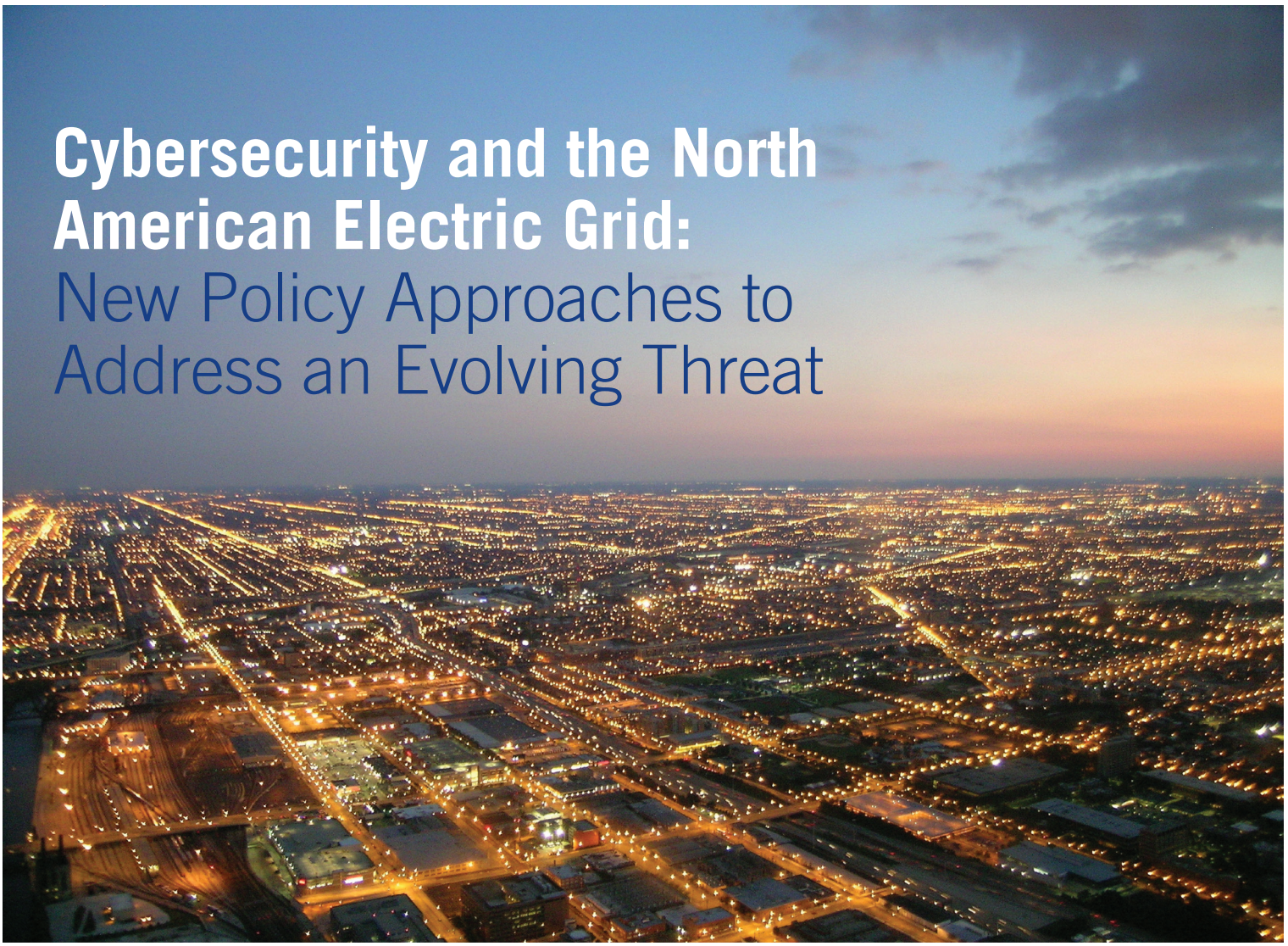
**Energy & Infrastructure Program**
*Energy Project*

**National Security Program**
*Homeland Security Project*

# Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat



A Report from the Co-chairs of the Bipartisan Policy Center's Electric Grid Cybersecurity Initiative

February 2014

BIPARTISAN POLICY CENTER

## DISCLAIMER

The findings and recommendations expressed within this report are those of the co-chairs of the Bipartisan Policy Center's Electric Grid Cybersecurity Initiative. While these findings and recommendations were informed by the discussion with the advisory group listed on page 1, they do not necessarily represent the views or opinions of advisory group members or the organizations they represent.

# Bipartisan Policy Center Electric Grid Cybersecurity Initiative Participants

## CO-CHAIRS

**General (Ret.) Michael Hayden**
Principal, The Chertoff Group; former Director, CIA; former Director, NSA

**Curt Hébert**
Partner, Brunini, Grantham, Grower & Hewes, PLLC; former Chairman, FERC; former Chairman, Mississippi Public Service Commission

**Susan Tierney**
Managing Principal, Analysis Group; former Assistant Secretary for Policy, DOE; former commissioner, Massachusetts Department of Public Utilities

## ADVISORY GROUP MEMBERS

**Scott Aaronson**
Senior Director, National Security Policy, Edison Electric Institute

**Scott Baron**
Director, Digital Risk and Security Governance, National Grid

**Jim Burpee**
President & CEO, Canadian Electricity Association

**Terry Boston**
President & CEO, PJM Interconnection

**Robert Caldwell**
Chief Cyber Security Architect, General Electric

**Paul Centolella**
Vice President, Analysis Group; former commissioner, Public Utilities Commission of Ohio

**Roger Duncan**
Research Fellow, Energy Institute, University of Texas; former General Manager, Austin Energy

**Jessica Matlock**
Director, Government Relations, Snohomish County Public Utility District

**Jeff Nichols**
Director, Information Security and Management, Sempra Energy Utilities

**James Sample**
Chief Information Security Officer, Pacific Gas and Electric Company

**Paul Stockton**
Managing Director, Sonecon; former Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs

**Mark Weatherford**
Principal, The Chertoff Group; former Deputy Undersecretary for Cybersecurity, DHS

## BPC ELECTRIC GRID CYBERSECURITY INITIATIVE STAFF

**Margot Anderson**
Executive Director, Energy Project

**Joe Kruger**
Director for Energy and Environment

**Carie Lemack**
Director, Homeland Security Project

**Blaise Misztal**
Acting Director, Foreign Policy Project

**Meghan McGuinness**
Associate Director for Energy and Environment

**Jason Burwen**
Senior Policy Analyst

**Blair Beasley**
Policy Analyst

**Rosemarie Calabro Tully**
Press Secretary, Energy

**Abbey Brandon**
Press Assistant

**Amanda Kaster**
Project Assistant

## ACKNOWLEDGEMENTS

The Bipartisan Policy Center (BPC) would like to thank its funders for their strong support. We also thank advisory board members Paul Stockton of Sonecon, LLC, who drafted Chapter 5 of this report, and Paul Centolella of the Analysis Group who drafted portions of Chapters 2, 3, and 6. We are grateful for their expertise and contributions. We thank Doug Smith and Andrew Art of Van Ness Feldman, LLP for their invaluable input. We are grateful to Colleen Kelly, former policy analyst with the Energy Project, and Blake Harwood, former intern with the Homeland Security Project, for their work on the early stages of this project. In addition, we would like to thank NARUC and Commissioner Phillip Jones of the Washington Utilities and Transportation Commission for their helpful comments on a draft of this report. Special appreciation is also due to Marika Tatsutani for editing the report. Finally, we would like to acknowledge the following key staff or colleagues of advisory board members for the many contributions to this report:

Patrick Brown, Director, U.S. Affairs, Canadian Electricity Association
Chris Foster, Manager, Federal Government Relations, Pacific Gas and Electric Company
Scott King, Information Security Manager, Sempra Energy Utilities
Sean Mackay, Government Affairs, Sempra Energy

# List of Acronyms

| | |
|---|---|
| **AFNG** | Air Force National Guard |
| **AMI** | Advanced Metering Infrastructure |
| **BPC** | Bipartisan Policy Center |
| **CCRIC** | Canadian Cyber Incident Response Centre |
| **CEDS** | Cybersecurity for Energy Delivery Systems |
| **CIP** | Critical Infrastructure Protection |
| **CISO** | Chief Information Security Officer |
| **CISPA** | Cyber Intelligence Sharing and Protection Act |
| **CRISP** | Cybersecurity Risk Information Sharing Program |
| **DHS** | U.S. Department of Homeland Security |
| **DOC** | U.S. Department of Commerce |
| **DOE** | U.S. Department of Energy |
| **DOJ** | U.S. Department of Justice |
| **ECPA** | Electronic Communications Privacy Act |
| **EPRI** | Electric Power Research Institute |
| **ESCC** | Electricity Sub-sector Coordination Council |
| **ES-C2M2** | Electricity Sector Cybersecurity Capability Maturity Model |
| **ES-ISAC** | Electricity Sector Information Sharing and Analysis Center |
| **FBI** | Federal Bureau of Investigation |
| **FEMA** | Federal Emergency Management Agency |
| **FERC** | Federal Energy Regulatory Commission |
| **GAO** | Government Accountability Office |
| **GCC** | Government Coordinating Council |
| **GICSP** | Global Industrial Cyber Security Professional |
| **GRID** | Grid Reliability and Infrastructure Defense |
| **GridEx** | Grid Security Exercise |
| **GridSecCon** | Grid Security Conference |
| **ICS-CERT** | Industrial Control Systems Cyber Emergency Response Team |
| **INPO** | Institute of Nuclear Power Operations |
| **ISAC** | Information Sharing and Analysis Center |
| **MOU** | Memorandum of Understanding |
| **NARUC** | National Association of Regulatory Utility Commissioners |
| **NCCIC** | National Cybersecurity and Communications Integration Center |
| **NCIRP** | National Cyber Incident Response Plan |
| **NCRAL** | National Cyber Risk Alert Level |
| **NEIL** | Nuclear Electric Insurance, Ltd. |
| **NERC** | North American Electric Reliability Corporation |
| **NIST** | National Institute of Standards and Technology |
| **NRF** | National Response Framework |

| | |
|---|---|
| **NSF** | National Science Foundation |
| **PSC** | Public Safety Canada |
| **PUC** | Public Utility Commission |
| **RMP** | Risk Management Process |
| **SAFETY** | Support Anti-Terrorism by Fostering Effective Technologies |
| **SCADA** | Supervisory Control and Data Acquisition |
| **SnoPUD** | Snohomish County Public Utility District |
| **STIX** | Structured Threat Information Expression |
| **TAXII** | Trusted Automated Exchange of Indicator Information |
| **TRIA** | Terrorism Risk Insurance Act |
| **UCG** | Unified Coordination Group |
| **US-CERT** | U.S. Computer Emergency Readiness Team |

■ **Energy & Infrastructure Program**
*Energy Project*

■ **National Security Program**
*Homeland Security Project*

# Summary of Findings and Recommendations

## Introduction

Protecting the nation's electricity grid from cyber attacks is a critical national security issue. Evidence collected by the U.S. Department of Homeland Security (DHS) suggests that cyber attacks on key energy infrastructure—and on the electricity system in particular—are increasing, both in frequency and sophistication. These trends are alarming because the potential consequences of a successful large-scale cyber attack—or combined cyber and physical attack—on the electric power sector are difficult to overstate. As previous grid failures, including the multiday Northeast blackout of 2003, have shown, any event that causes prolonged power outages over a large area would not only be extremely costly, it would wreak havoc on millions of people's daily lives and could profoundly disrupt the delivery of essential services, including communications, food, water, health care, and emergency response. Moreover, cyber threats, unlike traditional threats to electric grid reliability such as extreme weather, are less predictable in their timing and more difficult to anticipate and address. A cyber attack could come from many sources and—given the size and complexity of the North American electric grid—could target many potential vulnerabilities. For this reason, experts agree that the risk of a successful attack is significant, and that the system and its operators must be prepared to contain and minimize the consequences.

Current efforts to provide for electric grid cybersecurity are dispersed and involve numerous federal, state, and local agencies. In some ways, the electric sector is in a stronger position than other sectors to address cyber threats because it already has extensive policies in place—including mandatory federal standards that apply to the bulk power system and nuclear power plants—to assure reliability. In addition, a number of mechanisms have been introduced to facilitate relevant information sharing between the public and private sectors, and within the power sector itself. But given the complexity, fast-changing nature, and magnitude of potential cyber threats, it is also clear that more must be done to improve grid cybersecurity. Urgent priorities include strengthening existing protections, for the distribution system as well as the bulk power system; enhancing coordination at all levels; and accelerating the development of robust protocols for response and recovery in the event of a successful attack.

This report summary highlights key findings and recommendations from the co-chairs of the Bipartisan Policy Center's (BPC) Electric Grid Cybersecurity Initiative. It covers four topic areas: standards and best practices, information sharing, response to a cyber attack, and paying for cybersecurity. Recommendations in these areas target Congress, federal government agencies, state public utilities commissions (PUCs), and industry. The Initiative was launched as a collaboration of BPC's Energy and Homeland Security Projects in May 2013. Its goal was to develop policies—aimed at government agencies as well as private companies—for protecting the North American electric grid from cyber attacks. To guide the Initiative, BPC assembled a diverse and highly knowledgeable advisory group that included cybersecurity experts and managers, grid operators, and former energy and national security officials. BPC also held a public workshop on August 6, 2013, in Washington, D.C., to solicit additional perspectives and insights. Information on the Initiative and materials from the workshop can be accessed at http://bipartisanpolicy.org/events/2013/08/protecting-electric-grid-cyber-attacks-where-do-we-stand. A more detailed discussion of these issues and additional recommendations can be found in the main report.

## Standards and Best Practices

The U.S. bulk power system is already subject to mandatory federal reliability standards that include some cybersecurity protections. Critical infrastructure protection (CIP) standards are developed by the North American Electric Reliability

Corporation (NERC) and approved by the Federal Energy Regulatory Commission (FERC). These standards cover critical cyber asset identification, security management controls, personnel and training, electronic security, physical security, systems security, incident reporting and response planning, and recovery plans. While standards provide a useful baseline level of cybersecurity, they do not create incentives for the continual improvement and adaptation needed to respond effectively to rapidly evolving cyber threats. Distribution facilities generally operate outside of FERC jurisdiction. In some cases attacks at the distribution-system level could have consequences that extend to the broader grid. Our recommendations in this area aim to elevate cybersecurity at both the bulk power system and at the distribution system levels.

A particularly important recommendation concerns the establishment of a new industry-led body, comprising power sector participants across North America and modeled on the nuclear power industry's Institute of Nuclear Power Operations (INPO). Based on experience with INPO, we believe such an organization could substantially advance cybersecurity risk-management practices across the industry and, in doing so, serve as a valuable complement to existing NERC standards. In addition, we offer recommendations aimed at encouraging participation in this new institute, managing cyber risks that may originate in the supply chain, and training a cybersecurity workforce.

- NERC should continue to develop and enforce cybersecurity standards in a manner that is consistent with a risk-management approach and that provides affected entities with compliance flexibility. FERC and applicable authorities in Canada should be supportive of this approach in their review of NERC standards.
- The electric power industry should establish an organization, similar to INPO, that would develop cybersecurity performance criteria and best practices for the entire industry. This new institute should include the full range of participants in the North American power sector, and it should engage in several activities, including (a) developing performance criteria and conducting detailed cybersecurity evaluations at individual facilities; (b) analyzing systemic risks, particularly on the distribution system; (c) analyzing cyber events as they occur and disseminating information about these events; (d) providing technical assistance, including assistance in the use of new cybersecurity tools; and (e) cybersecurity workforce training and accreditation.
- Congress should adopt legislation that would encourage power sector entities to participate in the new institute by providing liability protection to entities that achieve a favorable cybersecurity evaluation by that body.
- The federal government should provide backstop cybersecurity insurance until the private market develops more fully. Legislation modeled on the Terrorism Risk Insurance Act (TRIA) could extend reinsurance coverage to insurers following cybersecurity events that require payouts in excess of some predetermined amount. Such a backstop should be withdrawn gradually after the private insurance market has had sufficient time to develop.
- The electric power sector and the federal government should collaborate to establish a certification program that independently tests grid technologies and products to verify that a specified security standard has been met. Such a program would provide equipment manufacturers and vendors with a strong incentive to invest in cybersecurity features, and it would benefit utilities by allowing them to select products that incorporate such features.
- The National Institute of Standards and Technology (NIST) should include guidelines for related skills training and workforce development in its Cybersecurity Framework.

- DHS should work with universities and colleges to develop engineering and computer science curricula built around industrial control system cybersecurity. These curricula should include vulnerabilities and threat analysis. DHS should also coordinate with the Department of Defense to identify ways that some of the cybersecurity defense training undertaken by the military might be offered more broadly to personnel in critical infrastructure sectors.
- The U.S. Department of Energy (DOE) should assist states in providing funds so that regulatory staff can participate in academic programs, more intensive training institutes, and continuing education programs.

## Information Sharing

Timely information sharing—between industry and government, within industry and across critical infrastructure sectors, and across government agencies and different levels of government—is an essential component of an effective cybersecurity strategy. It is also the primary way to identify, assess, and respond to threats in real time. While government and industry are doing a better job of sharing information on cyber threats, two fundamental challenges persist. The first is industry's reluctance to share data for fear of triggering regulatory non-compliance actions, violating privacy or antitrust protections, or potentially disclosing proprietary or confidential business information. A second challenge is obtaining intelligence information from government authorities that is sufficiently timely, specific, and actionable. Our recommendations target these issues as well as the need for enhanced information sharing with international and state-level counterparts, and across critical infrastructure sectors.

- Efforts to create a firewall between information sharing and regulatory compliance should continue, and additional steps should be taken to pursue the full functional separation of NERC (as a regulatory entity) and the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), which is housed within NERC. For example, NERC could establish the ES-ISAC as a subsidiary of NERC, with ties only in funding, and physically separate the two organizations. Going forward, DOE and NERC should work with industry to evaluate whether and to what extent NERC's firewall policy improves industry's confidence that sharing timely information with NERC does not risk triggering potential compliance or enforcement action.
- Policymakers and federal agencies should work with industry to better understand how much sharing of customer data is needed to provide relevant threat and vulnerability information. This would help all parties gain a better understanding of how privacy concerns relate to electric grid cybersecurity.
- Congress and executive branch agencies should continue to develop information sharing provisions that balance concerns about customer privacy with the imperative for timely and effective information sharing.
- Congress should continue to pursue legislation that protects utilities from civil and criminal liability for "good faith" information sharing. The "good faith" standard should be defined in terms that are sufficiently clear and specific so as to minimize the risk of litigation; one component of this standard should require utilities to take all reasonable measures to remove personally identifiable information from shared data. In addition, Congress may wish to consider limiting liability protections to situations in which information is shared at the direction of, or with the permission of, government authorities.
- Efforts to streamline the security clearance process for selected power sector employees, as required by Executive Order 13636, should continue. At the same time, intelligence agencies should declassify relevant threat and vulnerability information when possible and use other methods, such as tear lines, to separate

classified and unclassified information in order to facilitate the sharing, for official use only, of otherwise classified or restricted reports with power sector partners.

- Utility-led efforts to collect and share information on threats and vulnerabilities should be expanded and should complement information sharing between the government and industry.
- DHS, the ES-ISAC, and industry should consider how to most efficiently share threat and intelligence information with trusted vendors.
- The U.S. intelligence community, DHS, and DOE should conduct regular outreach to state utility commissions, other relevant state agencies, and public and municipal utilities on cyber threats and vulnerabilities. These federal agencies should identify best practices for sharing classified information with private sector entities as needed to protect critical infrastructure.
- U.S. intelligence officials should conduct regular outreach and briefings, including classified briefings with relevant state officials and with Canadian and Mexican industry counterparts. DHS and DOE should also work to ensure that these counterparts are able to engage in all relevant government-industry forums.
- DHS should encourage organizational standardization to promote a more efficient flow of information between the Information Sharing and Analysis Centers (ISACs) of various critical infrastructure sectors and the government. In addition, mechanisms should be developed to facilitate direct industry-to-industry information sharing (or company-to-company) communication.

## Responding to a Cyber Attack

A large-scale cyber attack on the electric grid would present governance and coordination challenges in addition to difficult technical and logistical challenges. Not only would a successful attack require cyber-specific responses, such as the removal of malware, it would likely also require more traditional disaster response operations to deal with resulting threats to public health and safety. Efficient and ongoing communication will clearly be critical, along with effective coordination, a clear chain-of-command, and the ability to adapt quickly as new information emerges. While Executive Order 13636 has helped clarify cybersecurity roles and responsibilities within the federal government, questions remain concerning the specific responsibilities of different agencies and chain-of-command in the event of an attack. We provide recommendations for improving government and industry readiness for a cyber event, and for reconciling differences between the existing National Response Framework (NRF) and the 2010 Interim National Cyber Incident Response Plan (NCIRP). The NRF, which was developed in 2008 and updated in 2010, was designed to address physical and other impacts from "traditional" disasters (such as a hurricanes or floods); by contrast, the NCIRP is specifically intended to respond to a cyber event.

- Federal policymakers should strengthen the governance and coordination framework for cyber-event response by (a) clarifying and further developing federal government chain-of-command and decision-making mechanisms; (b) clarifying the roles and responsibilities of different agencies; (c) strengthening protocols for government and industry interaction; (d) clarifying thresholds for federal involvement and conditions under which the Stafford Act would apply; (e) further developing the National Cyber Risk Alert Level (NCRAL) system; (f) updating information sharing protocols; and (g) better defining the roles, responsibilities, and authorities of the Unified Coordination Group, which is the interagency body with substantial responsibility for executing the NCRIP.
- The NCIRP should be changed to elevate the role of governors in the event of a successful cyber attack. More generally, improved integration is needed between the

NRF and NCIRP with respect to chains-of-command across government, coordinating mechanisms, thresholds for initiating response efforts and providing federal assistance, and state versus federal authority.

- Governors should further strengthen state-wide governance structures for cyber preparedness.
- Response protocols should provide clarity on the respective roles and responsibilities of law enforcement, who are seeking to preserve information for criminal investigations and public- and private-sector responders seeking to reestablish critical services.
- State and federal agencies and critical infrastructure operators should continue to conduct scenario exercises, such as the National Level Exercise, to practice responses to a cyber attack.

## Paying for Electric Grid Cybersecurity

U.S. utilities are expected to spend about $7 billion on cybersecurity by 2020. An important question is how the costs of these investments will be distributed among utility shareholders and customers. Some entities will be able to seek cost recovery through FERC- or state-approved tariffs; for others, the ability to recover cybersecurity costs will depend on contract terms and market conditions. The challenge for regulators lies in determining whether a particular investment is prudent, or whether other needed investments are being overlooked. Unfortunately, many regulators lack the expertise to make these judgments. In addition, the task is complicated by the "public goods" nature of many cybersecurity investments. To the extent that the benefits of a given investment (or conversely, the costs of a failing to make the investment) extend beyond an individual company, that company can be expected to underinvest from the perspective of the system as a whole. Moreover, current regulatory processes tend to overlook systemic risks.

- DOE should fund efforts—to be undertaken via the new industry-led institute described previously—to understand systemic cyber risks, including risks involving interdependencies and the spillover of consequences from one firm or jurisdiction to another. DOE should also fund research to help regulators better evaluate the potential impacts of cyber attacks and weigh the benefits of cybersecurity investments.
- State PUCs should work with the new institute to normalize cybersecurity best practices and to increase confidence in cybersecurity-related cost-recovery decisions.
- DOE should work with industry and state regulators to develop metrics for evaluating utility investments in cybersecurity. Alternative approaches are conceivable, including approaches that focus on compliance with NERC CIP standards and/or guidance provided by the new industry-led institute. These metrics could then be used in cost-recovery determinations.
- Given the adaptive nature of cyber threats, regulation should encourage continuously improving cyber capabilities. This may require alternative regulatory models that go beyond a reasonable/unreasonable (pass/fail) test and that provide dynamic incentives for ongoing improvement.
- Policymakers and industry should consider supporting cybersecurity investments by entities that may own critical assets but that might otherwise fail to undertake these investments because of insufficient resources or an inability to recover costs. An assistance fund for these situations could be administered by the new institute.
- DOE should continue to advance cybersecurity research and development. Congress should continue to provide resources to enable this support.
- State and federal regulators should proactively engage with companies to establish priorities and needs that

companies have for improving their cybersecurity posture. Where possible, this can be undertaken outside of a docketed proceeding to minimize the risk of broadly disclosing vulnerabilities.

## Conclusions and Next Steps

As noted throughout this report, the electric power industry and the government agencies that oversee it have already done much to improve grid cybersecurity. Our recommendations target areas where gaps or limitations in current policies and practices leave room to further reduce the vulnerability of the electric grid—and the broader U.S. economy—to fast-growing and rapidly evolving cyber threats. Several themes emerge across these recommendations, including the need for greater clarity about the roles and responsibilities of different entities, the need for effective public-private partnerships and improved information sharing, and the need to address incentives and cost-allocation issues in light of the diversity of parties involved and the "public good" nature of many cybersecurity investments.

In the coming months, BPC staff and Initiative co-chairs will reach out to policymakers and stakeholders to advance the recommendations outlined in this report. At the same time, BPC will work to advance progress on challenges that would remain even if all these recommendations were adopted, such as addressing the privacy concerns that continue to present a stumbling block for legislative efforts to enhance information sharing between industry and government. Going forward, BPC's Homeland Security Project will explore further options to resolve these challenges. In the coming months, BPC's Energy Project plans to address the broader issue of electric grid resilience, including the role of modern grid technologies and practices in addressing multiple threats (e.g., weather, physical, cyber, geomagnetic) to the grid.

Founded in 2007 by former Senate Majority Leaders Howard Baker, Tom Daschle, Bob Dole and George Mitchell, the Bipartisan Policy Center (BPC) is a non-profit organization that drives principled solutions through rigorous analysis, reasoned negotiation and respectful dialogue. With projects in multiple issue areas, BPC combines politically balanced policymaking with strong, proactive advocacy and outreach.

BIPARTISAN POLICY CENTER

1225 Eye Street NW, Suite 1000
Washington, DC 20005
(202) 204-2400

WWW.BIPARTISANPOLICY.ORG