.

ects that align with government objectives. A government cyber bank or low-interest cyber fund could help qualifying companies, including critical infrastructure owners and operators, obtain financing at low rates—which also could include loan forgiveness provisions tied to metrics—to advance the state of cyber readiness. The centralizing function of a bank of this kind, much like the International Development Finance Corporation, would help to manage the program holistically instead of having piecemeal programs spread across the federal bureaucracy that are hard to track and manage.

The Department of Energy's Loan Programs Office is one such example.[45] Since 2009, DOE LPO has provided USD 35 billion in financing and loan guarantees to over thirty projects in areas such as energy infrastructure, nuclear construction, and utility-scale solar and wind generation.[46] This model could be leveraged for scaling cybersecurity technologies and upgrading assets. Such a program could allow small and midsize organizations to implement leading security solutions as quickly as possible.

With regard to supply chain vulnerabilities for physical components from certain nation states, there is a role for a cyber bank here as well. Recognizing that energy sector investments are generally capital intensive and amortized over a long life, addressing supply chain concerns with a "rip-and-replace" approach is unrealistic—unless government can step in to reduce or assume some or all of the costs of the vulnerable equipment.

Targeting Tax Policy

Tax policy is another potential avenue to address this cost burden.[47] Current federal tax incentives specific to cybersecurity come primarily in the form of preexisting R&D tax incentives, when applicable. These incentives were not targeted at cybersecurity initiatives specifically, and do not constitute a prescriptive system of incentives for the sector.[48] Offering tax incentives to encourage regulatory compliance and support organizations with the costs associated with increasing cybersecurity measures is commonplace in other industries. Such incentives can be tailored to specific objectives and include benchmarks and metrics by which to measure success for taxpayers, investors, and organization executives.

3.4 Recommendations

Realigning the focus of DHS and DOE should aim to create complementary roles and responsibilities. Such a realignment would allow DHS to focus on coordination, cross-sector analysis, risk mitigation, and incident response activities. Meanwhile, DOE can focus on building deeper sector-specific expertise to add more value through its support than it ever could through building duplicative systems. The private sector's ability to secure the connected assets that power the energy transition hinges on the federal government improving its authority structure and operational model. Clearly defined roles and responsibilities among federal agencies dictate the sector's preparedness, resilience, and ability to respond to cyberattacks—both within government and for owners and operators.

Establishing Bureaucratic Roles and Responsibilities

- The president should update or abrogate dated executive mandates such as Presidential Policy Directives (PPDs) 21 and 41, which form the basis of the interagency relationship for critical infrastructure protection and incident response. This update should crystalize DHS CISA's role as leader of the national unity of effort for critical infrastructure protection such that all SRMAs are in a supporting role.
- Congress should reduce duplicative efforts, including aligning the jurisdictional bounds of Senate and House committees to minimize areas of overlapping oversight to the extent possible, working to abrogate inconsistent or duplicative authorities between departments and agencies, and reducing duplicative funding and appropriations.
- Congress should direct the Government Accountability Office to study the feasibility of centralizing energy-specific pipelines under the authority of FERC with DOE serving as SRMA due to the critical dependencies of the energy sector.

45 DOE Loan Programs Office (home page), https://www.energy.gov/lpo/about-us-home.

46 DOE Loan Programs Office (home page).

47 "From a policy perspective, government can send many signals," said Schneider Electric Energy Management's Megan Samford, vice president and chief product security officer, in an interview for this report. "One that resonates with equipment manufacturers, owners and operators, and integrators is the ability to offset capital expenditures that advance the cybersecurity of the sector against their tax liability. If a company can choose between paying taxes or making investments to better secure their infrastructure—whether that means testing equipment for potential problems, hiring a reputable vendor to conduct penetration testing, replacing legacy systems that are no longer supported, for example—the company chooses better security 100 percent of the time."

48 US Department of the Treasury, *Treasury Department Report to the President on Cybersecurity Incentives Pursuant to Executive Order 13636*, n.d., https://www.hsdl.org/?abstract&did=750516.

SECURING THE ENERGY TRANSITION AGAINST CYBER THREATS

Setting an Effective Investment Framework for Energy Cybersecurity

- FERC, NERC, and NIST should coordinate mandatory and voluntary standards to create a road map for future requirements and give the private sector more latitude and flexibility to manage risk.
- DHS CISA and SRMAs should consider a baseline set of standards for cybersecurity applicable to organizations of various sizes and criticality that may be extended by those SRMAs with regulatory authority to address industry-specific issues and concerns.
- DOE and FERC in coordination with state regulatory bodies should study rate-based or tax incentive structures and develop several models to apportion the cost of cybersecurity in the energy sector between owners and operators, consumers, and government.

4. Improving Cybersecurity across the Energy Marketplace

Aligned with these improvements in the federal cyber policy landscape is an urgent need for improvements in how the private sector secures its critical technologies and works with the public sector to respond to the most accurate and timely threat information. This section addresses the private sector side of this landscape, addressing the threat of supply chain compromise, need for better collective defense and information sharing, calls for improved incident response coordination, and the opportunity for markets to get smarter about cyber risk.

Holding tanks are seen in an aerial photograph at Colonial Pipeline's Dorsey Junction Station in Woodbine, Maryland, on May 10, 2021. A single ransomware cyberattack prompted the shutdown of the pipeline system for a week. REUTERS/Drone Base

4.1 Cyber Hygiene to Sustain Supply Chain Security

The Colonial Pipeline attack offers a stark warning on cyber hygiene. An audit conducted three years before the 2020 incident characterized Colonial's cyber defenses as "a patchwork of connected and secured systems."[49] In congressional testimony on June 8, 2021, Colonial Pipeline CEO Joseph Blount revealed that attackers had exploited the fact that Colonial used an old virtual private network (VPN) system that lacked basic cyber hygiene like multifactor authentication.[50] Reports published after the Colonial incident suggest that the company voluntarily skipped TSA's audit of its computer networks in the year preceding the attack.[51]

Proper cyber hygiene makes digital supply chain attacks significantly more difficult to execute. Cyber hygiene includes basic steps like asset visibility and management, two-factor authentication, changing passwords regularly, and closing dormant profiles, but it may also include more rigorous protocols to check for exploitable bugs in software systems and unpatched vulnerabilities. In a 2021 report, IBM identified a USD 2.3 million differential in average data breach costs between companies with high and low levels of compliance failures.[52]

The digital backbone running today's energy and critical infrastructure sectors relies heavily on self-assessment and implementation to maintain cyber hygiene. While CISA, NIST, and a host of other governmental and industry bodies provide digital security playbooks, best practices, and voluntary frameworks, implementing these resources is left to owners and operators, OEMs, and systems integrators—unless they work with the federal government.

4.2 Supply Chain Security amid the Energy Transition

The risk of digital supply chain attacks is amplified in the energy sector. Energy infrastructure is expensive, and by necessity is distributed in far-flung facilities. Even if vulnerabilities are discovered, the mitigation can be costly and complex, requiring equipment to be replaced and, oftentimes, technicians to travel hundreds of miles to effectuate updates. Supply chain risks include an overwhelming number of third parties. In 2016, researchers looking in depth at a group of twenty utilities found that on average each utility had 3,647 total active suppliers, thirty-nine strategic relationships, and 140 suppliers that accounted for eighty percent of total external outlay.[53] Attackers who find the core business well-defended may instead target a known business partner, gain a foothold, and move laterally once inside the targeted supply chain.[54] Without durable and concrete frameworks and coordination with policymakers, private-sector companies are left with uncertainty regarding standards on physical devices, digital security, cyber hygiene, and more.

Getting Smart About Physical Standards

Establishing cybersecurity standards and protocols that can serve large swaths of the industry would help reconcile the dynamism of the energy transition with the relatively slow pace of government rulemaking. Outside of mandatory regulations, energy sector owners and operators, OEMs, and systems integrators follow a patchwork of government and industry-endorsed guidelines, best practices, and frameworks.

The voluntary approach has its benefits in allowing companies to craft policies and solutions that meet the unique attri-

49 F. Bajak, "Tech Audit of Colonial Pipeline Found 'Glaring' Problems," Associated Press, May 12, 2021, https://apnews.com/article/va-state-wire-technology-business-1f06c091c492c1630471d29a9cf6529d.

50 S. Kelly and J. Resnick-ault, "One Password Allowed Hackers to Disrupt Colonial Pipeline, CEO Tells Senators," Reuters, June 9, 2021, https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/.

51 D. Uberti, "Colonial Pipeline Missed Requested Security Review before Hack," *Wall Street Journal*, May 26, 2021, https://www.wsj.com/articles/colonial-pipeline-missed-requested-security-review-before-hack-11622067027.

52 IBM, *Cost of a Data Breach Report 2021*, IBM with research by Ponemon Institute, July 2021, https://www.ibm.com/security/data-breach.

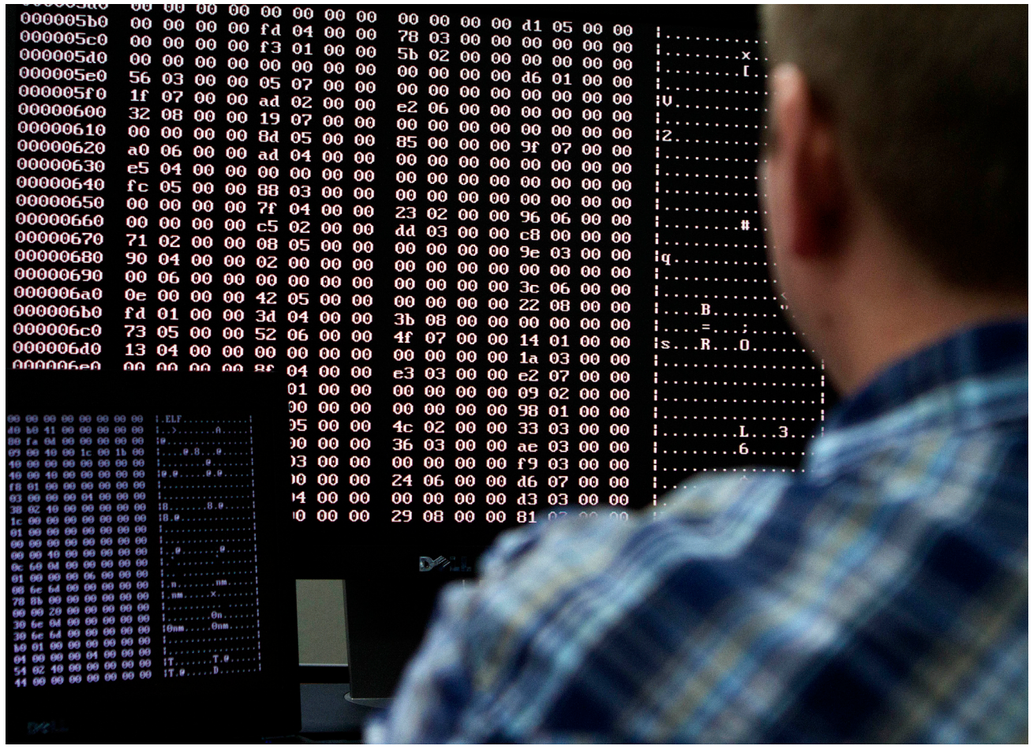
53 Steve Livingston et al., "Managing Cyber Risk in the Electric Power Sector," *Deloitte Insights*, Deloitte, January 31, 2019, https://www2.deloitte.com/us/en/insights/industry/power-and-utilities/cyber-risk-electric-power-sector.html; and Tim Schmidt, "Three Critical Procurement Best Practices for Electric Utilities: Are You Doing These?," https://www.procureware.com/three-procurement-best-practices-utilities/.

54 Richard J. Campbell, "*Evolving Electric Power Systems and Cybersecurity,*" Congressional Research Service, November 4, 2021, https://crsreports.congress.gov/product/pdf/R/R46959.

butes of the business model. Currently, the energy industry relies heavily on two voluntary models for product and component security standards: the US government's NIST CSF and a model developed by the ISA/IEC 62443. Compared to NIST CSF, which can be made universal across sectors and heavily used in the United States, the ISA/IEC 62443 standard provides more prescriptive recommendations which address specific security issues in ICS and OT, ranging from the areas of organizational policy to system technologies and product technical requirements.[55]

Voluntary approaches have serious drawbacks as well. There is no consistent framework to secure existing and future energy systems. Unable to rely on a known standard or a regulatory body, each organization must expend effort assessing its own supply chain or accept increased risk. With only voluntary frameworks to secure the physical-digital divide, supply chain cybersecurity leaves many weak, unprotected attack pathways into energy sector companies, suppliers, and government partners. Unfortunately, the energy sector in the United States has never been subject to a system wherein OT products connected to the grid must meet an enforceable set of standards beyond the most rudimentary and basic principles of cybersecurity. In general, the federal government has not interfered or provided guidance regarding the acceptability—or unacceptability—of specific products or equipment connected to critical infrastructure.

With the exception of two now-rescinded executive orders (EOs)—EO 13920 and the DOE's corresponding Prohibition Order, enacted in 2020 and 2021—the government allows companies to acquire and deploy technologies of their choosing.[56] The two orders, however, marked a shift in industrial policy for express national security purposes. The EOs precluded the installation of equipment on the grid where a foreign adversary has an interest. The now defunct orders



An analyst examines code in a cyber security defense lab at the Idaho National Laboratory in Idaho Falls, Idaho, September 29, 2011. REUTERS/Jim Urquhart

55 Ron Brash, "The Ultimate Guide to Protecting OT Systems with IEC 62443," Verve Industrial (blog), February 28, 2022, verveindustrial.com/resources/blog/the-ultimate-guide-to-protecting-ot-systems-with-iec-62443/.

56 Exec. Order No. 13920, 85 Fed. Reg. 26595 (May 4, 2020), www.federalregister.gov/documents/2020/05/04/2020-09695/securing-the-united-states-bulk-power-system; and Prohibition Order, US Department of Energy, 86 FR 533 (January 6, 2021), www.federalregister.gov/documents/2021/01/06/2020-28773/prohibition-order-securing-critical-defense-facilities.

caused significant challenges for foreign manufacturers already deeply integrated into the US energy sector's supply chain.

Regulators should be wary of issuing guidance that will swiftly become obsolete. Rather, a system of accountability tailored to an industry baseline of standards, such as ISA/IEC 62443 as a complement to NIST CSF, offers a pathway appropriate to the rapid changes seen in cybersecurity. Given that ISA/IEC 62443 is in use in Europe as a component of the Common Regulatory Framework on Cybersecurity, voluntary adoption of this internationally certified standard has wide risk-reduction incentives for businesses operating around the world, however it is not yet the global status quo.[57]

Testing for Cybersecurity Up and Down the Supply Chain

Digital supply chains also require protection. Although not focused on the energy sector, the recent SolarWinds attack illustrated an attack method that injected malicious code into the software shipped by a trusted supplier.[58] Relatively little work has been done to create or enforce clear standards for digital supply chains in the energy sector, a notable gap in existing cybersecurity frameworks.

Managing today's supply chain risk pales in comparison to the task ahead. The foreseeable future will add over a billion endpoints, many built by new and nascent manufacturers, with software made by a smorgasbord of developers. Currently, there are entities in the private and public sector that provide cybersecurity testing and certifications, which could serve as a baseline framework for a future certifications ecosystem. A program at DOE's Idaho National Laboratory (INL) called Cyber Testing for Resilient Industrial Control Systems (CyTRICS), tests industrial control systems and OT equipment on a range of cybersecurity criteria. CyTRICS partners include Schneider Electric and Hitachi Energy (formerly known as Hitachi ABB Power Grids) and have signed agreements to provide equipment for analysis and testing.[59] The value to all parties is evident: government and asset owners and operators have advance warning of vulnerabilities with potential mitigations before incidents occur, and manufacturers have an additional level of testing on their products that allows them to be proactive instead of reactive in serving their customers.

Scaling CyTRICS and programs like it will help the sector fill a notable gap. The resources of the National Laboratories are insufficient to address testing at scale, but the federal government could establish standards and certify other organizations to conduct testing. Under the right framework, the private sector can provide the resources to scale testing. The government can encourage large, global OEMs to participate in such programs through tax incentives, which would help to cover the significant R&D costs that manufactures invest in ensuring their products are secure by design before they reach the market. Meanwhile, private testing and certification entities, such as TÜV SÜD AG, already provide IoT security testing and certification service based on the NIST CSF[60] and ISA/IEC 62443.[61] The government and insurance companies can incentivize or cover the cost of product security to encourage secure supply chains.

4.3 Improving Information Sharing for Collective Defense

The convergence of cybersecurity and the rapidly evolving digital energy ecosystem requires developing systems of collective defense that meet the needs of both the government and the private sector. Every stakeholder in the energy ecosystem has a role and responsibility in quickly sharing actionable information and threat intelligence, and coordinating across various federal, state, and private sector entities to respond to incidents. In a robust collective defense system, the government would support the private sector in defense and grow a network of connective cybersecurity tissue between owners and operators, OEMs, and systems integrators. Quickly sharing information is one of the

57 "UN to Integrate ISA/IEC 62443 into Cyber Framework," *InTech* (magazine), International Society of Automation, January 31, 2022, https://www.isa.org/intech-home/2019/january-february/departments/united-nations-commission-to-integrate-isa-iec-624. Separately, in her interview for this report, Schneider Electric Energy Management's Samford said: "Today, the ISA/IEC 62443 standard is the most cited OT cybersecurity standard in the [United States] next to the NIST CSF. It is also the gold standard on OT cybersecurity in the European Union and in other major economic hubs like Singapore. Widespread adoption of ISA/IEC 62443—with enthusiastic government support for adoption of all controls—would put in place an OT cybersecurity that is aligned along the roles of owners and operators, equipment manufacturers, and system integrators and against the end state security levels required for types of equipment resulting in an integrated security road map from design to implementation and operation. And from a US perspective, certification to the ISA/IEC 62443 standard is a viable and preferable alternative to government regulation, which has historically lagged technological advancement."

58 Fireye, "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor," Mandiant (website), December 13, 2020, Product Name Updated May 2022, https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.

59 "DOE CESER Partners with Schneider Electric to Strengthen Energy Sector Cybersecurity and Supply Chain Resilience," DOE Office of Cybersecurity, Energy Security, and Emergency Response CESER (website), September 23, 2020, https://www.energy.gov/ceser/articles/doe-ceser-partners-schneider-electric-strengthen-energy-sector-cybersecurity-and; and "DOE Announces Hitachi ABB Power Grid's Participation in CyTRICS Program," DOE CESER, April 29, 2021, https://www.energy.gov/ceser/articles/doe-announces-hitachi-abb-power-grids-participation-cytrics-program.

60 Michael Fagan et al., "Foundational Cybersecurity Activities for IOT Device Manufacturers," Computer Security Resource Center, National Institute of Standards and Technology, May 29, 2020, csrc.nist.gov/publications/detail/nistir/8259/final.

61 "IEC 62443 Industrial Cybersecurity Certification," TÜV SÜD (website), www.tuvsud.com/en-us/industries/manufacturing/machinery-and-robotics/iec-62443-industrial-security. Accessed July 5, 2022.

DATA SHARING SILOED BY BUREAUCRACY, SECTOR, AND MANUAL SYSTEMS

For government to share information on threats and vulnerabilities in real-time or near real-time, it must ingest information, distribute information across federal agencies, perform rapid analysis, and disseminate actionable results to owners and operators quickly. Yet, the actual information-sharing process is often cumbersome and fails to produce actionable intelligence.

For the electricity subsector to share information through DOE, a statute mandates reporting of cyber incidents via form OE-417, which incorporates FERC's NERC CIP 8-6 reporting requirements that are more closely coordinated with CISA.[I] The time burden for energy companies to fill out this form is not insignificant: the stated completion time is 1.8 hours, and the form is submitted by email, requiring a human being to process it upon receipt.[II]

The form itself is built as a regulatory check list of items that is not automatically shared with interagency partners, rather than one that seeks more qualitative and quantitative information that may be relevant for situational awareness or ongoing threats. The OE-417 form creates a mechanism for broader distribution to NERC, E-ISAC, and CISA. Despite the focus on interagency information sharing, the OE-417 offers only permissive—and not mandatory—information sharing with CISA, NERC, and E-ISAC, if and only if the submitter checks a box. This stands in contrast to the NERC CIP 8-6 standard, which automatically shares reported incidents to FERC, CISA, and the E-ISAC.

I 15 U.S.C. § 761 et seq; US Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, Electric Disturbance Events (DOE-417), https://www.oe.netl.doe.gov/oe417.aspx.

II US DOE, Electric Disturbance Events (DOE-417).

most important ways the government and owners and operators can mitigate cyberthreats, and enables defenders to address threats in real time. Unfortunately, this sharing is often bogged down by a complex intragovernmental system riddled with duplicative actors and processes making it difficult, costly, and inefficient for the private sector to cooperate with their government counterparts.[62] Information and threat intelligence must move at the speed of attackers. This means IT and OT data should be analyzed and treated based on the risk it poses to ICS, supervisory control and data acquisition (SCADA), or software systems.

To establish a system of collective defense, the government must make it easy for owners and operators to share data from their networks, both technically and legally, and then provide them with synthesized and helpful information back to secure their networks. Automated information sharing platforms can significantly improve sharing between the federal government and state, local, tribal, and territorial (SLTT) authorities, and within industries. Automated threat information would also improve situational awareness, allowing authorities to expand data sharing within and among sectors and include supply chains.[63]

Understanding Information Sharing

The federal government's decentralized authority structure and operational model for information sharing often leaves operators and owners without usable or timely information. Without clarified liability protections and robust technical and financial support for monitoring and detection capabilities, owners and operators will remain disincentivized or unable to share information with government partners.

62 "The US government is failing the private sector by not providing actionable information, which requires appropriate distribution and access, including downgrading classification," said Brian J. Cavanaugh, senior vice president of American Global Strategies and former senior director for resilience policy on the National Security Council, in an interview for this report conducted on February 17, 2022. "Meanwhile, the private sector is failing the US government by restricting access to proprietary information, which prevents the government from understanding the scope and footprint of key organizations that own and operate critical infrastructure and their associated vulnerabilities. Together these issues present a feedback loop that perpetuates ignorance and ineffective assumptions, preventing the adequate assessment of risk and timely actions to prevent disruptions."

63 Constance Douris, *Cyber Threat Data Sharing Needs Refinement*, Lexington Institute, Future of the Power Grid Series, August 2017, 13, https://www.lexingtoninstitute.org/cyber-threat-data-sharing-needs-refinement/.

SECURING THE ENERGY TRANSITION AGAINST CYBER THREATS

Source	Information Type	Information Flow	Recipient
DHS Homeland Security Information Network (HSIN)	Information sharing on threats, including how analysts, investigators and private sector partners collaborate	⟷	Vetted members of federal, SLTT and private sector. State EEACs may request access
FBI InfraGard Program	Threats, attacks vulnerabilities, risk mitigation	⟷	Private and public vetted membership and local chapters
State Energy Emergency Assurance Coordinators	Potential energy supply disruptions, Incidents, events, and responses (all-hazards)	⟷	DOE/CESER other states in the impacted region
Multi-State ISAC (Primary focus is SLTT-operated computer networks)	Threats, attacks vulnerabilities, risk mitigation	⟷	State fusion centers and chief information officers (CIO)
Electric Utilities	OE-417 Electric Disturbance Events report	→	DOE/CESER
Electric Utilities	Intelligence sharing, threats, attacks	⟷	E-ISAC private sector and public utilities
Electric Utilities	Threats, attacks	⟷	NERC via critical infrastructure protection incident reporting; DHS NCCIC
Electric Utilities	Threats, attacks	→	State PUCs that have adopted rules or procedures
Oil and Natural Gas (ONG) Industries	Information sharing, threats, attacks	⟷	ONG ISAC private sector only
Natural Gas Transmission and Distribution Companies	Information sharing, threats, attacks	⟷	DNG ISAC private sector only
Pipelines Operators	Incidents of abnormal operations and SCADA systems	⟷	Pipeline and Hazardous Materials Safety Administration (PHMSA)
DHS National Risk Management Center (NRMC)	Strategic and cross-cutting understanding of risk analysis and planning	⟷	Federal, SLTT, and private/public energy sectors including state fusion centers
DHS National Cybersecurity and Communications Integration Center (NCCIC) US-CERT and ISC-CERT	Information sharing, threats, attacks, and collaboration.		Federal, SLTT, and private/public energy sectors including state fusion centers
EnergySec monthly threat briefing webinar	Threats, attacks vulnerabilities		State PUCs and other approved attendees

This table outlines the key flows of cyber threat and risk data between senders and recipients and, importantly, whether the flow is unidirectional or bidirectional. The structures and entities involved are highly segmented and siloed by industry, and fragmented by government, private sector, or nonprofit groups. Siloed information thus fails to provide a complete picture to government agencies or owners and operators, and fails to deliver full situational awareness.

SOURCE: National Association of State Energy Officials

Presently, two overlapping—and often competing—models exist for information sharing with the federal government. All critical infrastructure organizations, including the energy sector, can share information with CISA under a hub-and-spoke model that collects information centrally and then coordinates with relevant SRMAs. Alternatively, energy sector stakeholders can share information with DOE in a decentralized model using its own technologies and programs before it is passed on to CISA or other SRMAs.[64] The result is parallel tracks and unnecessary complexity for critical infrastructure and energy sector organizations.

Liability Concerns

For energy sector owners and operators, OEMs, and systems integrators, there also is a prevailing fear that their own data might be used against them by regulators or law enforcement officials should an event occur. Private-sector organizations fear that this exposure could lead to serious criminal or civil liabilities for accidently disclosing personally identifiable information (PII) or sensitive corporate information, which could negatively impact an organization's reputation or position in the market.[65]

Private-sector data collected through information sharing programs are a necessity for the federal government to lead its national unity effort on critical infrastructure protection and energy sector coordination. Under the Critical Infrastructure Information (CII) Act of 2002, the federal government attempted to address the private sector's legal concerns by codifying robust liability protections, under a program called Protected Critical Infrastructure Information (PCII), which allowed critical infrastructure organizations to voluntarily share information with DHS with some protections from disclosure and use in civil proceedings.[66] In 2015, Congress created a separate designation for Critical Energy Infrastructure Information (CEII) under the FAST Act, vesting in DOE and FERC the ability to grant liability protections to energy sector organizations that voluntarily shared information with the department and commission. That same year, Congress also codified some of the most robust liability protections for sharing of "cyber threat indicators, defensive measures, and information relating to cybersecurity threats" with government to date in the Cybersecurity Information Sharing Act of 2015 (CISA 2015).[67]

To encourage participation, liability protections are a must. The federal government must first and foremost reconcile the CEII framework supported by DOE and CISA 2015 and PCII frameworks supported by DHS in favor of one common framework for liability protection. While existing programs are designed to alleviate the private sector's concerns with sharing data and information with the federal government, there are limitations of the protections themselves should a private-sector organization fail to meet strict conditions under each program. For example, organizations sharing information with the federal government under PCII must strip all PII from all data before sharing. An organization's failure to comply with this stipulation—even if accidental—could risk losing liability protections. While some organizations can automatically and easily take out PII, others must perform the task manually.[68]

Worker protections also have a role to play. Across the energy sector, there is a culture of safety. Workers are often encouraged to inform management of unsafe working conditions or potential dangers. Workers also have clear whistleblower protections and can turn to federal authorities when owners and operators fail to address unsafe conditions in a timely manner. The safety culture, however, does not appear to extend to cybersecurity. Despite the existence of various whistleblower statutes that can apply in many scenarios, workers observing risky cybersecurity practices do not appear to raise concerns as often. They also appear to hesitate to disclose concerns beyond their organization. Cultural improvement is important. Organizations cannot remedy issues they do not know about. Formalizing the appropriate reporting pathways to call attention to cybersecurity risks within critical infrastructure would align individual and organizational interests with national security interests.

Organizing for Failure?

There are also organizational issues. Much of the energy sector's existing collective defense framework remains siloed by industry. For decades, nonprofit industry groups served as the connective tissue between government and the private sector to help facilitate information sharing, coordinate across the industry during incidents, and share best practices. Electric utilities were organized around collaborating with one industry group, whereas the oil and gas pipeline industry would coalesce around another group.

Energy Sector Coordinating Councils (SCC) and Information Sharing and Analysis Centers (ISACs) were established under the NIPP structure to serve as an intermediary between the private sector and its assigned SRMA.[69] These industry organizations were developed to serve as the connective tissue between industry and government, and from industry to industry. Just as the system was first conceived in 1998, the industry-led coordinating councils today remain "self-organized and self-governed councils that enable critical infrastructure owners and operators, their trade associations, and other industry representatives to interact on a wide range of sector-specific strategies, policies, and activities."[70] Under this framework, network data were treated as industry specific, rather than in terms of how a threat or vulnerability could impact any energy asset or the broader ecosystem—whether it be a solar farm, an electric substation, or a gas pipeline.

Today, the ISACs such as E-ISAC remain membership-based organizations and, by extension, membership-focused organizations, open to investor-owned or publicly owned utilities "responsible for the management, distribution of electricity."[71] For companies that fit neatly into the ISAC structure, such as large utilities, this coordination system can provide significant benefits to both companies and the federal government to grow strong relationships between participating entities.[72] However, the membership-based and siloed nature of the E-ISAC structure can leave small and midsize utilities out of such organizations due to membership criteria or cost.

In addition to making information sharing less burdensome and costly to private-sector participants, developing an incentive structure would encourage private-sector organizations to share information. The private sector's information sharing capacity varies significantly by organization size and level of sophistication. Creating incentive structures to share information with the government—especially for small and midsize organizations—would help encourage participation in government-run programs. These organizations can greatly benefit from ways to alleviate the time and costs needed to continuously package network data and then analyze reports from the government or other sources.[73]

AUTOMATING INFORMATION-SHARING

Automated information sharing across a broad range of critical infrastructure organizations would ensure newly-identified threats can be quickly addressed, and has been attempted previousy. However, automation presents both technical and organizational challenges.

Existing Federal automated data-sharing standards provide technical means for implementing information sharing, and could be expanded. These include open format for sharing data called Structure Threat Information Expression (STIX) as well as the protocol for automated machine-to-machine data exchange without the need for an operator, called Trusted Automated Exchange of Indicator Information (TAXII).[I]

The predecessor to CISA developed the Automated Indicator Sharing (AIS) program using open standards like STIX and TAXII, but could not overcome hurdles to widespread adoption.[II]

A 2017-18 review of AIS found that the program lacked participation from both public- and private-sector organizations, did not sufficiently provide helpful alerts to participants, and had fallen behind on supporting technical updates to STIX.[III] The strength of such a program comes from broad participation, timely dissemination of information, and the usefulness of the information disseminated. To ensure broad participation, information sharing programs should be inexpensive, timely, and easy for participants to implement.

64 One of the more notable programs is the Cyber Risk Information Sharing Program (CRISP) operated by the Energy Information Sharing and Analysis Center (E-ISAC). CRISP sensors are deployed on the infrastructure of participating North American power utilities to offer detection and analysis of anomalous and malicious activity. The program has recently expanded to include OT pilot programs, an important step toward threat detection and correlation between IT and OT systems.

65 "The private sector is reluctant to share information," observed Lauren Zabierek et al., "as there are no defined circumstances under which federal agencies can share information with the private sector. Fears of liability, litigation, and additional regulatory action on one end, and the lack of security and safety regulations on the other make up the center piece of current legal challenges that stymie information sharing." See Lauren Zabierek, Felipe Bueno, Andrew Sady-Kennedy, Ngasuma Kanyeka, and Graham Kennis, "Toward a Collaborative Cyber Defense and Enhanced Threat Intelligence Structure," Harvard Kennedy School's Belfer Center for Science and International Affairs, August 2021, 7, https://www.belfercenter.org/publication/toward-collaborative-cyber-defense-and-enhanced-threat-intelligence-structure#toc-2-0-0.

66 Department of Homeland Security, Protected Critical Infrastructure Information, 6 C.F.R. §§ 29.1-29.9 (2002).

67 Protection from Liability, 6 U.S.C. 1505 (2015).

68 Douris, *Cyber Threat Data Sharing*, 6.

69 Exec. Order No. 13691 of 2015, 81 Fed. Reg. 23506 (April 21, 2016).

70 "Sector Coordinating Councils," Cybersecurity and Infrastructure Security Agency (website), Critical Infrastructure Sector Partnerships, n.d., accessed January 12, 2022, https://www.cisa.gov/sector-coordinating-councils.

71 "Electricity ISAC," ISAO Standards Organization (website), n.d., accessed March 12, 2022, https://www.isao.org/information-sharing-group/sector/electricity-isac/.

72 Douris, *Cyber Threat Data Sharing*, 9.

73 "DHS Made Limited Progress," 8.

I "Automated Indicator Sharing | CISA," accessed September 27, 2021, https://www.cisa.gov/ais.

II "Automated Indicator Sharing | CISA," accessed September 27, 2021, https://www.cisa.gov/ais.

III Miller, J. (2020, October 6). *CISA's still overcoming challenges 5 years after Cybersecurity Information Sharing Act became law*. Federal News Network. Retrieved February 16, 2022, from https://federalnewsnetwork.com/reporters-notebook-jason-miller/2020/10/cisas-still-overcoming-challenges-5-years-after-cybersecurity-information-sharing-act-became-law/; DHS Made Limited Progress to Improve Information Sharing under the Cybersecurity Act in Calendar Years 2017 and 2018, U.S. Department of Homeland Security, Office of the Inspector General. September 25, 2020, https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-74-Sep20.pdf

4.4 Improving Incident Response Coordination

To lead response efforts for major cyber incidents and threats, the government must have a clear and well-established leadership system, ability to delegate authorities to SLTT organizations, and work hand-in-hand with owners and operators. Meanwhile, when it comes to leading in defending assets, the private sector must be prepared with the monitoring and detection technologies and response efforts to coordinate and communicate with government officials. The energy transition is expanding the physical and digital attack surface that malicious actors increasingly seek to exploit; so while it is the responsibility of the owner of the asset to understand and protect connected assets from cyber threats, the government must have clear guidelines indicating what types of attacks require official intervention—whether from federal, state, or local authorities—and who should respond to such a threat. This means operating with a clear incident response authority structure and increased resources for SLTT cyber capabilities to meet the needs of the industry's increasingly decentralized business model.

Federal Support in the Field

Meeting the energy sector's future business model will require substantially greater coordination, cooperation, funding, and programmatic support from the federal government to state authorities and the private sector. It must mirror the energy sector's decentralized, multidirectional, and prosumer-based business model, which means helping regions, states, and the private sector to build more resilient capabilities. As the former director of CISA, Chris Krebs, noted, "The future of CISA is the field."[74]

As the Russian war against Ukraine began to unfold in late winter and early spring of 2022, CISA led a whole-of-government campaign called Shields Up to help prepare US critical infrastructure sectors for possible spikes in Russian cyberattacks. CISA's Shields Up campaign listed nearly a dozen short- and long-term actions that public- and private-sector organizations should take to help bolster their defenses against the increased threat of cyberattacks.[75] The recommendations range from suggested improvements in basic cyber hygiene and reviewing internal cybersecurity plans to incident response sets should a breach occur.

A line of utility trucks drive north on Interstate 75 in Florida on September 11, 2017. Such scenes are common when large segments of an electric system go down. REUTERS/Mark Makela

74 Lauren Zabierek et al., "Toward a Collaborative Cyber Defense."

Increasing Federal Funds for Securing the Energy Sector

The newly passed Infrastructure Investment and Jobs Act (IIJA), is a promising sign of greater attention and resources devoted to bolstering state and regional capabilities. The bill provides an unprecedented investment in energy sector cybersecurity, including resources for the local and regional level. For instance, the bill provisions a total of USD one billion for SLTT entities for cyber modernization, and response is a component. Additionally, USD 250 million is apportioned for rural and municipal utility operators to make cyber detection and response investments. Lastly, USD 100 million is directed to a Cyber Response and Recovery Fund, which makes a cash injection available to public and private entities alike.[76]

These investments are essential, but securing the energy sector will require consistent and likely increasing levels of funding that state and local governments and small and midsize energy companies can rely on annually. Current levels of federal funding lack a consistent support for the energy industry. For example, while the IIJA provides USD one billion in federal grants for state and local governments, the payments are dispersed over four years in inconsistent amounts: USD 200 million in FY 2022, USD 400 million in FY 2023, USD 300 million in FY 2024, and USD 100 million in FY 2025.[77]

Placing Federal Support in the Field

The federal government can dedicate personnel to support state and local officials and the private sector in the field. Improvements in federal coordination in the field are underway. Notably, the addition of cybersecurity state coordinators by CISA offers the opportunity to not only improve the linkage between federal and local partners, but also to add expertise. The program is in its nascent stage. As of January 2022, thirty-sevent of fifty coordinators have been hired by CISA. These coordinators, in functioning as subject-matter experts on resources available to private and public entities within each state, can go beyond information sharing and contribute to a more robust decentralized response. The new Joint Cyber Defense Collaborative (JCDC), launched by CISA with several private-sector partners in August 2021, likewise shows potential for improving incident response. The JCDC is designed to protect infrastructure from a more holistic perspective, bridging OT and IT. The inclusion of private-sector members focused on OT supports this goal, although it remains to be seen how the JCDC will coordinate and collaborate with SRMAs.

Building on these resources and personnel, the companies can do more to work with the government to continually map out improvements, anticipating changes in cyber threats and their operations. Several existing exercise series do just that, but as cyber threats to the energy sector increase, so must participation rates, exercise types, and the matrices of the organizations involved. The Grid Security Exercise (GridEx) is a two-day exercise held every two years by NERC to test responses to grid security emergencies such as simulated physical attacks and cyberattacks on the power grid.[78] Clear Path, sponsored by DOE, is another exercise series focused on "all-hazards energy security and resilience" in the energy sector and, like GridEx, brings together energy sector stakeholders to identify areas for improvement and collaboration between industry and government.[79] Although exercises generally focus on an all-hazards approach, the missed opportunity of having a cyber component to every exercise can easily be remedied. Indeed, the private sector is beginning to specifically ask for it. Participants in the GridEx V exercise appear to have taken note of the scale of the threat and have asked for more cybersecurity exercises with deeper content.[80] Exercises must also be expanded to convene federal and state authorities—not just with utilities and owners and operators, but organizations spanning the energy sector's supply chain.

Awareness and joint road-mapping campaigns must become a feature of federal support for state, local, and private-sector organizations. The process involves careful analysis of recent history, ongoing threats, intelligence about what adversaries may target in the future, and can be informed by the efforts of critical infrastructure owners and operators and industry

75 White House, "Fact Sheet: Act Now to Protect against Potential Cyberattacks," Briefing Room Statements and Releases, March 22, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/fact-sheet-act-now-to-protect-against-potential-cyberattacks/.

76 *Infrastructure Investment and Jobs Act*, Pub. L. No. 117-58, (2021).

77 S. Ferber and T. Alexander, "The *Infrastructure Investment and Jobs Act* Invests Heavily in Cybersecurity," *National Law Review XII*, No. 183, November 30, 2021, https://www.natlawreview.com/article/infrastructure-investment-and-jobs-act-invests-heavily-cybersecurity; Ferber and Alexander are with McDermott Will & Emery.

78 "GridEx," North American Electric Reliability Corporation (website), https://www.nerc.com/pa/CI/ESISAC/Pages/GridEx.aspx, accessed July 5, 2022.

79 US Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, ClearPath VIII After Action Report, March 2021, https://www.energy.gov/ceser/downloads/clear-path-outcomes-report-viii.

80 Bridget Johnson, "Participants Want More Cyber Challenges After 'Exciting' GridEx V Attack Simulation," *Homeland Security Today*, April 8, 2020, https://www.hstoday.us/subject-matter-areas/infrastructure-security/participants-want-more-cyber-challenges-after-exciting-gridex-v-attack-simulation/.

more broadly, to provide concrete actions and resources to improve cyber defenses against the most pressing risks. Guidance must be targeted, as is the case with CISA's Shields Up campaign, but also address longer-term vulnerabilities that require more resources to address, such as best practices for supply chain security or information sharing.

Scaling Industrial Cybersecurity Technologies

Energy companies must build the capabilities to continuously monitor, detect, report, and remediate threats across the nation's diverse energy assets. The challenge for many private-sector companies is scaling new technologies to cover needed assets and compensate for cybersecurity talent scarcity.

New technologies tailored to monitor and detect industrial threats to the energy sector's IT and OT assets are emerging. Leveraging machine learning (ML) monitoring and detection software can help identify anomalies, contextualize potentially malicious behavior, and help guide CISOs on mitigation techniques that potentially avoid costly and disruptive full system shutdowns. However, machine learning techniques create volumes of false positives and configuration challenges and are not yet a turnkey solution. Zpryme, a research firm, predicted that the US market for utility-scale cybersecurity solutions for the grid would total around USD 7.2 billion in 2020.[81] There are many technological approaches to enhancing threat detection—from situational awareness software to automatic anomaly detection algorithms and technology to pinpoint and evaluate malicious software.

"For small and midsize energy companies, budgets for OT security often will not exceed USD 30,000 to USD 50,000 annually," says Leo Simonovich, vice president and global head of industrial cyber at Siemens Energy Inc. "At the end of the day, CISOs with such a small budget will simply lack technological capabilities to monitor and detect threats on their network. Not only does this leave these small and midsize organizations vulnerable to cyber threats, but it has a cascading effect across the environment, including exposing weaknesses in supply chains and limits information sharing capabilities."[82]

With uneven cybersecurity capabilities across the industry, government will lack contextualized data for information sharing and adversaries will exploit the defenses of the weakest link in the ecosystem. According to a 2019 Ponemon Institute-Siemens survey of more than 1,700 professionals, only forty-two percent of global utility professionals said their organization had a "high" level of readiness to respond to cyber threats. Additionally, smaller utilities had considerably lower levels of confidence to monitor and detect threats compared to their peers at organizations with more than 5,000 employees.[83] These sentiments are consistent—if not worsening—across the energy sector. EY's 2021 Global Information Security Survey (GISS) found that CISOs working in the power and utility sector reported that "one in two (fifty percent) [flagged] that they are working with budgets that are insufficient to manage the cybersecurity challenges that have emerged over the past twelve months. A more modest forty-two percent of leaders in other sectors, on average, share the same concern."[84]

MODELS TO SCALE CYBERSECURITY SOLUTIONS

Creative public-private partnerships involving the government, technology companies, OEMs, systems integrators, and owners and operators can help shift resources where they are most helpful to scale cutting-edge technology solutions and expertise to more rapidly secure energy infrastructure.

One way to foster such partnerships is to create a center of excellence. In 2020, Siemens Energy and the New York Power Authority (NYPA) established a Center of Excellence (COE) to improve industrial cybersecurity for small and midsize utilities owned and operated by NYPA. The COE is a multipronged approach to monitor and detect industrial threats to NYPA's municipal and cooperative utilities, conduct new research at NYPA's Advanced Grid Laboratory for Energy (AGILe), and implement cyber hygiene and educational programs to train the workforce of today and prepare the next generation of industrial security professionals. Under a collective defense umbrella, Siemens Energy provided its managed detection and response platform and service to identify and prevent threats for small and midsize utilities that lack the OT security budgets or expertise to purchase the technology on their own.

81 Douris, *Cyber Threat Data Sharing*, 15.

82 Leo Simonovich (vice president and global head, industrial cyber, Siemens Energy Inc.) in a telephone interview for this publication, Friday, March 4, 2022.

83 Ponemon Institute and Siemens Energy, "Caught in the Crosshairs: Are Utilities Keeping Up with the Industrial Cyber Threat?," Siemens Gas and Power, October 19, 2019, 15, https://www.siemens-energy.com/global/en/news/magazine/2019/cyber-security-ponemon-study.html.

84 A. Campbell and C. M. Firth, "How Power and Utility CISOs Can Adapt to Enable a Digital Future, EY (website), September 30, 2021, https://www.ey.com/en_gl/power-utilities/how-power-and-utility-cisos-can-adapt-to-enable-a-digital-future.

Informing a More Effective Federal Cyber Response Model

The federal government's incident response framework must clarify roles and responsibilities at the interagency level, while bolstering its ability to provide leadership and support to state authorities and the private sector. The energy sector has a responsibility to protect its own systems and networks. This must begin with a clear and real-time understanding of an organization's assets, and a comprehensive vulnerability discovery and mitigation effort. To defend assets, the private sector must practice consistent cyber hygiene and mature toward cutting-edge monitoring and detection systems with personnel capable of identifying threats and anomalies, as well as close cooperation and coordination with public-sector counterparts. Increasingly, the United States is also prioritizing resilience and recovery along with protection as evidenced in the FY 2021 National Defense Authorization Act's inclusion of a "continuity of the economy plan" to set prioritization of efforts to "maintain and restore the economy of the United States in response to a significant event."[85]

Adjusting the federal government's existing framework to address the energy sector's increasingly digitally dependent business model calls for clearer understanding of the following key questions: what constitutes significant cyber breaches and requires federal intervention; who should lead incident response for the federal government and how should they coordinate with interagency and SLTT partners; and what adjustments are needed to build incident response capacity at the state and regional level appropriate to an increasingly decentralized ecosystem.

Efforts to improve federal government cyber incident response should aim to reduce interagency conflict, improve decision-making, and place a greater focus on asset response during an ongoing crisis. Leveraging CISA as the lead agency for incident response will help to focus the federal government's actions on preventing or remediating the effects of an

Rear Admiral Mike Brown, deputy assistant secretary for Cyber Security and Communications, briefs the media on Cyber Storm III exercise at the National Cybersecurity & Communications Integration Center (NCCIC) located just outside Washington in Arlington, Virginia on September 24, 2010. REUTERS/Hyungwon Kang

85 National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, 116th Cong. (2021), https://www.acq.osd.mil/dpap/dars/docs/early_engagement_opportunity/HR_6395-116_Enrolled_FY21_NDAA.pdf.

ongoing national security crisis—a cyberattack on CI assets. Elevating CISA as lead coordinator, with law enforcement and intelligence to maintain their incident response requirements, can best help the energy sector respond to attacks. CISA's recent guidance anticipating an increase of cyberthreats related to the conflict in Ukraine is a useful example. Elevated threat warnings must become routine and mirror guidance during other national emergencies, such as natural disasters.

Protection of critical infrastructure assets may occasionally call for more than defensive measures to defend national security interests. There is no substitute for the ability to engage an adversary on the digital battlefield to simultaneously degrade their capabilities and defeat their attack. Only certain parts of the defense apparatus have the authorities and resources for this mission space. Any update to PPD-41 that fails to define the difference in circumstances triggering civilian asset response versus a military defensive action to reduce the lag between discovery and action would be a missed opportunity.

Securing the energy transition will require making annual federal appropriations for states and energy-specific programs permanent. In the past decade less than four percent of DHS's budget went to grant funding for state cybersecurity budgets.[86] The IIJA was a significant step toward elevating cybersecurity as a federal priority; it included USD 46 billion allocated to cybersecurity for critical infrastructure and USD 73 billion under the bipartisan Energy Infrastructure Act for grid reliability and resiliency.[87] This spending, however, is neither reoccurring nor exclusively intended for the energy sector. In the long-term, federal funding must become an annual and distinct line item.

The private sector must be both incentivized and held accountable for understanding, protecting, and defending their networks. While it is their role to ensure systems are secure by design, build resilience, and invest in their own security, the government must provide technical, policy, and financial support for these critical efforts. Monitoring and detection technologies can help the energy sector identify threats in their operating environments in time to mitigate their most devastating consequences. Some large and profitable energy companies will not need assistance deploying these technologies, but most will need some type of financial or technical assistance with anomaly detection solutions.[88] It is in the government's interest to encourage the energy sector to deploy solutions so they can better monitor and detect threats, and then share this information. Although beyond the scope of this report, it is worth mentioning that market tools that assign a price to cyber risk—such as cyber insurance—offer additional tools to encourage robust private-sector cybersecurity efforts.

4.5 Recommendations

Improving Supply Chain Security

- DHS CISA and SRMAs should coordinate with NIST and other recognized standards organizations to develop clear guidelines on product and supply chain security, and lower financial costs for product certifications.

- For a limited subset of critical infrastructure, Congress should consider providing DHS CISA the authorities, funding, and leeway to—in consultation with appropriate defense, intelligence, and domestic security organizations—conduct robust penetration testing and proactive measures beyond what is commercially available to better secure infrastructure against sophisticated threat actors, specifically nation-states.

Information Sharing and Coordination

- The president should reconcile and abrogate information-sharing roles and responsibilities between DHS CISA, DOE, FERC, and the SRMAs. DHS CISA and the SRMAs should improve and streamline information-sharing programs to include interchangeable data formats, consistent data across critical infrastructure sectors (where possible), sector-specific context (as available), with built-in sharing in real-time to the necessary parties.

- In recognition of the widespread reluctance of the private sector to share information with agencies with regulators, Congress should consider granting to cabinet-level leadership at DHS and the SRMAs the authority to exempt select suboffices and individuals conducting critical infrastructure protection work from regulatory roles and responsibilities to foster candid communication about risk.

- DHS CISA and the SRMAs should endeavor to provide actionable and timely information to the private sector. These efforts should include classified information as allowable and declassification or the lowest allowable classification, as necessary.

- DHS CISA, SRMAs, and industry groups should work with the private sector to design a technology-neutral, international standards-based, information-sharing framework to include the process of data collection, expanding security clearance processes, quality, and timeframe of information provided back to the private sector. This includes reforming and reconciling existing liability protection programs. Liability reform should be focused on reducing interagency complexity and coverage limitations. This may be a task for the new JCDC.

Incident Response and Improving Resilience

- The president, in consultation with DHS CISA and DOD, should establish a clear line of demarcation in federal incident response under PPD-41 between what constitutes civilian asset response and protection of the kind that DHS CISA can support and what constitutes a more sophisticated matter which necessitates a response by appropriate defense and domestic security organizations in accordance with existing law and authorities.

- DHS CISA should expand ongoing efforts to fund and provide cybersecurity state coordinators, providing them with the necessary tools and staffing to adequately support state efforts to secure critical infrastructure and effectuate lead incident response in instances where a federal response is not warranted.

86 National Associate of State Chief Information Officers, "Ensure Dedicated Cybersecurity Funding for State and Local Governments with CIOs as Key Decisionmakers," 2020, accessed April 20, 2022, https://www.nascio.org/wp-content/uploads/2020/01/NASCIO-Dedicated-Cyber-Funding-2020.pdf.

87 "Bipartisan *Infrastructure Investment and Jobs Act* Summary: A Road to Stronger Economic Growth," National Conference of State Legislatures, (n.d.), accessed April 20, 2022, https://www.ncsl.org/documents/statefed/IIJA-Section-by-Section.pdf.

88 C. Vasquez, "N.Y. Utility, Siemens Energy Plan First-of-a-kind Cyber Hub," Energywire, *E&E News*, July 29, 2020, https://www.eenews.net/articles/n-y-utility-siemens-energy-plan-first-of-a-kind-cyber-hub/.

SECURING THE ENERGY TRANSITION AGAINST CYBER THREATS

5. Conclusion

Securing the evolving energy sector from the rising threat of cyberattacks is one of the most pressing national, economic, and environmental challenges facing the United States. Increasing reliance on digital technology means that cybersecurity will be necessary to reliably achieve any of the expected benefits to national security, to climate security, or to energy consumers. The existing set of institutions and authorities cannot adequately secure the energy transition. The historic and existing structure of the United States' energy industry – coupled with its rapid shift to digitally-driven business models – has left the public and private sectors without a unified or strategic framework to secure the industry.

The interconnected relationship between government and the private sector is a defining feature of both the challenges and solutions to securing the energy sector's vastly expanding attack surface. A new framework to secure the energy transition must reconcile the government's responsibility for the country's national and economic security with the fact that the majority of US physical and digital assets in need of protection lie in the private sector's hands. Clarifying and improving this symbiotic relationship will greatly improve the US energy sector's preparedness, resilience, and capabilities to defend against cyberattacks.

To secure the energy transition, policymakers must realign the energy sector's existing cybersecurity laws and regulations into a more cohesive and responsive system. Such a realignment of government authorities and polices would deepen federal centers of expertise, sharpen coordination and response functions, and reduce duplicative—and sometimes rivalrous — functions within government. It would also unlock government funding and resources to spur private sector innovation and investment in new technologies, encourage public-private collaboration on supply chain security, information sharing, and incident response, and surmount looming challenges like access to capital and workforce shortages.

Securing the energy industry and critical infrastructure from cyber threats is increasingly a vital interest for the United States and countries around the world. The future of US national, economic, and environmental security depends on harnessing the power of digitally connected and electrified clean and low-carbon energy technologies. These technologies will lead to innovation and economic growth, and will define future geopolitical competitiveness. Globally, rapidly replacing fossil fuels with digitally driven low- and zero-carbon technologies to avoid the most devastating effects of climate change. Reimagining existing frameworks to secure the energy transition is a complex but urgent endeavor. The choices the United States makes will result either in a fragile, vulnerable energy sector, or a solid foundation for a more sustainable and secure future.

SECURING THE ENERGY TRANSITION AGAINST CYBER THREATS

Biographies

Co-Chairmen

Secretary Michael Chertoff is co-founder and executive chairman of The Chertoff Group, providing high-level strategic counsel to corporate and government leaders on a broad range of security issues.

As secretary of the US Department of Homeland Security from 2005 to 2009, Mr. Chertoff led the country in blocking would-be terrorists from crossing our borders or implementing their plans if they were already in the country. He also transformed FEMA into an effective organization following Hurricane Katrina. His greatest successes have earned few headlines, because the important news is what didn't happen.

At The Chertoff Group, Mr. Chertoff provides high-level strategic counsel to corporate and government leaders on a broad range of security issues, from risk identification and prevention to preparedness, response and recovery.

Before leading the Department of Homeland Security, Mr. Chertoff served as a federal judge on the US Court of Appeals for the Third Circuit. Earlier, during more than a decade as a federal prosecutor, he investigated and prosecuted cases of political corruption, organized crime, corporate fraud and terrorism—including the investigation of the 9/11 terrorist attacks.

Mr. Chertoff is a *magna cum laude* graduate of Harvard College (1975) and Harvard Law School (1978). From 1979-1980 he served as a clerk to Supreme Court Justice William Brennan, Jr.

In addition to his role at The Chertoff Group, Mr. Chertoff is senior of counsel at Covington & Burling LLP, and a member of the firm's White Collar Defense and Investigations practice group.

General Wesley K. Clark is a businessman, educator, writer, and commentator.

General Clark serves as chairman and CEO of Wesley K. Clark & Associates, a strategic consulting firm; chairman and founder of Enverra, Inc. a licensed investment bank; chairman of Energy Security Partners, LLC; as well as numerous corporate boards. He is active in the energy industry, including the oil and gas, biofuels, electric power and batteries, finance, and security sectors. During his business career he has served as an advisor, consultant, or board member of over ninety private and publicly traded companies. In the not-for-profit space, he is a senior fellow at UCLA's Burkle Center for International Relations; board director of the Atlantic Council; and founding chair of City Year Little Rock/North Little Rock. A best-selling author, he has written four books and is a frequent contributor on TV and to newspapers.

General Clark retired as a four-star general after thirty-eight years in the US Army, having served in his last assignments as commander of US Southern Command and then as commander of US European Command/Supreme Allied Commander, Europe. He graduated first in his class at West Point and completed BA and MA degrees in philosophy, politics, and economics at Oxford University as a Rhodes Scholar. While serving in Vietnam, he commanded an infantry company in combat, where he was severely wounded and evacuated home on a stretcher. He later commanded at the battalion, brigade, and division level, and served in a number of significant staff positions, including service as the director, Strategic Plans and Policy (J-5). He was the principal author of both the US National Military Strategy and Joint Vision 2010, prescribing US warfighting for full-spectrum dominance. He also worked with Ambassador Richard Holbrooke in the Dayton Peace Process, where he helped write and negotiate significant portions of the 1995 Dayton Peace Agreement. In his final assignment as Supreme Allied Commander Europe, he led NATO forces to victory in Operation Allied Force, a seventy-eight-day air campaign, backed by ground invasion planning and a diplomatic process, saving 1.5 million Albanians from ethnic cleansing.

General Clark's awards include the Presidential Medal of Freedom, Defense Distinguished Service Medal (five awards), Silver Star, Bronze Star, Purple Heart, honorary knighthoods from the British and Dutch governments, and numerous other awards from other governments, including the award of Commander of the Legion of Honor from France. He has also been awarded the Department of State Distinguished Service Award and numerous honorary doctorates and civilian honors.

Rapporteurs

Pedro M. Allende is an attorney, policy adviser, professor, strategic adviser, and serves as a nonresident fellow at the Atlantic Council Global Energy Center. Most recently, he served as deputy assistant secretary for infrastructure, risk, and resilience policy with the Office of Strategy, Policy, and Plans at the Department of Homeland Security. There he led policy development to protect US critical infrastructure against cyber, physical, and natural threats, while overseeing policy efforts to increase federal, state, and local preparedness, response, and recovery capabilities.

Prior to that, Mr. Allende served as senior adviser and director of strategic initiatives at the Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response. He has also advised on domestic and international labor policy, trade policy, and development finance as counselor to the secretary of labor. Before working in government, he practiced law at Boies Schiller Flexner, where he cofounded the firm's data privacy and cybersecurity practice and litigated high-stakes cases including class actions and cross-border disputes. Mr. Allende is an adjunct professor at the University of Florida College of Law, where he focuses on cybersecurity and law. He earned a JD, MS in decision and information science, a BA in political science, and a BS in economics from the University of Florida.

Andrew Gumbiner is the founder of AJG Strategies, LLC, a public affairs consultancy based in Washington, DC, focused on advising energy sector and industrial cybersecurity clients on strategic communications and public policy issues. He also serves as a nonresident fellow at the Atlantic Council Global Energy Center. Before starting AJG Strategies, LLC, in 2019, Mr. Gumbiner was a spokesman for Siemens USA, managing public affairs for the company's energy and cybersecurity business and serving as an advisor to the US CEO.

Previously, Mr. Gumbiner served in the Obama administration as the press secretary and spokesman at the US Department of Energy (DOE), and aide to Secretary Ernest Moniz. Before his role as DOE press secretary, Mr. Gumbiner was the spokesman and head of communications for DOE's Advanced Research Projects Agency-Energy (ARPA-E) and worked as a consultant with Booz Allen Hamilton. In Congress, Mr. Gumbiner was communications director in the US House of Representatives, and he started his career as a press aide in the House Democratic Caucus.

Mr. Gumbiner received his BA from Hamilton College in Clinton, NY, and his MA from Johns Hopkins University's School of Advanced International Studies in Washington, DC.

John La Rue is a writer based in Washington, DC, with a focus on energy and public policy. He is currently a nonresident fellow at the Atlantic Council Global Energy Center, and has previously served as the chief speechwriter for the US Secretary of Energy and the senior speechwriter for the director of the US Office of Personnel Management. In 2019, he won the top honors in the Professional Speechwriters Association's Cicero Awards. Mr. La Rue holds a master's degree in Public Administration from the Harvard Kennedy School of Government.

Task Force Co-Directors

Randolph Bell is a distinguished fellow at the Atlantic Council Global Energy Center and head of international government affairs at Commonwealth Fusion Systems, where he helps lead international market entry for CFS's commercial fusion plants in the 2030s.

From 2018–2022, Mr. Bell was the Global Energy Center's senior director and the inaugural holder of the Richard Morningstar Chair for Global Energy Security. In this capacity, he set the center's strategy and oversaw the center's research and programs, including the annual Atlantic Council Global Energy Forum in Abu Dhabi, through a period of remarkable growth. His research and writing focused on hydrogen policy, advanced technologies and innovation, oil & gas in the energy transition, and energy geopolitics. He joined the Global Energy Center in 2017 as its director of business strategies. From 2014–2016, Mr. Bell led the launch of the center in his capacity as director of business development and new ventures for the Atlantic Council.

From 2011–2014, Mr. Bell was managing director at the International Institute for Strategic Studies–US, where in addition to holding overall responsibility for the operations and programming of the IISS's Washington, DC office he published extensively on African, South Asian, and cyber security issues. From 2010–2011, he was manager of national security at the Markle Foundation, where he worked on cyber security, intelligence community information sharing, and technology policy issues.

Mr. Bell has an MPP from the John F. Kennedy School of Government at Harvard University, where he was a Public Service and Belfer International and Global Affairs fellow, and graduated *magna cum laude* from Harvard College.

Olga Khakova is the deputy director for European energy security at the Atlantic Council's Global Energy Center, where she manages transatlantic energy initiatives. Before joining the Atlantic Council, Ms. Khakova was a senior program coordinator for US Energy Association's Energy Technology and Governance Program. She helped start and coordinate the Western Balkans' Electricity Market Initiative working group, which provides technical expertise on creating better-connected electricity markets.

Ms. Khakova also worked as a program director for a leading energy non-profit in the Midwest, The Climate + Energy Project (CEP). While at CEP, she co-led the conception and development of the Clean Energy Business Council, a network of businesses seeking to capitalize on renewable energy resources in Kansas and the greater Kansas City area through legislative, regulatory, and educational solutions. Ms. Khakova facilitated state-wide stakeholder engagement on energy issues, such as education and outreach on rate design dockets at the Kansas Corporation Commission. During her time at Bombardier Aerospace, Ms. Khakova organized events and developed communications strategies in Brazil, Canada, China, and the US for a distinguished human factors safety program called Safety Standdown.

Ms. Khakova has a business administration degree from Wichita State University and a professional science master's in environmental assessment from the University of Kansas. She is originally from Ukraine.

Atlantic Council

Board of Directors

CHAIRMAN
*John F.W. Rogers

EXECUTIVE CHAIRMAN EMERITUS
*James L. Jones

PRESIDENT AND CEO
*Frederick Kempe

EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

VICE CHAIRS
*Robert J. Abernethy
*C. Boyden Gray
*Alexander V. Mirtchev

TREASURER
*George Lund

DIRECTORS
Stéphane Abrial
Todd Achilles
Timothy D. Adams
*Michael Andersson
David D. Aufhauser
Barbara Barrett
Colleen Bell
Stephen Biegun
Linden P. Blue
Adam Boehler
John Bonsell
Philip M. Breedlove
Myron Brilliant
*Esther Brimmer
Richard R. Burt
*Teresa Carlson
*James E. Cartwright
John E. Chapoton
Ahmed Charai
Melanie Chen
Michael Chertoff
*George Chopivsky
Wesley K. Clark
*Helima Croft
*Ankit N. Desai
Dario Deste
*Paula J. Dobriansky
Joseph F. Dunford, Jr.
Richard Edelman
Thomas J. Egan, Jr.
Stuart E. Eizenstat
Mark T. Esper
*Michael Fisch
*Alan H. Fleischmann
Jendayi E. Frazer
Meg Gentle
Thomas H. Glocer
John B. Goodman
*Sherri W. Goodman
Murathan Günal
Frank Haun
Michael V. Hayden
Tim Holt
*Karl V. Hopkins
Kay Bailey Hutchison
Ian Ihnatowycz
Mark Isakowitz
Wolfgang F. Ischinger
Deborah Lee James
*Joia M. Johnson
*Maria Pica Karp
Andre Kelleners
Brian L. Kelly
Henry A. Kissinger
John E. Klein
*C. Jeffrey Knittel
Franklin D. Kramer
Laura Lane
Yann Le Pallec
Jan M. Lodal
Douglas Lute
Jane Holl Lute
William J. Lynn
Mark Machin
Mian M. Mansha
Marco Margheri
Michael Margolis
Chris Marlin
William Marron
Christian Marrone
Gerardo Mato
Timothy McBride
Erin McGrain
John M. McHugh
Eric D.K. Melby
*Judith A. Miller
Dariusz Mioduski
Michael J. Morell
*Richard Morningstar
Georgette Mosbacher
Dambisa F. Moyo
Virginia A. Mulberger
Mary Claire Murphy
Edward J. Newberry
Franco Nuschese
Joseph S. Nye
Ahmet M. Ören
Sally A. Painter
Ana I. Palacio
*Kostas Pantazopoulos
Alan Pellegrini
David H. Petraeus
*Lisa Pollina
Daniel B. Poneman
*Dina H. Powell McCormick
Michael Punke
Ashraf Qazi
Thomas J. Ridge
Gary Rieschel
Lawrence Di Rita
Michael J. Rogers
Charles O. Rossotti
Harry Sachinis
C. Michael Scaparrotti
Ivan A. Schlager
Rajiv Shah
Gregg Sherrill
Ali Jehangir Siddiqui
Kris Singh
Walter Slocombe
Christopher Smith
Clifford M. Sobel
James G. Stavridis
Michael S. Steele
Richard J.A. Steele
Mary Streett
Gil Tenzer
*Frances M. Townsend
Clyde C. Tuggle
Melanne Verveer
Charles F. Wald
Michael F. Walsh
Ronald Weiser
Maciej Witucki
Neal S. Wolin
*Jenny Wood
Guang Yang
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
James A. Baker, III
Ashton B. Carter
Robert M. Gates
James N. Mattis
Michael G. Mullen
Leon E. Panetta
William J. Perry
Condoleezza Rice
Horst Teltschik
William H. Webster

**Executive Committee Members*

List as of June 1, 2022