NATIONAL ELECTRIC GRID SECURITY AND RESILIENCE ACTION PLAN

Product of the

Executive Office of the President

DECEMBER 2016

Table of Contents

Introduction

The *Joint United States-Canada Electric Grid Security and Resilience Strategy* (Strategy) is a collaborative effort between the Federal Governments of the United States and Canada and is intended to strengthen the security and resilience of the U.S. and Canadian electric grid from all adversarial, technological, and natural hazards and threats. The Strategy, released concurrently with this *National Electric Grid Security and Resilience Action Plan* (Action Plan), details bilateral goals to address the vulnerabilities of the respective and shared electric grid infrastructure of the United States and Canada, not only as an energy security concern, but for reasons of national security. The implementation of the Strategy requires continued action of a nationwide network of governments, departments and agencies (agencies), and private sector partners. This Action Plan details the activities, deliverables, and timelines that will be undertaken primarily by U.S. Federal agencies for the United States to make progress toward the Strategy's goals.

The security and resilience of the integrated U.S. and Canadian electric grid is dynamic. New threats, hazards, and vulnerabilities emerge even as the two countries work to prevent, protect against, and mitigate their potential consequences and to improve their ability to respond to, and recover from, disruptive incidents. Secure and reliable electricity is essential for safe and continued operation of infrastructure owned by businesses, governments, schools, hospitals, and other organizations.

Structure of the Action Plan

The Strategy defines three strategic goals to reduce the systemic risk to the electric grid through combined and aligned organizational, technical, and policy efforts across the public and private sectors. This Action Plan is organized around the same three strategic goals:

1. Protect Today's Electric Grid and Enhance Preparedness
2. Manage Contingencies and Enhance Response and Recovery Efforts
3. Build a More Secure and Resilient Future Electric Grid

Implementation of the Strategy and Action Plan

The Secretaries of Energy and Homeland Security, in coordination with other agencies and stakeholders, will lead the implementation of the Strategy and Action Plan. The Secretaries of Energy and Homeland Security will report annually to the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Science and Technology on progress made in implementing the Strategy and Action Plan in coordination with other agencies. Agencies are also expected to take steps to increase the security and resilience of the electric grid that are not explicitly included in either the Strategy or Action Plan. These efforts will also be included in the progress report to the President. This Action Plan is not intended to, nor does it, create any binding obligations under international law.

The Action Plan focuses on U.S. Federal actions that may be taken within current statutory authorities and resources. Implementation of these actions will occur in consultation with State and provincial

governments, regulators, and utilities, where applicable, and will require the sustained, coordinated, and complementary efforts of individuals and groups from both the United States and Canada, including many who contributed to the development of the Strategy, such as private sector partners, policy makers, and the public. Agencies will engage with private sector partners to the extent permitted by and consistent with applicable law and policy, including, but not limited to, the Federal Advisory Committee Act (FACA), 5 U.S.C. App. 2.

Iterations and future developments of this effort will be guided by each country's Action Plan to pursue the goals of the Strategy. The Strategy sets the groundwork upon which to build future activity, just as multiple prior executive branch efforts informed the Strategy:

- Presidential Policy Directive (PPD) 8, "National Preparedness" (2011), PPD 21, "Critical Infrastructure Security and Resilience" (2013), and PPD 41, "United States Cyber Incident Coordination" (2016);
- Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," Executive Order 13653, "Preparing the United States for the Impacts of Climate Change" (2013), and Executive Order 13744, "Coordinating Efforts to Prepare the Nation for Space Weather Events" (2016);
- Presidential Memorandum, "Climate Change and National Security" (2016);
- *National Space Weather Strategy* and *National Space Weather Action Plan* (2015).

Statement from the Office of Management and Budget

The actions specified in the *National Electric Grid Security and Resilience Action Plan* are intended to inform the policy development process and are not intended as a budget document. The commitment of Federal resources to support these activities will be determined through the usual executive branch budget processes. Implementation of many of the actions in this report may require additional resources, and these resources could be newly authorized or redirected from lower-priority Federal agency activities.

Goal 1: Protect Today's Electric Grid and Enhance Preparedness

Introduction

A secure and resilient electric grid that protects system assets and critical functions and is able to withstand and recover rapidly from disruptions is a priority of the United States. To achieve the goal of protecting today's grid, private sector entities, as well as Federal, state, and local governments, must coordinate their activities through timely and effective information sharing. Information sharing is crucial for ensuring electric grid security, and must involve Federal Government agencies, industry owners, operators, third-party participants from the private and public sector, and other key stakeholders who would benefit from actionable threat, hazard, and vulnerability information. Further, information sharing across and within these groups must be timely and effective to facilitate prudent, efficient, evidence-based investments in the electric grid's security.

Protecting against and mitigating cyber and physical risks to the electric grid in a prioritized manner requires that public and private sector partners continue to work together to: improve their joint understanding of threats, hazards, vulnerabilities, and consequences; prioritize protection and mitigation efforts against cyber and physical risks; build and validate response capabilities and investigate threats; and enhance the current performance of the electric grid and dependent systems.

Isolated or complex events with cascading effects that take place can have major consequences for the electric grid and adversely affect national security, economic stability, and public health and safety. Securing and encouraging investments in risk reduction in the existing electric grid and against such consequences is central to the national security goals of the United States. The United States will strengthen interactions between regulatory structures and operational requirements and augment current incentives to encourage investment in protective measures for both persistent risks and outlier events.

Ensuring the security and resilience of the electric grid requires analyzing system vulnerabilities, including interdependencies, to identify risk management priorities. These measures will improve the electric grid's physical security and cybersecurity and accelerate the restoration of electricity after disruptions.

The United States will pursue the following objectives to achieve the strategic goal of protecting today's electric grid and enhancing preparedness:

- **1.1.** Enhance Information Sharing
- **1.2.** Coordinate and Improve Forensic, Law Enforcement, and Protection Capabilities
- **1.3.** Protect against Major Isolated and Cascading Events
- **1.4.** Align Standards, Incentives, and Investments with Security Goals
- **1.5.** Understand and Mitigate Vulnerabilities from Interdependencies with Other Critical Infrastructure

1.1. Enhance Information Sharing

Measures to improve security and resilience rely on timely and effective information sharing across and within governments and industry. The United States will enhance information sharing across and within governments and industry with partners who own, operate, protect, and rely on the electric grid. The Nation will build organizational capacity to manage risks jointly and establish clear roles and responsibilities for communicating risks and other information. Further, we will develop timely and effective responses to critical threat, hazard, and vulnerability information, including tactical and strategic intelligence data.

The following actions will be taken to enhance information sharing:

1.1.1 The Department of Energy (DOE) will improve tools, protocols, and methods for sharing essential elements of information and situational awareness.

Deliverable: Strategy to identify, develop, and improve situational awareness tools

Timeline: Within 180 days of the publication of this Action Plan

1.1.2 The Department of Homeland Security (DHS), through the National Cybersecurity and Communications Integration Center (NCCIC), will continue to share regular alerts, warnings, and bulletins on cybersecurity vulnerabilities, mitigations, and best practices developed by the U.S. Computer Emergency Readiness Team (US-CERT) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

Deliverable: Various alerts, advisories, and related products and information

Timeline: Ongoing

1.1.3 DHS will provide programs to expand and expedite the flow of cybersecurity information with critical infrastructure partners to enable protection of the electric grid.

Deliverable: Continued enhancement and development of the Cyber Information Sharing and Collaboration Program (CISCP), Enhanced Cybersecurity Services (ECS) program, and the Automated Indicator Sharing (AIS) initiative

Timeline: Ongoing

1.1.4 DHS, through the NCCIC, will collaborate with the Government of Canada and U.S. and Canadian critical infrastructure owners and operators to exchange information on vulnerabilities, threats, mitigations, and best practices concerning the electric grid.

Deliverable: Product exchanges and participation in joint industry briefings

Timeline: Ongoing

1.1.5 DHS, in coordination with other Federal partners including DOE and other Sector Specific Agencies (SSAs) as warranted through the existing partnership framework model, will continue to convene threat and information sharing engagements comprised of government entities and private-sector partners, including those from

the Electricity Subsector. Leveraging lessons learned and best practices, DHS will work closely with SSAs to help inform products and resources intended to mitigate risk and inform security decisions.

Deliverable: Targeted threat outreach and information sharing engagements

Timeline: As needed (threat-dependent)

1.1.6 DOE, in coordination with electric sector stakeholders, will further enhance cyber incident response and information sharing programs to facilitate the exchange of cybersecurity information to enable protective actions or response strategies, such as the Cybersecurity Risk Information Sharing Program (CRISP).

Deliverable 1: Continued enhancement and exercise of cyber incident response coordination and information sharing procedures, through existing platforms as appropriate

Timeline 1: Within 120 days of the publication of this Action Plan

Deliverable 2: Demonstrated ability to share and analyze information related to control system networks across multiple private sector sites

Timeline 2: Within 180 days of the publication of this Action Plan

1.1.7 DOE, as a next step to the Joint Electromagnetic Pulse Resilience Strategy, which was developed by DOE and the Electric Power Research Institute (EPRI), will generate and publically disseminate specific actions for DOE to coordinate with other Federal agencies, particularly the SSAs, national laboratories, EPRI, electric utilities, and other stakeholders through the Electricity Subsector Coordinating Council (ESCC) and the Energy Sector Government Coordinating Council (EGCC) to reduce electromagnetic pulse (EMP) vulnerabilities to the electricity sector.

Deliverable: DOE EMP Resilience Action Plan

Timeline: Within 30 days of the publication of this Action Plan

1.1.8 DOE, in coordination with other agencies, will convene a discussion around roles and responsibilities for meeting industry partner information needs in the context of the electric grid. These include ensuring appropriate industry personnel have security clearances and working with the Electricity ISAC (E-ISAC) and the ESCC to disseminate both unclassified and classified information.

Deliverable: Analysis of information dissemination needs

Timeline: Within 120 days of the publication of this Action Plan

1.1.9 DOE will improve infrastructure security preparedness by working with government and industry partners on updating tools and best practice guidelines.

Deliverable: Improvements to the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) to address the changing threat landscape

Timeline: Within 1 year of the publication of this Action Plan

1.1.10 DHS will ensure awareness of cyber risk and assessment tools that can be used by industry to measure and improve security, such as the ICS-CERT Cybersecurity Evaluation Tool (CSET) and other assessment offerings.

Deliverable: DHS CSET and assessment tools

Timeline: Ongoing

1.1.11 DOE, in coordination with DHS, the Department of Defense (DOD), and other agencies; state, local, territorial, and tribal (SLTT) government partners; and the electric industry, will implement an energy sector exercise strategy through a robust exercise program. The program will be aligned to the National Exercise Program, the National Planning System, and associated response plans, including the National Cyber Incident Response Plan. It will build on existing exercises and include cross-sector government coordination with critical infrastructure SSAs and participation in industry-hosted exercises to enhance the ability of the energy sector to respond to and recover from catastrophic events, including through Black Start capability.

Deliverable: An exercise strategy that outlines goals, objectives, and planned exercise program activities

Timeline: Within 1 year of the publication of this Action Plan

1.1.12 The Department of Justice (DOJ), through the Federal Bureau of Investigation (FBI) will share, as appropriate, including via the E-ISAC and NCCIC, information relevant to, and stemming from, investigative activity, including activity undertaken pursuant to PPD 41.

Deliverable: FBI Liaison Alert System (FLASH) reports and FBI Private Industry Notifications (PINs)

Timeline: Ongoing

1.1.13 DOJ, operating through the FBI, in conjunction with DHS, DOE, the U.S. Intelligence Community, the North American Electric Reliability Corporation (NERC), law enforcement partners, and others as appropriate, will engage the electric industry and private sector through "campaigns" based on emerging cyber threats. More specifically, when an adversary prepares to engage, or engages in, cyber network exploitation activity that targets the electric sector, the FBI will, as appropriate, create targeted briefings and engage with the sector to provide both technical and contextual threat and vulnerability information to aid the sector in defending their systems. Briefings can be held at the unclassified or classified level depending on the topic, and information provided will be the result of ongoing investigative activity.

Deliverable: Contextual briefings to provide enhanced awareness, defensive capabilities, and lessons learned

Timeline: As needed

1.2 Coordinate and Improve Forensic, Law Enforcement, and Protection Capabilities

Federal Government agencies play an essential role in identifying threats to the electric grid. In a dynamic threat environment, the continued improvement of tools and methods to discern threats more effectively is critical. The United States will coordinate and improve processes for detecting, monitoring, analyzing, reporting, investigating, and mitigating threats to the electric grid. The Nation will also improve coordination between responsible government agencies and electric grid owners and operators to defend the electric grid.

The following actions will be taken to coordinate and improve forensic, law enforcement, and protection capabilities:

1.2.1 DOE, in coordination with the electric industry and other agencies as appropriate, will develop a malware analysis platform for assessing threats to the electric grid and leverage currently available law enforcement platforms and cyber analysis capabilities where applicable, including design, development, testing, validation, and transition to practice of a distributed malware analysis platform. This platform will enable DOE to reverse-engineer malware to help determine any negative effects and develop a mitigation process to neutralize the malware.

Deliverable: Virtual energy sector advanced digital forensics platform

Timeline: Within 1 year of the publication of this Action Plan

1.2.2 DOJ, through the FBI, will conduct appropriate investigative activity to respond to threats to the electric grid, including as warranted by PPD 41 and in coordination with other relevant agencies. These activities will include conducting appropriate law enforcement and national security investigative activity at the affected entity's site; collecting evidence and gathering intelligence; providing attribution; linking related incidents; identifying additional affected entities; identifying threat pursuit and disruption opportunities; developing and executing courses of action to mitigate the immediate threat; acting as the main hub for coordination with other law enforcement agencies; and facilitating information sharing and operational coordination with asset response.

Deliverable: Engagement in ongoing threat response activities

Timeline: Ongoing

1.3 Protect against Major Isolated and Cascading Events

Protection of the electric grid against major events necessitates prudent investments, more robust designs, and an all-hazards—adversarial, natural, and technological—risk approach to understanding system performance and vulnerabilities across generation, transmission, and distribution systems. The United States will continue to work in coordination with owners, operators, and other stakeholders, including SLTT governments and NERC, to protect and harden existing features of the electric grid,

identify and mitigate system-wide criticalities, and put in place measures that reduce system-wide risk. The Nation will work with partners to develop guiding principles and technical means, including automated and manual approaches, to prevent events, including cascading blackouts.

The following actions will be taken to protect against major isolated and cascading events:

1.3.1 DOE, in coordination with SSAs as needed and other partners as appropriate, will develop methods to assess the risks of natural and human-made disasters on the electric grid and interdependencies to other sectors. DOE will coordinate with others to use the methods to assess risks and interdependencies.

Deliverable: Assessment of the risk to the electric grid and interdependent sectors from high-consequence threats and hazards

Timeline: Within 18 months of the publication of this Action Plan

1.3.2 DHS, through the Regional Resiliency Assessment Program and in coordination with other agencies as appropriate, will continue to conduct voluntary, cooperative assessments of specific, critical electric infrastructure within a designated geographic area and conduct a regional analysis of the surrounding infrastructure to address a range of infrastructure resilience issues that could have regional or national consequences.

Deliverable: Assessment of the electric power sector and lifeline functions focused on regional resilience

Timeline: Within 1 year of the publication of this Action Plan

1.3.3 DOE, in collaboration with SLTT communities, will support the development of plans to facilitate and accelerate the restoration of energy systems during emergencies.

Deliverable: Regional/state energy assurance plans

Timeline: Within 1 year of the publication of this Action Plan

1.3.4 DOE, in coordination with industry, will continue to develop operational tools that complement current efforts in the private sector to mitigate cascading events.

Deliverable: Dynamic contingency analysis tool

Timeline: Within 180 days of the publication of this Action Plan

1.3.5 DOE, in coordination with other agencies, will investigate the need for revised procedures to protect or restore the reliability of critical electric infrastructure and complete the analytical report titled "Grid Modernization Laboratory Consortium (GMLC) Metrics Development Project (1.1)" under the Grid Modernization Initiative

Deliverable: GMLC report

Timeline: Within 180 days of the publication of this Action Plan

1.3.6 DOE, in coordination with existing exercise formats like GridEx, where appropriate,

will train and exercise the Electric Grid Security Emergency authority as required by the Fixing America's Surface Transportation (FAST) Act.

Deliverable: Exercise, coordinated with existing exercise programs, where appropriate, to test procedures for executing the Electric Grid Security Emergency authority enumerated in the FAST Act

Timeline: Within 1 year of the publication of this Action Plan

1.3.7 DHS, through its Cyber Resilience Review (CRR) and CSET, will offer risk-based assessments to supplement existing risk management activities in the private sector.

Deliverable: Cyber risk assessments made available to private sector partners

Timeline: Ongoing

1.4 Align Standards, Incentives, and Investment with Security Goals

Investment planning for security and resilience measures necessitates a clear assessment of the potential value of the proposed investments and operating costs, and an alignment of those costs with regulatory processes and tools for prudent cost recovery, including tools for valuing security. The United States will develop tools to connect security and resilience decision-making to infrastructure investment and financing, and to improve the balance of investment in risk-reduction measures and response and recovery investments.

The following actions will be taken to align standards, incentives, and investment with security goals:

1.4.1 DOE, in coordination with other agencies, will inform decisions incorporating security and resilience concerns—especially to improve the balance of investment in risk reduction versus response and recovery investments—including value proposition.

Deliverable: A project plan for reports on key questions informing policymaker and stakeholder discussions and decisions, that incorporates expertise from across DOE and other agencies

Timeline: Within 180 days of the publication of this Action Plan

1.4.2 DOD, in coordination with DHS, DOE, and other agencies, will work with utilities to identify segments of the commercial electric grid that most directly support key national security missions.

Deliverable: Identification of the defense critical electric infrastructure and associated owners and operators

Timeline: Within 180 days of the publication of this Action Plan

1.4.3 DHS, DOE, and DOD will engage with the Federal Energy Regulatory Commission (FERC) and commercial electric grid owners and operators of the defense critical electric infrastructure to determine how they can increase security and resilience of this infrastructure and expedite recovery in case of disruption.

Deliverable: Coordinated DHS, DOE, and DOD plan, including other agencies as appropriate, to engage with electric infrastructure owners and operators

Timeline: Within 180 days of the publication of this Action Plan

1.4.4 DHS and DOE, in coordination with DOD and other agencies as appropriate, will work with utilities to develop methods to conduct and subsequently prioritize vulnerability and security assessments of critical electric infrastructure and dependent lifeline functions and assets.

Deliverable: Multi-year DHS strategy for assessing infrastructure security

Timeline: Within 1 year of the publication of this Action Plan

1.4.5 The National Institute of Standards and Technology (NIST), in coordination with DOE and other stakeholder agencies and with private-public partnership organizations such as the NIST-initiated Smart Grid Interoperability Panel (SGIP) non-profit membership organization, will work with the private sector to support the coordination of industry-led development of smart grid interoperability standards that will promote technology deployment and improve system integration.

Deliverable: Open Field Message Bus (OpenFMB), as coordinated by SGIP with multi-stakeholder participation, which would support distributed intelligent nodes to interact with each other through loosely coupled, secure peer-to-peer messaging for devices and systems at the edge of the electric grid, as well as the additional analysis to evaluate and enhance cybersecurity within OpenFMB to support secure deployments

Timeline: Within 1 year of the publication of this Action Plan

1.4.6 DOE, in coordination with other agencies, will identify potential opportunities to create incentives to industry to deploy new technologies that will mitigate and identify risks to the electric grid and also take operational practices into account.

Deliverable: Technology innovation coordination strategy

Timeline: Within 180 days of the publication of this Action Plan

1.4.7 DOE will engage the electric power industry on supporting Design Basis Threat (DBT) analysis for critical facilities.

Deliverable: Educational briefings/webinars to industry on how to best use the recently developed DBT guide to evaluate the effectiveness of the security of their facilities and operations and to design appropriate systems to protect their assets

Timeline: Within 180 days of the publication of this Action Plan

1.5 Understand and Mitigate Vulnerabilities from Interdependencies with Other Critical Infrastructure

The U.S. electric grid is a highly interdependent and complex system on which societal functions depend. Critical infrastructure sectors have grown increasingly reliant on continued grid operations. Likewise, in order to function, the electric grid increasingly depends on other infrastructure, such as communications systems necessary for controlling electric grid systems. The United States will work with owners, operators, and other stakeholders to improve monitoring of system-wide performance of the electric grid, improve forecasting and modeling of effects on dependent systems, and work through public-private partnerships to address vulnerabilities, including social vulnerabilities associated with dependence on the electric grid. The Nation will enhance our understanding of how different demographics may be more vulnerable in the face of disruptions. In addition, we will work with owners, operators, and other stakeholders to identify and mitigate both cyber and physical risks to and from the electric grid and other types of infrastructure, including the potential for increased vulnerability introduced by the internet of things, and electric grid interdependencies on water, natural gas, telecommunications, transportation, financial services, and national defense.

The following actions will be taken to understand and mitigate vulnerabilities from interdependencies with other critical infrastructure:

1.5.1 DOE, in coordination with other agencies, will identify and map interdependencies to improve the ability to monitor system-wide performance of the electric grid and to forecast and model impacts on dependent systems.

Deliverables: Extreme event modeling and GMLC regional partnerships

Timeline: Within 180 days of the publication of this Action Plan

1.5.2 The Department of Health and Human Services (HHS), in coordination with other agencies, will provide data, tools, methods, and peer-reviewed publications to support situational awareness of health and social vulnerabilities associated with dependence on electric grid systems.

Deliverables: Data, tools, and peer-reviewed publications to advance community situational awareness, preparedness, and resilience activities for electricity-dependent, at-risk populations that may be affected by energy security and reliability

Timeline: Within 240 days of the publication of this Action Plan

1.5.3 DOE, in coordination with other agencies, will develop models and methods to understand interdependencies related to the complex system of the electric grid.

Deliverables: GMLC architecture and interdependencies modeling tools

Timeline: Within 180 days of the publication of this Action Plan

Goal 2: Manage Contingencies and Enhance Response and Recovery Efforts

Introduction

The electric grid is composed of a highly diverse set of assets, systems, and functions, and is primarily owned and operated by the private sector in the United States or by provincial, territorial, investor-owned, and municipal utilities in Canada. In part because of its complexity and physical size, the electric grid is vulnerable to disruptions from many types of hazards and threats. Enhancing response and recovery efforts depends on collaboration with all stakeholders. In the face of evolving physical threats, technological risks, cyber incidents, and natural hazards, the electric power industry has recognized the increased need for enterprise-level security and resilience by investing in response and recovery capabilities, including business continuity plans and assessments of the vulnerabilities of critical single-point assets, such as power plants, and networked features, such as transmission lines and cyber systems. The United States will work with public and private partners, especially electric grid owners and operators, to manage contingencies and enhance response and recovery efforts more effectively.

The United States will pursue the following objectives to achieve the strategic goal of managing contingencies and enhancing response and recovery efforts:

2.1. Improve Emergency Response and Continuity

2.2. Support Mutual Assistance for Recovering from Disruptions Caused by Physical and Cyber Threats

2.3. Identify Dependencies and Supply Chain Needs During Emergencies

2.4. Recover and Rebuild

2.1 Improve Emergency Response and Continuity

Improving the ability of the United States to respond to an emergency and to enhance continuity of operations is imperative to building a resilient, reliable, safe, and secure electric grid, a national priority vital to competitiveness, jobs, energy security, national security, and the clean energy future for the United States. The United States will improve the ability of the public and private sectors to respond to electric grid-related emergencies through enhancing capabilities to identify the location of the problem and re-route power around affected areas. The Nation will improve the ability to assess the state of the electric grid by supporting research, development, and deployment of initiatives such as "smart grid" technology and of technological advances in electric grid monitoring. As a result, utilities can quickly and efficiently respond to power outages as well as improve business continuity when there are cyber incidents. These technologies will be designed to boost the efficiency of outage response teams and reduce utilities' operational costs by identifying where resources are needed to make repairs.

The United States will also seek to encourage the expansion of public and private resources for response to and recovery from major loss-of-power events through electric grid modernization. Additional resources should include more robust equipment and systems, research and development for more resilient critical electric grid components, and hardening of assets. The Nation will coordinate assistance programs as appropriate to encourage the public and private sectors to refine existing response and recovery plans, develop new ones, and engage in training for and exercising of those plans.

The following actions will be taken to improve emergency response and continuity:

2.1.1 DOE will continue to engage with electric power public and private partners to encourage the development and implementation of secure smart grid technologies.

Deliverable: Analysis of the electric power sector outlining the level of implementation of smart grid technologies in electric grid infrastructure

Timeline: Within 1 year of the publication of this Action Plan

2.1.2 DHS, through the Federal Emergency Management Agency (FEMA) and in coordination with DOE and other agencies, will finalize and publish an all-hazards Power Outage Incident Annex (POIA) to the Federal Interagency Operations Plans (FIOPs) for response and recovery.

Deliverable: POIA

Timeline: Within 6 months of the publication of this Action Plan

2.1.3 DHS, in coordination with other agencies, will produce the National Cyber Incident Response Plan (NCIRP).

Deliverable: Updated NCIRP

Timeline: Within 180 days of the publication of this Action Plan

2.1.4 DHS, through FEMA, in coordination with DOE, DOJ through the FBI, other agencies, SLTT governments, and industry, will plan and exercise response procedures for incidents that may exploit sector interdependencies and that would require cross-sector coordination. The plans and procedures should complement PPD 41, the National Planning Frameworks, and, for significant cyber incidents, the NCIRP.

Deliverable: Cross-sector electric grid response exercise

Timeline: Within 240 days of the publication of this Action Plan

2.1.5 DOE will increase the ability to monitor grid impacts and restoration through enhancing situational awareness tools such as the Environment for Analysis of Geo-Located Energy Information (EAGLE-I) by integrating the ability to intake data directly from energy sector partners, perform big data analysis as appropriate, and share energy sector situational awareness with interagency mission partners.

Deliverable: Data coverage expansion of the EAGLE-I tool and additional functions for use by the response community

Timeline: Within 120 days of the publication of this Action Plan

2.1.6 DOE, in coordination with regulatory agencies and the electric power industry and in support of the *National Space Weather Strategy* and the *National Space Weather Action Plan*, will define data requirements that facilitate a centralized reporting system to collect real-time information on the status of the electric power transmission and distribution system during geomagnetic storms.

Deliverable: Defined data requirements

Timeline: Within 90 days of the publication of this Action Plan

2.2 Support Mutual Assistance for Recovering from Disruptions Caused by Physical and Cyber Threats

The speed with which power systems can be restored after a disruption depends, in part, on the resources available for recovery. Utilities in the United States have a long history of providing mutual assistance in the event of disruptions through agreements, whereby requesting utilities typically reimburse responding companies on a cost-recovery basis. The United States will continue to explore organizational and regulatory options to enhance the effectiveness and efficiency of these mutual assistance groups, especially in terms of cross-border collaboration. The Nation will encourage utilities to collaborate when there are cyber incidents by developing plans and capabilities, assigning roles, and developing procedures to respond.

The following action will be taken to support mutual assistance for recovering from disruptions caused by physical and cyber incidents:

2.2.1 DOE, in coordination with interagency partners and in accordance with PPD 41, will explore options for supporting private sector response efforts to a significant cyber incident in the energy sector.

Deliverable: Practical process for DOE to support the private energy sector in response to a significant cyber incident in the energy sector

Timeline: Within 1 year of the publication of this Action Plan

2.3 Identify Dependencies and Supply Chain Needs During Emergencies

Because the U.S. and Canadian electric grids are so interconnected, communities, businesses, and industries may not be fully aware of their dependence on an integrated electric grid infrastructure that depends on interconnected operations in both countries. Likewise, the operation of the electric grid depends on other infrastructure, such as communications, fuel, and water. The United States will continue to work to model these complex relationships, to identify vulnerabilities and points of criticality, and to address those risks. The Nation will help states and regions better understand their electric grid risks and assist them in adopting more effective resilience strategies through modeling and identifying supply chain vulnerabilities.

The following actions will be taken to identify dependencies and supply chain needs during emergencies:

2.3.1 DHS and DOE, in coordination with other agencies, will develop a better understanding of supply chains for emergency replacement equipment and fuels, identifying upstream and downstream impacts.

Deliverable: Study identifying supply chain vulnerabilities during an electric grid emergency

Timeline: Within 1 year of the publication of this Action Plan

2.3.2 DOE, in coordination with applicable state energy officials and private sector partners, will conduct a review of state energy assurance plans to account for dependencies and supply chain needs affecting the energy sector and will develop actionable methods for addressing identified gaps and shortfalls.

Deliverable: Formal review of state energy assurance plans to identify supply chain and dependency issues

Timeline: Within 1 year of the publication of this Action Plan

2.3.3 DOE, in support of the FAST Act and in coordination with other agencies, will develop a plan to reduce the risk to grid reliability and resilience posed by the loss of critical power transformers due to the impacts of physical or cyber incidents or natural hazards.

Deliverable: Technical assessment of the strategic transformer reserve requirements submitted to Congress

Timeline: Within 180 days of publication of this Action Plan

2.4 Recover and Rebuild

Recovery does not end as the result of immediate power restoration. Improvements in the electric grid that go beyond restoration of previously existing infrastructure are likely to need approval from state regulatory agencies that have the authority to determine whether rates may be raised or revenues used to cover improvements. The U.S. Government and its partners will explore and study cost-effective proposals to improve resilience during reconstruction after disruptions, including the effects of climate change. The United States will also consider any regulatory changes that are recommended to cover the costs of these improvements.

The following action will be taken to recover and rebuild:

2.4.1 DOE, in coordination with DHS through FEMA and private industry partners, will explore whether feasible options for providing financial assistance or other incentives to smaller utilities, in particular, are applicable and appropriate to incorporate improvements to energy infrastructure promoting security and resilience beyond the status quo.

Deliverable: Feasibility report

Timeline: Within 1 year of the publication of this Action Plan

Goal 3: Build a More Secure and Resilient Future Electric Grid

Introduction

The United States and Canada are working to build a more secure and resilient electric grid that is responsive to a variety of threats, hazards, and vulnerabilities. To achieve this, the electric grid will need to be more flexible and agile, with an architecture into which new technologies can be readily incorporated. As the electric grid evolves, the electric grid owners and operators are integrating a variety of approaches to risk management, including more diverse and distributed generation that could provide a more resilient and secure electric grid. Greater use of intermittent sources of power will elevate the role of energy storage systems and enable a more flexible system. In the future, the electric grid will likely draw on new combinations of generation, incorporate evolving energy storage and distribution systems, and accept new technologies, many of which are emerging much more rapidly than the electric grid technologies of the last century. Owners and operators will need to protect the electric grid from new and evolving risks, cyber threats in particular, that stem from such technologies. Utilities have varying levels of resources to make the investments necessary to meet their needs, so incentives that go beyond those provided for by current policy may be needed. In addition, global climate change will increasingly create new stresses to which the electric grid will need to adapt.

The electric grid gains reliability from the development and integration of new technologies, but technology also introduces new potential security vulnerabilities. Expanding networks of sensors are improving the amount, speed, and quality of data generated about the electric grid. With advanced computation and analytics, a more accurate picture of electric grid status is becoming available in real time, providing greater decision capabilities and more reliable automated responses to events. These changes also increase the number of vulnerabilities to cyber incidents.

The United States will pursue the following objectives to achieve the strategic goal of building a more secure and resilient electric grid:

- **3.1.** Understand and Manage New and Evolving Risks from Electric Grid Technologies and Electric Grid Design
- **3.2.** Develop and Deploy Security and Resilience Tools and Technologies
- **3.3.** Integrate Security and Resilience into Planning, Investment, Policy Decision-Making, and Coordination Regarding Cross-Border Grid Integration Between the United States and Canada
- **3.4.** Understand and Mitigate Risks Posed by Climate Change
- **3.5.** Develop a Highly Skilled Workforce

3.1 Understand and Manage New and Evolving Risks from Electric Grid Technologies and Electric Grid Design

The electric grid in the United States is encountering new and evolving risks that arise, in part, from the rapid growth of new technologies within and connected to the electric grid. As new sources of energy generation are increasingly incorporated into the electric grid, they drive adaptations in new technologies. In addition, impacts from increasingly severe weather events due to climate change, as well as space-weather and other high-impact events, create the requirement for continuous assessment and design improvements. To the extent possible, the United States will identify, understand, and address these emerging and evolving threats, hazards, and vulnerabilities. The Nation will seek to ensure that continued integration of electric grid and information technology infrastructures is a security benefit despite any new challenges posed by enhanced integration.

The following actions will be taken to understand and manage new and evolving risk from electric grid technologies and electric grid design:

3.1.1 DOE, in collaboration with DHS and the Electricity Subsector Coordinating Council (ESCC), will facilitate a Resilience Roadmap for the energy sector with milestones out to 2040, with the objective of increased implementation of resilience into U.S. transmission and distribution systems.

Deliverable: Resilience Roadmap

Timeline: Within 1 year of the publication of this Action Plan

3.1.2 DOE, through the ESCC and working with ISACs, will continue to facilitate a dialog between key stakeholders in the United States and Canada on best practices to amplify and further augment actionable information to utilities in a timely manner to enable utilities to protect against emerging threats.

Deliverable: Working group with key stakeholders

Timeline: Ongoing and as needed

3.1.3 DOE, in coordination with DHS, FERC, other agencies, the ESCC and the Critical Manufacturing Sector Coordinating Council as appropriate, will develop a better understanding of products and infrastructure supply chains related to the electric grid, and their potential vulnerabilities, identifying upstream and downstream impacts. A working group of manufacturers, energy asset owners, and trade associations will be appointed to identify the most pressing concerns within equipment supply chains.

Deliverable: Outreach plan on supply chain security issues and a working group report of findings to the manufacturing and energy sector coordinating councils in order to characterize supply chain risks to the electric grid, and to identify best practices for managing such risks.

Timeline: Within 180 days of the publication of this Action Plan

3.1.4 DOE will conduct modeling and testing of grid components to improve

understanding of susceptibility to threats, such as EMP and geomagnetic disturbances, in partnership with other agencies, the national laboratories and industry.

Deliverable: Report on assessment methodology and results

Timeline: Within 2 years of the publication of this Action Plan

3.1.5 DOE, in coordination with DHS, the Department of Commerce, and other agencies and stakeholders in the electricity sector, and in support of the *National Space Weather Strategy* and the *National Space Weather Action Plan*, will develop plans to provide monitoring and data collection systems. The plans will inform a system-wide, real-time view of geomagnetically induced currents (GICs) at the regional level and, to the extent possible, display the status of power generation, transmission, and distribution systems during geomagnetic storms.

Deliverable: Plan for national GIC and grid monitoring system and delineation of responsibilities for deployment

Timeline: Ongoing

3.1.6 DOE will conduct research and design sensors that will enable detection and monitoring of grid anomalies to enable full integration of networked microgrids, including developing both advanced, secure, low-cost sensors and advanced distribution management system applications.

Deliverable: Development of a design support tool that is used by at least one remote community for designing an alternating or direct current microgrid for off-grid applications

Timeline: Within 2 years of the publication of this Action Plan

3.1.7 DOE will facilitate the development by the United States and Canada of a framework for convening stakeholders in states, provinces, and the private sector to improve cross-jurisdictional coordination on mitigation, response, and recovery efforts for a range of threats.

Deliverable: Mechanism that outlines regular exchanges to address cross-jurisdictional issues

Timeline: Within 180 days of the publication of this Action Plan

3.1.8 DOE will work with the North American SynchroPhasor Initiative and other stakeholders to facilitate a panel to determine industry lessons learned and best practices to detect and mitigate electric grid anomalies.

Deliverable: Workshop proceedings that include research, techniques, and best practices to detect and mitigate electric grid anomalies

Timeline: Within 180 days of the publication of this Action Plan

3.2 Develop and Deploy Security and Resilience Tools and Technologies

In the context of increased distributed generation, the United States will pursue the technological, institutional, and architectural evolution of the electric grid when it enhances security and resilience. The United States will work with partners to research, identify, develop, assess, and facilitate the adoption of new technologies where they will improve electric grid security and resilience, and explore whether alternative solutions are preferable where new technologies fail to improve security and resilience. The Nation also will work to reduce vulnerabilities to critical, hard-to-construct components like large power transformers by incorporating more robust advanced components and power electronics into next-generation equipment. To achieve an electric grid that is able to heal itself following major disruptions, we will work to develop a system where power flow can be quickly reconfigured, frequencies can be stabilized, and voltages can be controlled. The United States will identify, develop, and facilitate the adoption, where appropriate, of advanced system design tools to mitigate cyber threats in an increasingly decentralized electric system.

The following actions will be taken to develop and deploy security and resilience tools and technologies:

3.2.1 DOE, in coordination with other agencies as appropriate, will support the development of guidance for electric grid structure and functions to address security and resilience objectives through the application of electric grid architecture.

Deliverable: Initial architecture framework under the GMLC

Timeline: Within 180 days of the publication of this Action Plan

3.2.2 DOE, in coordination with other agencies, will develop innovative electric grid modeling approaches that improve computational speeds by several orders of magnitude and validate power system models in real-world environments using real-world data.

Deliverables: Tested advanced computational and modeling capabilities, including dynamic operation, real-time analysis, and predictive response to simulate power system behavior in a real-world environment

Timeline: Within 2 years of the publication of this Action Plan

3.2.3 DOE will identify research needs for next-generation electric grid transmission and distribution components to make them more resilient in a future electric grid.

Deliverable: Workshop to inform a multi-year program plan

Timeline: Within 180 days of the publication of this Action Plan

3.3 Integrate Security and Resilience into Planning, Investment, Policy Decision-Making, and Coordination Regarding Cross-Border Electric Grid Integration between the United States and Canada

Utilities, electric grid operators, and government authorities in the United States have a long history of collaborating on planning for investments and regulatory policy. As the electric grid becomes more

agile and multi-directional, and new threats like climate change evolve, institutions will need to enhance their capabilities for modeling and quantitative risk analysis to characterize electric grid threats, hazards, and vulnerabilities more effectively; understand the consequences of loss-of-power events; and support risk-informed decisions. The United States will explore improved mechanisms to value prudent investments for security and resilience adequately and to harmonize security and reliability regulation with the evolving strategic environment for the electric grid. Where current processes are poorly aligned with the goal of improving electric grid security and resilience, the Nation will identify the causes of misalignment and provide information for appropriate adjustments, including through cost recovery.

The following actions will be taken to integrate security and resilience into planning, investment, policy decision-making, and coordination regarding cross-border electric grid integration between the United States and Canada:

3.3.1 DOE will convene a workshop to examine existing methods and potential advancements in data sharing between utilities and power marketing authorities with respect to planning studies and modeling data.

Deliverable: Workshop report that outlines the requirements for and benefits of regional planning studies

Timeline: Within 270 days of the publication of this Action Plan

3.3.2 DOE, in coordination with DOD and other agencies as appropriate, under existing engagements and authorities, will facilitate workshop discussions on microgrids and energy resilience with utilities, sharing lessons learned and modeling techniques.

Deliverable: Workshop report

Timeline: Within 120 days of the publication of this Action Plan

3.3.3 DOE will facilitate a discussion with FERC, NERC, and other organizations as appropriate, such as the National Association of Regulatory Utility Commissioners, to provide technical assistance and identify and encourage approaches that include security and resilience considerations into cost recovery criteria for the electric grid.

Deliverable: Report outlining consistent methods of cost recovery and investment planning among Federal, state, and regional entities

Timeline: Within 1 year of the publication of this Action Plan

3.3.4 DOE will facilitate studies on the effects of Distributed Energy Resources (DER) on the electric grid to increase resilience.

Deliverable: GMLC analysis of DER effects

Timeline: Within 180 days of the publication of this Action Plan

3.3.5 DOE will conduct a study into the backup methods of communication currently used by generation and transmission operators and balancing authorities. The study will include recommendations for effective communications during natural disasters and other emergencies.

Deliverable: Report on backup methods of communication with recommendations

Timeline: Within 1 year of the publication of this Action Plan

3.3.6 DOE and DHS will develop a plan for conducting stakeholder outreach through workshops with municipal utilities and cooperatives to understand their unique security and resilience challenges, and will provide technical assistance on incorporating security and resilience into their planning and operational practices.

Deliverables: Two regional technical assistance workshops

Timeline: Within 180 day of the publication of this Action Plan

3.3.7 The United States Department of Agriculture (USDA) Rural Utilities Service, in coordination with DOE, will support existing and new developments in future electric grid security and resilience, including renewables, "smart-grid" technology, energy efficiency and effectiveness, hardening and redundancy improvements, cost containment, system delivery flexibility, climate change solutions for flooding and wildfires, and sustainable solutions of reliable electricity and transmission.

Deliverables: Continued investment in U.S. rural electric infrastructure and development of effective performance measurements

Timeline: Ongoing

3.4 Understand and Mitigate Risks Posed by Climate Change

As global temperatures rise, wildfires, drought, and high demand for electricity put stress on the energy infrastructure. Severe weather is a leading cause of power outages and fuel supply disruption and the principal contributor to an observed increase in the duration of U.S. power outages since 2000. Climate change is projected to cause an increase in the frequency, duration, and intensity of many types of extreme weather. The United States will support research and innovation through new or existing initiatives that will make our electric grid more flexible and more efficient as we work toward a cleaner, more climate-resilient energy system.

The following actions will be taken to understand and mitigate risks posed by climate change:

3.4.1 DOE, in coordination with other agencies and stakeholders, including through the Partnership for Energy Sector Climate Resilience, will continue to encourage and facilitate enhanced resilience planning and implementation through the electricity sector.

Deliverables: Publication of best practices for utilities to conduct vulnerability self-assessments and develop plans for enhanced climate resilience and of resilience planning guides and synthesis reports to summarize related materials developed by partners.

Timeline: Ongoing.

3.4.2 DOE and DHS, in coordination with other agencies per the Presidential Memorandum,

"Climate Change and National Security," issued on September 21, 2016, will develop an Action Plan to identify specific steps that are required to perform the Climate and National Security Working Group's functions. The Action Plan shall also include specific objectives, milestones, timelines, and identification of agencies responsible for completion of all actions described therein.

Deliverable: Action Plan that supports the objectives of the Presidential Memorandum "Climate Change and National Security"

Timeline: Within 90 days of the publication of the Presidential Memorandum

3.5 Develop a Highly Skilled Workforce

As the electric grid system evolves and new threats emerge, the United States, in coordination with industry and academia, will strive to advance the training and education of next-generation workers. The Nation will work to address the gap created by the retirement of existing highly skilled workers. We will also help ensure awareness of future employment opportunities to prepare for work in this sector.

The following action will be taken to develop a highly skilled workforce:

3.5.1 DOE and DHS will work with key U.S. interagency partners and the ESCC to develop standardized curricula and training materials for utilities to educate their workforces on protection against a range of emerging threats

Deliverable: A webinar and an online resource that provides training materials to utilities for workforce development

Timeline: Within 240 days of the publication of this Action Plan

Conclusion

A robust, secure, and resilient electric grid is essential to serving the needs of the public in terms of health and safety, economic security, and national security. A physical incident, cyber incident, or natural event affecting the electric grid can be potentially catastrophic for our way of life. A security mechanism that works today may not be effective tomorrow—the ways and means of threats and hazards constantly change, whether by design of a cyber incident or through unpredicted climate trends. Electric grid stakeholders must prepare for disruptive events and continue to work to address the potential threats, hazards, and vulnerabilities in the systems they manage.

In accordance with this Action Plan, Federal Government agencies will continue to work with utility owners and operators and with SLTT governments to maintain preparedness, obtain predictive information, and protect vulnerabilities. Based on the significance of critical infrastructure, such as the electric grid, in broader national and economic security strategies, it is in the interest of the Federal Government to ensure updates and adaption to evolving and emerging risks. To fulfill the Federal vision for energy grid security and resilience, as the very nature of the electric grid itself continues to evolve, establishing and maintaining security measures for the electric grid will continue to require a significant dedication of resources from all participants. The electric grid transcends political and geographic boundaries, and its operations shift based on demand or availability of natural resources. The United States shares responsibility with Canada for making every reasonable effort to fulfill our commitment to the electricity system of the 21st century.

Bibliography

Department of Energy. "Launch of the Grid Modernization Laboratory Consortium." Last updated November 17, 2014. http://energy.gov/articles/launch-grid-modernization-laboratory-consortium.

Department of Energy. Office of Electricity Delivery and Energy Reliability. *Insurance as a Risk Management Instrument for Energy Infrastructure Security and Resilience*. 2013.

Department of Homeland Security. "National Infrastructure Protection Plan." Last updated June 16, 2015. https://www.dhs.gov/national-infrastructure-protection-plan.

Executive Office of the President (EOP). "Principles for Federal Engagement in Standards Activities to Address National Priorities." EOP Memorandum M-12-08. January 17, 2012.

––––––––.*U.S. Open Data Action Plan*. Washington, DC: EOP, May 9, 2014.

Executive Order 13636. "Improving Critical Infrastructure Cybersecurity." February 12, 2013.

Executive Order 13653. "Preparing the United States for the Impacts of Climate Change." November 1, 2013.

Executive Order 13744. "Coordinating Efforts to Prepare the Nation for Space Weather Events." October 13, 2016.

Federal Emergency Management Agency (FEMA). "Emergency Support Function 15: Standard Operating Procedures." Last updated August 21, 2014.

––––––––."National Planning Frameworks." Last updated March 19, 2015. www.fema.gov/national-planning-frameworks.

––––––––. "National Preparedness Goal." Last updated March 19, 2015. www.fema.gov/national-preparedness-goal.

––––––––. "Whole Community." Last updated June 10, 2016. https://www.fema.gov/whole-community

––––––––. *A Whole Community Approach to Emergency Management: Principles, Themes, and Pathways for Action*. FDOC 104-008-1. December 2011.

ICF International, "Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats." June 2016.

National Science and Technology Council (NSTC). *National Space Weather Strategy*. Washington, DC: OSTP, October 2015.

––––––––. *National Space Weather Action Plan*. Washington, DC: OSTP, October 2015.

Office of Management and Budget (OMB). "Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities." OMB Circular A-119. Washington, DC: OMB, February 10, 1998.

Presidential Memorandum, "Climate Change and National Security." September 21, 2016.

Presidential Policy Directive 8. "National Preparedness." March 30, 2011.

Presidential Policy Directive 21. "Critical Infrastructure Security and Resilience." February 12, 2013.

Presidential Policy Directive 41. "United States Cyber Incident Coordination." July 26, 2016.

Abbreviations

AIS	Automated Indicator Sharing
CISCP	Cyber Information Sharing and Collaboration Program
CRISP	Cybersecurity Risk Information Sharing Program
CRR	Cyber Resilience Review
CSET	Cybersecurity Evaluation Tool
DBT	Design Basis Threat
DER	Distributed Energy Resources
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
E-ISAC	Electricity Information Sharing and Analysis Center
ECS	Enhanced Cybersecurity Services
EGCC	Energy Sector Government Coordinating Council
EMP	electromagnetic pulse
EPRI	Electric Power Research Institute
ES-C2M2	Electricity Subsector Cybersecurity Capability Maturity Model
ESCC	Electricity Subsector Coordinating Council
FAST	Fixing America's Surface Transportation
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FERC	Federal Energy Regulatory Commission
FLASH	FBI Liaison Alert System
FIOP	Federal Interagency Operations Plan
GIC	geomagnetically induced current
GMLC	Grid Modernization Laboratory Consortium
HHS	Department of Health and Human Services
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team

ISAC	Information Sharing and Analysis Center
NCIRP	National Cyber Incident Response Plan
NCCIC	National Cybersecurity and Communications Integration Center
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
OpenFMB	Open Field Message Bus
PIN	Private Industry Notification
POIA	Power Outage Incident Annex
PPD	Presidential Policy Directive
SGIP	Smart Grid Interoperability Panel
SLTT	State, local, tribal, and territorial
SSA	Sector-Specific Agency
US-CERT	U.S. Computer Emergency Readiness Team
USDA	United States Department of Agriculture