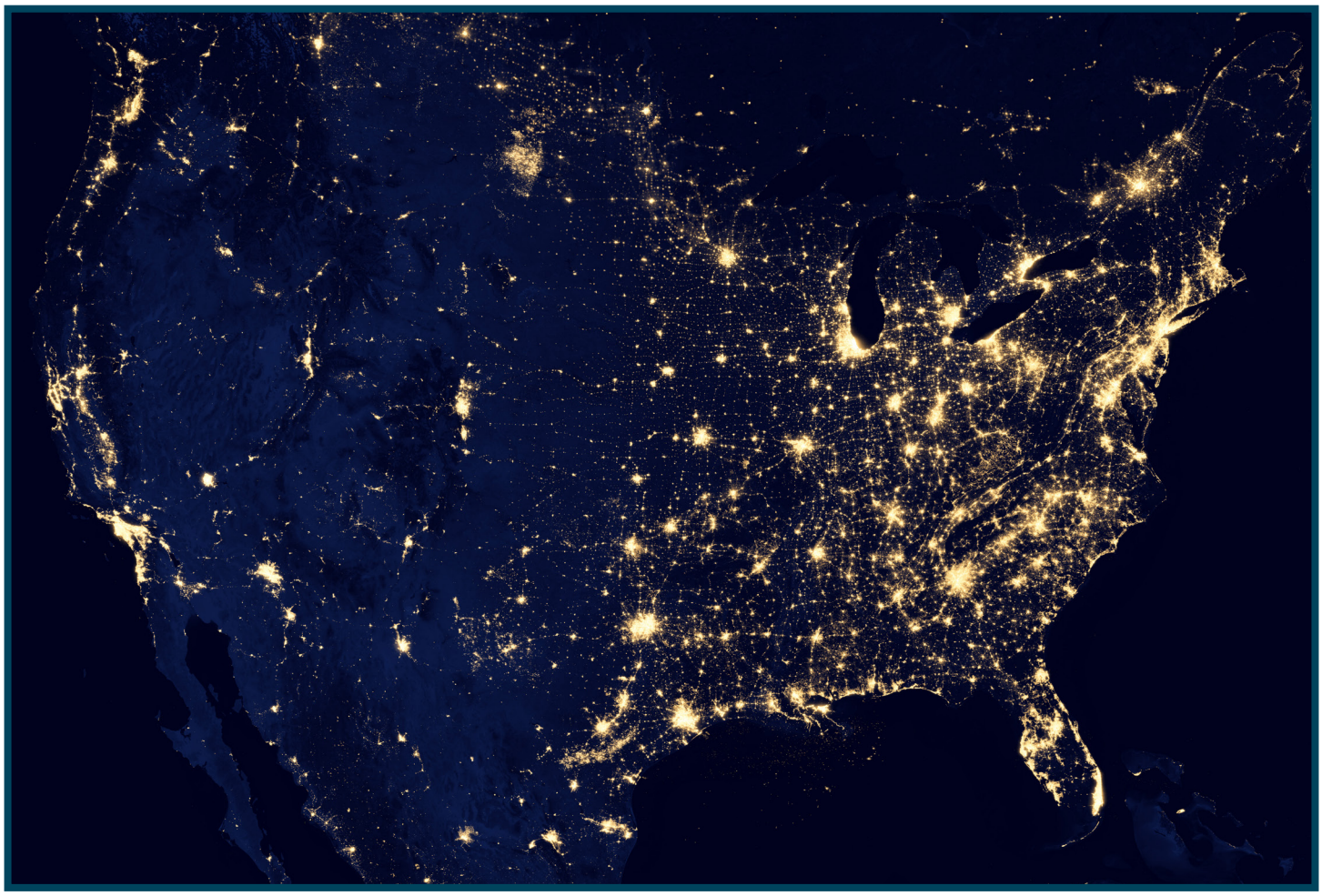
CONGRESS OF THE UNITED STATES
CONGRESSIONAL BUDGET OFFICE

CBO

Enhancing the Security of the North American Electric Grid



MARCH 2020

At a Glance

The electric grid is collection of generating facilities that produce electricity, customers that use it, and intermediate power lines and other equipment that deliver it to those customers. The vast majority of the threats it faces are localized and handled by the grid's operators with minimal disruption for customers. But some threats to the grid might cause a widespread and long-lasting outage. Threats of that scale are the topic of this report, along with potential approaches to improve the grid's security against those threats.

- Major threats derive from both natural disturbances and human adversaries. Naturally occurring threats include a severe solar storm, a major hurricane, and a major earthquake. Human-made threats include a high-altitude electromagnetic pulse, a large cyberattack, and a physical attack. The likelihood of such natural disasters and attacks is generally expected to be quite small, but their costs could be high if they occur.

- Policy approaches that would prevent or mitigate damage include, among others, building more early-warning satellites or sensors, improving information sharing, enhancing cyber protections, and improving physical security.

- Policy approaches that would improve recovery after a disaster or attack include increasing the number of transformers (which are critical transmission components) that are stockpiled, improving the security of certain types of power plants necessary to help bring the grid back into operation, increasing backup power for critical infrastructure, and providing more disaster response training.

The Congressional Budget Office has identified some key considerations for policymakers by examining two approaches in detail: deploying new space-based sensors to warn of solar storms and thus better enable operators to prevent or limit damage to the grid and increasing the stock of large transformers to aid recovery if significant damage occurs. Those considerations include determining the appropriate role for the federal government, deciding what factors to weigh, and comparing the advantages and disadvantages of federal intervention amid uncertainty.

Contents

Notes

Numbers in the text may not add up to totals because of rounding.

To remove the effects of inflation, the Congressional Budget Office adjusted dollar amounts with the gross domestic product price index from the Bureau of Economic Analysis. Unless otherwise noted, dollar values are expressed as 2019 dollars.

The image on the cover was created by Robert Simmon of the National Aeronautics and Space Administration's Earth Observatory using satellite data from 2012 provided courtesy of Chris Elvidge of the National Oceanic and Atmospheric Administration's National Geophysical Data Center.

Enhancing the Security of the North American Electric Grid

Summary

A secure and reliable supply of electric power is a key component of modern economies. Not only are other energy sources often poor substitutes, but essentially every industrial and commercial process in the United States requires its use, and nearly all homes rely on it. Even short-term interruptions in the delivery of electric power result in economic losses or inconveniences for consumers and businesses. Longer outages can result in spoilage of food and other perishables, forgone sales, the idling of resources in production processes, disruptions to the supply of water and fuels, and other threats to health and safety.

This study by the Congressional Budget Office examines a range of threats that could cause widespread, long-lasting disruptions for the electric grid, including ones beyond historical experience. The study discusses a range of illustrative approaches to enhance the security of the electric grid and some considerations for policymakers to take into account.

The North American Power Grid and Major Threats It Faces

The power grid is a collection of generating plants, power transformers, transmission lines, and other equipment that helps move large quantities of electricity over long distances; components that distribute smaller quantities to end users; and collections of customers that use the power. The delivery of power to customers is usually highly reliable. Though the grid faces a wide range of threats, the vast majority are localized and are handled by grid operators with minimal disruption for customers.

But the grid also faces a number of larger but rare threats that have the potential to cause regional disruptions that last longer. Naturally occurring threats include a burst of solar particles—referred to as a solar storm—that interact with Earth's magnetic field and create a geomagnetic disturbance that could overload certain critical grid components; a hurricane that could affect the supply of power along an entire coastal region; and an earthquake that could damage or disrupt generating plants, transmission lines, and other equipment and, thereby, the power supply of extended areas. Human-made threats include a high-altitude electromagnetic pulse (EMP)—most likely created by the detonation of a nuclear weapon at high altitude—which, like a severe solar storm, could overload and disable key components; a cyberattack targeting generating plants or grid control systems; and a physical attack against certain critical components.

The likelihood of wide-ranging and long-lasting outages is small, but the consequences could be severe. Some estimates suggest that losses in the economy could be in the hundreds of billions of dollars or even more than a trillion dollars in some scenarios. Losses could also be considerably less depending on the extent of the disaster or attack; the condition of the system, including whether the grid retained enough power to handle emergencies; and the effectiveness of existing protections and recovery measures, among other factors.

Approaches to Reduce the Costs of Major Threats

The utility industry has a number of operational and procedural protections that it uses to enhance the security of the electric grid and prevent or limit power outages. Most are day-to-day protections. But events like the 2015 cyberattacks in Ukraine, which targeted that country's grid control systems, and a cyberattack in the western United States in early 2019, which briefly disrupted communications at several small generating sites, have increased awareness about risks and heightened concerns.

CBO identified a number of approaches for boosting the security of the grid—approaches to either prevent or mitigate damage or to improve recovery after the damage has occurred. The approaches identified are not an exhaustive list but, rather, illustrate the wide span of possibilities for reducing the risks of a large, long-lasting outage. The approaches include improving information

sharing, enhancing cyber protections, and improving physical security. They also include two approaches that CBO examined in relative detail: one to prevent or mitigate damage—deploying space-based sensors to monitor solar activity—and one to improve recovery—increasing the stock of replacement transformers, which are critical in allowing large amounts of electricity to flow throughout the grid.

Space-Based Sensors. One option for monitoring solar activity—a dedicated satellite placed in orbit between Earth and the sun—would provide early warnings of a solar storm. It would carry a coronagraph to provide images of the sun that would allow forecasters to provide long-term warnings (one day to four days in advance) of a solar storm that might strike Earth. It would also carry instruments to measure the solar wind, which would allow forecasters to provide short-term warnings (15 to 60 minutes in advance) with more accurate estimates of a solar storm's likely arrival time and the severity of its effects on Earth and on the grid. The United States has satellites that provide such warnings today, but they are old and are expected to stop functioning within several years. At a cost of about $500 million to purchase two satellites (one that would be launched in 2024 and another that would replace the first roughly five years later) and another $500 million to launch and support the satellites through 2029, this option would replace the current system and improve the reliability and quality of the data for more accurate forecasts of solar weather.

Two other options—placing coronagraphs on the next generation of weather satellites or on the International Space Station—would cost significantly less and maintain some capability for monitoring solar storms when the current space weather satellites fail. Building and deploying those chronographs might cost $100 million to $150 million over 10 years. But by themselves, neither of those two options would provide the data necessary for the accurate short-term warnings of an impending solar storm that grid operators rely on to take steps to protect their systems—warnings that are provided today and that would continue under the first option. More accurate warnings might also avoid the cost to operators of taking unnecessary steps to prepare for storms that end up having little effect on Earth.

The National Oceanic and Atmospheric Administration (NOAA) has published plans to deploy a dedicated satellite between Earth and the sun but without a follow-on spare satellite (as under the first option) and place a coronagraph on the next weather satellite (as under the second option) so that the agency would have two coronagraphs in orbit. But it has not yet secured most of the funding to implement that plan.

Replacement Transformers. Large power transformers can take a long time to manufacture, leaving portions of the grid vulnerable if they become disabled and need to be replaced. One option for boosting the stock of transformers would be to provide subsidies—in the form of funds or tax credits—to suppliers of electricity that they could use to buy and hold transformers in reserve. This option would leave various technical decisions in suppliers' hands, but setting the appropriate subsidy level would be difficult, and a significant share of the federal costs would only reduce the utilities' net cost of units that they would have purchased anyway. Another option would be for the federal government to own a stockpile of transformers, which, as necessary after a disaster or attack, it could sell or give to suppliers. By the Department of Energy's estimate, the stockpile would need to consist of at least 100 transformers, at a cost of $2 million to $9 million each.[1] Yet another option would be for the federal government to require suppliers to hold private reserves of a specified size. That option would have negligible costs for the government, but determining the appropriate size of such a requirement, like setting an appropriate subsidy level, would be difficult.

Some Key Considerations for Policymakers

One consideration for policymakers is the appropriate role for the federal government in improving the security of the electric grid. To what extent would the private sector acting alone take the full range of potential benefits into account when deciding what to invest in protection or recovery?

The benefits of a new class of space-based sensors dedicated to monitoring and evaluating space weather, for example, would extend beyond the electricity sector. Other industries, too, such as the telecommunications and transportation industries, could benefit from early warnings about potentially damaging solar storms. Because the benefits would be widespread and difficult, if not impossible, to limit only to parties that paid for

1. Department of Energy, Office of Electricity Delivery and Energy Reliability, *Large Power Transformers and the U.S. Electric Grid* (April 2014), https://go.usa.gov/xyu8R.

them, it is unlikely that the private sector would invest in space weather sensors on its own and more likely that the approach would depend on federal support, similar to the federal role in providing Earth weather satellites.

Private-sector electricity suppliers have a greater incentive to pursue some of the benefits associated with investing in reserve transformers. As a result, suppliers hold their own reserves, both individually as part of their business planning and collectively in reserve-sharing arrangements. But in making decisions from the perspective of their business and their geographic area, suppliers may not fully account for some benefits of avoiding outages, such as ensuring economic stability or public safety.

Another consideration is just which factors to weigh. CBO's analysis focused primarily on the potential loss of national economic output (gross domestic product, or GDP) resulting from major outages and on the budgetary costs of policy alternatives. But GDP does not capture all the costs of an outage—such as inconvenience, personal discomfort, or even loss of life—and policymakers could take those or other factors into account. Some threats to the electric grid also threaten military security and public health, so policymakers might weigh the benefit of avoided damage to those sectors—even in circumstances when the avoided loss of GDP would be relatively small or the costs of the policy would be high. Other potential factors are the possibility of inefficiencies that subsidies or regulations could impart to the economy and the effects that policy-induced changes in prices might have on households with different amounts of income or people who live in different regions of the country.

Still another consideration is the advantages and disadvantages of federal intervention amid the uncertainty surrounding estimates of them. Avoiding a loss of GDP is one benefit of improving the security of the grid and reducing the chance of a widespread, enduring power outage. But estimates of the size of potential losses are highly uncertain, as are estimates of their likelihood, suggesting a large range of possible outcomes and complicating decisions about investing in the security of the grid. Deploying new solar satellites, for example, which would probably cost about $1 billion over 10 years, could offer some protection from solar storms. Without it, the economic costs of a severe solar storm could be large, but the likelihood of such infrequent storms is uncertain. Moreover, the degree to which the early warning from a satellite would reduce the damage from a severe solar storm is also uncertain.

The North American Electric Grid

The electric grid is responsible for delivering power to some 150 million customers (households, businesses, and government facilities), sometimes across considerable distances. Those deliveries are usually very reliable: In recent years, the average annual loss of power for a typical customer has ranged between three and eight hours (roughly one-tenth of one percent of the time or less).[2] The higher end of the range occurred because of what the industry classifies as major events: snowstorms, hurricanes, and others. But usually, the cause of an outage is something affecting local delivery, such as less severe weather or an equipment problem, and the outage affects a small area and is not long-lasting.

But the overall stability of the electric grid has also been punctuated by rare, wide-ranging outages of greater magnitude. Those outages are often caused by severe coastal storms or by system failures on especially hot days. In one of the most significant instances, states in the Northeast and portions of Canada experienced a major outage in August 2003, when a blackout spread regionally: A localized power failure, coupled with a control system failure, in Ohio overloaded nearby transmission facilities, which in turn progressively overloaded other portions of the network. The cascading effects were large enough to leave 50 million people without power for several days in many locations and up to a week in others. The cost of the 2003 blackout has been estimated by several researchers at between $5 billion and $14 billion (in 2019 dollars), mostly reflecting lost income and forgone profits, losses of perishable inventories, and expenses for repairs to the electric system—though some

2. Energy Information Administration, "EIA Data Show Average Frequency and Duration of Electric Power Outages," *Today in Energy* (September 12, 2016), www.eia.gov/todayinenergy/detail.php?id=27892, "Average Frequency and Duration of Electric Distribution Outages Vary by States," *Today in Energy* (April 5, 2018), www.eia.gov/todayinenergy/detail.php?id=35652, and "Average U.S. Electricity Customer Interruptions Totaled Nearly 8 Hours in 2017," *Today in Energy* (November 30, 2018), www.eia.gov/todayinenergy/detail.php?id=37652.

or even much of the loss of economic activity reflected in those estimates may have been recouped once power returned.[3]

The threat of wildfires in California and temporary preventive blackouts provide a recent reminder of the disruption of outages. Because of high winds and dry conditions, power producers have temporarily shut off the electricity several times in counties throughout the state to help prevent downed power lines from sparking brush fires. By one account, a preventive blackout over the course of several days in October 2019 affecting some 700,000 homes and businesses may have resulted in $1 billion of economic damage.[4] (That sum reflects estimates of the average amount that customers would be willing to pay to avoid a loss of power, which incorporates the value of lost income, medical care, and spoiled food, among other items.) With dry seasonal conditions expected to persist in coming years, such outages and their attendant losses will probably continue.

Much of the oversight responsibility of the electric grid, including its reliability, lies with state and federal authorities; local authorities play a limited role.

Elements of the Electric Grid

The North American electric grid spans the continental United States, most of Canada, and a small portion of northern Mexico. The grid is composed of two main networks, or interconnections—Eastern and Western—which are largely electrically separate from other power regions, and three smaller interconnections for Texas, Quebec, and Alaska (see Figure 1). Hawaii, Puerto Rico, other island territories, and portions of Canada operate separate grids.

The grid broadly consists of four main elements (see Figure 2). Power is first produced at one of nearly 10,000 generating plants.[5] It is initially transported through high-voltage transmission lines for long distances and then delivered by lower-voltage distribution lines for shorter distances. Customers are the final component: industrial facilities, commercial establishments (usually considered to include government facilities as well), and residences. Power transformers, which are used in the grid at an estimated 56,000 substations (locations containing a variety of electrical equipment, including transformers, switches, system controls, and other components), first increase the voltage of the power produced at the generating station—so that it can be transported long distances more efficiently—and later reduce the voltage so that it can be used by customers.[6] Because transformers allow large amounts of electricity to flow throughout the transmission grid, they are among the grid's most critical components.

End-use customers are served by about 3,000 electricity providers.[7] Those providers include about 200 large investor-owned utilities, which provide about 65 percent of the power; 5 federal agencies that produce and sell about 1 percent of the power; and roughly 2,800 regional or local providers, which sell the remaining share.

3. See National Research Council, *Terrorism and the Electric Power Delivery System* (National Academies Press, 2012), https://doi.org/10.17226/12050; Kristina Hamachi LaCommare and Joseph H. Eto, *Understanding the Cost of Power Interruptions to U.S. Electricity Consumers*, LBNL-55718 (Ernest Orland Lawrence Berkeley National Laboratory, September 2004), https://go.usa.gov/xydaD; U.S.–Canada Power System Outage Task Force, *Final Report on the August 14, 2003, Blackout in the United States and Canada: Causes and Recommendations* (April 2004), https://go.usa.gov/xydaq; Electricity Consumers Resource Council, *The Economic Impacts of the August 2003 Blackout* (February 9, 2004), http://tinyurl.com/y286sep6; Patrick L. Anderson and Ilhan K. Geckil, *Northeast Blackout Likely to Reduce U.S. Earnings by $6.4 Billion*," Working Paper 2003-2 (Anderson Economic Group, August 19, 2003), http://tinyurl.com/yyeqjplf; and ICF Consulting, *The Economic Cost of the Blackout: An Issue Paper on the Northeastern Blackout, August 14, 2003*, www.solarstorms.org/ICFBlackout2003.pdf (190 KB).

4. For the estimate of the number of customers affected by the outage, see Andrew G. Campbell, "Northern California Goes Dark," *Energy Institute Blog* (October 14, 2019), https://tinyurl.com/r3a4b8n. For the estimate of economic losses from the outage, see Catherine *Wolfram,* "Measuring the Economic Costs of the PG&E Outages," *Energy Institute Blog* (October 14, 2019), https://tinyurl.com/wn4ep3h.

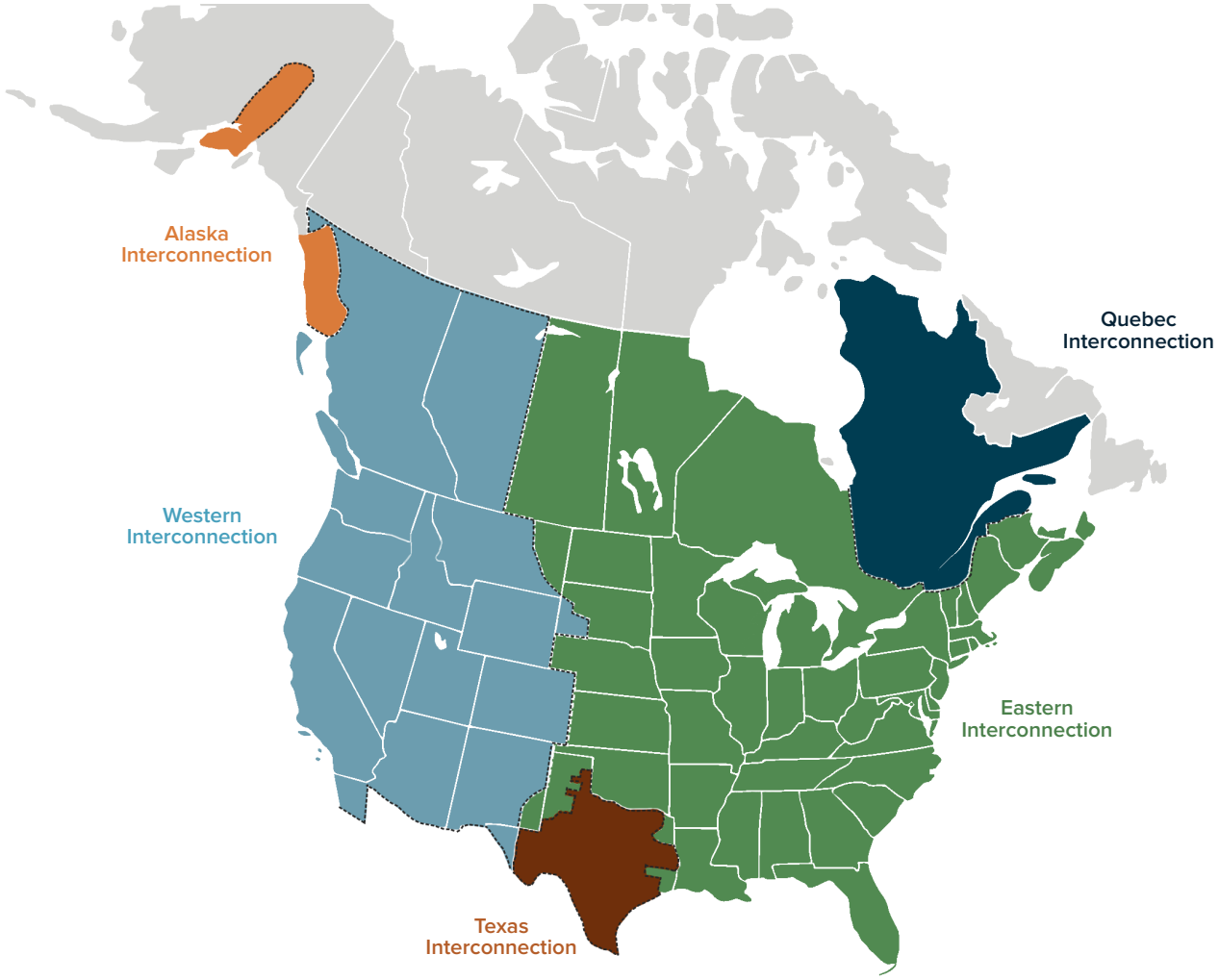
5. Energy Information Administration, *Electric Power Annual 2018* (October 2019), www.eia.gov/electricity/annual/.

6. Department of Energy, *Transforming the Nation's Electricity System: The Second Installment of the Quadrennial Energy Review* (January 2017), https://go.usa.gov/xydxn.

7. Calculation based on figures from Department of Energy, *Transforming the Nation's Electricity System: The Second Installment of the Quadrennial Energy Review* (January 2017), https://go.usa.gov/xydxn; and Energy Information Administration, "Electric Sales, Revenue, and Average Price," Table 10, "2018 Utility Bundled Retail Sales—Total" (October 1, 2019), www.eia.gov/electricity/sales_revenue_price/.

Figure 1.

The North American Electric Grid



Source: Congressional Budget Office, adapted from Western Electricity Coordinating Council, "The Bulk-Power System" (accessed October 23, 2019), https://tinyurl.com/y3tvrw8n.

The North American grid comprises two major networks, or interconnections—Eastern and Western—and three smaller interconnections—Quebec, Texas, and Alaska. Unlike Quebec and Texas, which have a few connections with the Eastern Interconnection, through which small amounts of power are exchanged, the Alaska Interconnection consists of two separate and unconnected networks, neither of which exchanges power with any other interconnection. Also, the State of Hawaii and Puerto Rico and other island territories operate their own grids (which are not shown).

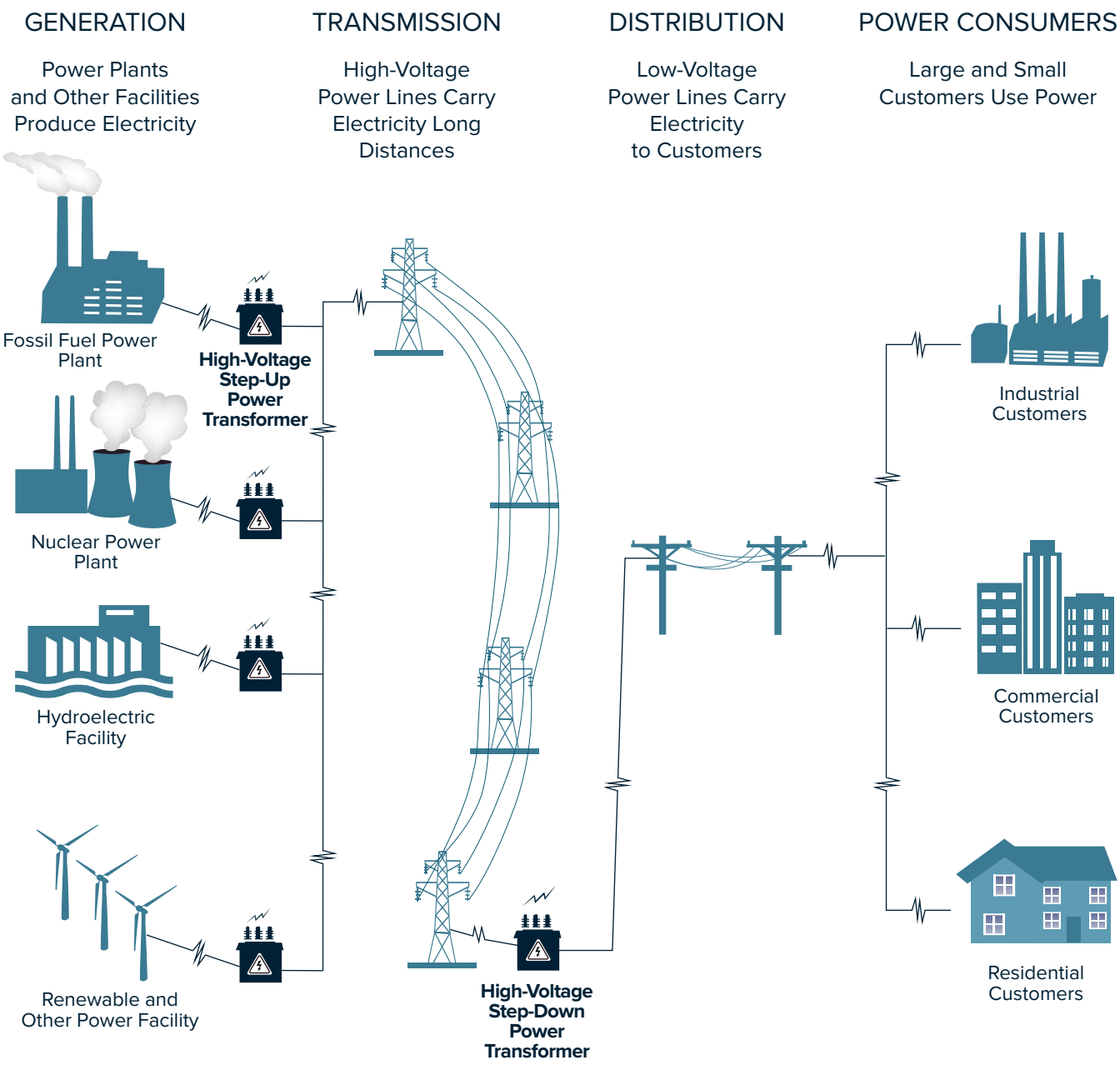
State and Federal Oversight of the Electric Grid

Oversight of the U.S. electric grid is shared primarily between state and federal authorities. State commissions are responsible for approving most aspects of electric utilities' operations, such as the siting and construction of new power plants, the local distribution of electricity to customers, and the retail prices customers pay for electric service. Local authorities provide some oversight, though it is generally limited to input into the siting of facilities as well as some review of the environmental impacts of certain projects.

The federal government, through the Federal Energy Regulatory Commission (FERC), regulates public utilities' transmission and wholesale sale of electricity that

Figure 2.

The Main Elements of the Electric Grid



Source: Congressional Budget Office.

A step-up power transformer takes electricity produced at generating plants and raises the voltage of that power so that it can be transmitted more efficiently. A step-down transformer reduces that voltage before the power is distributed to customers.

Commercial customers in this context include the federal government and state and local governments.

crosses state lines.[8] Wholesale transactions that take place entirely within state boundaries are regulated by state authorities.

Following the 2003 Northeast outage, lawmakers granted FERC oversight over the reliability of the bulk power system—that is, high-voltage transmission lines and associated facilities. (Individual states continue to oversee the reliability of local distribution.) By law, FERC conducts that oversight by reviewing and approving mandatory reliability standards proposed by what is referred to as an electric reliability organization. In 2006, FERC designated the nonprofit North American Electric Reliability Corporation (NERC) as the electric reliability organization of North America. Since then, NERC has established more than 100 mandatory reliability standards.[9] Most of those standards reflect general operational and planning requirements. But some specifically address threats to the electric grid examined in this report: physical attacks, cyberattacks, and solar storms.[10] The standards include requirements for administering personnel risk assessments and training, reporting incidents, protecting information, implementing operating procedures, and conducting vulnerability assessments. In most cases, options for compliance are open-ended: Electricity suppliers decide how best to meet NERC's guidelines. For instance, to comply with a standard that will require developing plans to meet performance requirements starting in 2022, suppliers may develop additional operational procedures, boost training, use new grid hardware, remove vulnerable components, or participate in sharing agreements for critical equipment.[11] Partly to comply with new reliability and security standards, but also to upgrade aging infrastructure and to enhance security otherwise, utilities have invested close to $50 billion annually in recent years for improvements to their transmission and distribution systems.[12]

NERC's standards have increased the security of the electric grid, particularly with regard to commonplace contingencies and threats, but vulnerabilities remain, especially for more serious threats. One recent finding, for example, is that the grid might be vulnerable to a geographically dispersed cyberattack that targets less protected electrical systems small enough to be exempt from full compliance with NERC's standards.[13] More broadly, the development of NERC's mandatory standards is relatively recent, so gauging their ultimate effectiveness against the more extreme types of threats examined in this study is difficult.

Major Threats to the Electric Grid and Their Potential Impact

Some threats to the U.S. electric grid are relatively common—such as wildlife, vegetation, equipment failure, and thunderstorms—and usually cause localized outages that are routinely managed by electricity suppliers and grid operators. But other threats are far less common and can be more severe in their geographic scope and duration, having a significant impact on economic activity and people's well-being.

8. FERC does not have regulatory jurisdiction over the transmission and wholesale sale of power within Hawaii, Alaska, or much of Texas. Power flows are considered to be in interstate commerce only when they cross state lines and are synchronous—that is, the power on each side of the state line has the same frequency, voltage, and other electrical characteristics. Hawaii and Alaska have no interstate connections, so they are not within FERC's jurisdiction. Although Texas is connected to adjacent states, a large portion of Texas is connected to those states only through a limited number of locations, where alternating current is converted into direct current, transferred over the border, and then converted back to alternating current on the other side. The power included in such transactions is not synchronous. Therefore, the portions of the Texas grid behind those connections are not subject to FERC's jurisdiction. See Jim Lazar, *Electricity Regulation in the US: A Guide*, 2nd ed. (The Regulatory Assistance Project, 2016), http://tinyurl.com/y647dzpg.

9. See Ashley J. Lawson, *Maintaining Electric Reliability With Wind and Solar Sources: Background and Issues for Congress*, Report R45764, version 2 (Congressional Research Service, June 10, 2019), https://go.usa.gov/xd5PB.

10. See North American Electric Reliability Corporation, "Mandatory Standards Subject to Enforcement" (accessed January 10, 2020), www.nerc.net/standardsreports/standardssummary.aspx.

11. See Government Accountability Office, *Critical Infrastructure Protection: Electricity Suppliers Have Taken Actions to Address Electromagnetic Risks, and Additional Research Is Ongoing*, GAO-18-67 (February 2018), www.gao.gov/products/GAO-18-67.

12. Energy Information Administration, "Major Utilities Continue to Increase Spending on U.S. Electric Distribution Systems," *Today in Energy* (July 20, 2018), www.eia.gov/todayinenergy/detail.php?id=36675, and "Utilities Continue to Increase Spending on Transmission Infrastructure," *Today in Energy* (February 9, 2018), www.eia.gov/todayinenergy/detail.php?id=34892.

13. See Government Accountability Office, *Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid*, GAO-19-332 (August 2019), www.gao.gov/products/GAO-19-332.

Those major threats can be broadly classified as naturally occurring or human-made. Naturally occurring threats include a solar storm, a coastal hurricane, and an earthquake, whereas human-made threats include the detonation of an EMP, a cyberattack, and a physical attack. Although all such threats share an element of unpredictability, the likelihood of the naturally occurring events is generally better understood because a historical record exists and the likelihood generally changes little over the course of years or even decades. In contrast, there is little historical basis to draw on to assess the likelihood of human-made threats. And even when some historical basis exists, the threats might change significantly over relatively short periods of time, possibly to the point of becoming unpredictable.[14]

Given the wide range of threats and the substantial uncertainties underlying estimates of the likelihood and costs of many of them, CBO has characterized them in broad terms that are expressed as approximate orders of magnitude. CBO focused on relatively large and potentially costly versions of the threats (such as a major hurricane or earthquake that results in substantial damage) and relied on approximations of costs cited in the literature given existing protections for the electric grid (where those are known). In general, events expected to be of higher probability are associated with expectations of smaller economic consequences and vice versa (see Figure 3). For example, a severe solar storm that causes a strong geomagnetic disturbance may be less than one-tenth as likely to occur as a major hurricane but has a cost that could be 50 times greater or more. Thus, decisions about enhancing the security of the electric grid range from considering approaches that target low-likelihood but high-cost threats, such as a severe solar storm or a high-altitude EMP, to considering approaches that target higher-likelihood, lower-cost threats, such as a hurricane or a physical attack.

Naturally Occurring Threats That Could Cause Significant Power Losses

Most naturally occurring threats have limited impact on the electric grid, either because the consequences are limited or because risk management practices are well established throughout the grid. However, some naturally occurring threats, such as a solar storm, if large enough, could cause more significant and wide-ranging damage to the grid.

Solar Storm. A severe solar storm could present a significant threat to the electric grid, especially at higher northern or southern latitudes. Originating from an eruption on the sun's surface and able to reach Earth generally within a few days, a mass of charged particles can interact with Earth's magnetic field and cause a geomagnetic disturbance.

If the disturbance is large enough, it could create strong electric currents along long-distance transmission lines that could overload and disable large power transformers. If enough transformers were affected, regional power losses could occur. Older transformers can be at a heightened risk because some of the components degrade over time and reduce the ability of the transformers to withstand the strong currents. With typical warranties of 30 to 35 years, large power transformers in the United States have an average age of about 40 years, and some are more than 70 years old.[15] By one set of estimates, perhaps 200 to 350 large power transformers within the United States would be at risk of damage from a severe solar storm, which amounts to roughly 10 percent to 20 percent of the large power transformers in the country.[16]

Another possibility following a solar storm—and one that some consider more likely—is that few transformers would be damaged but that systemwide losses of power could still occur because of what is termed a voltage collapse. Such a scenario could unfold if the resulting currents flowing through power lines overloaded power transformers and caused them to draw greater

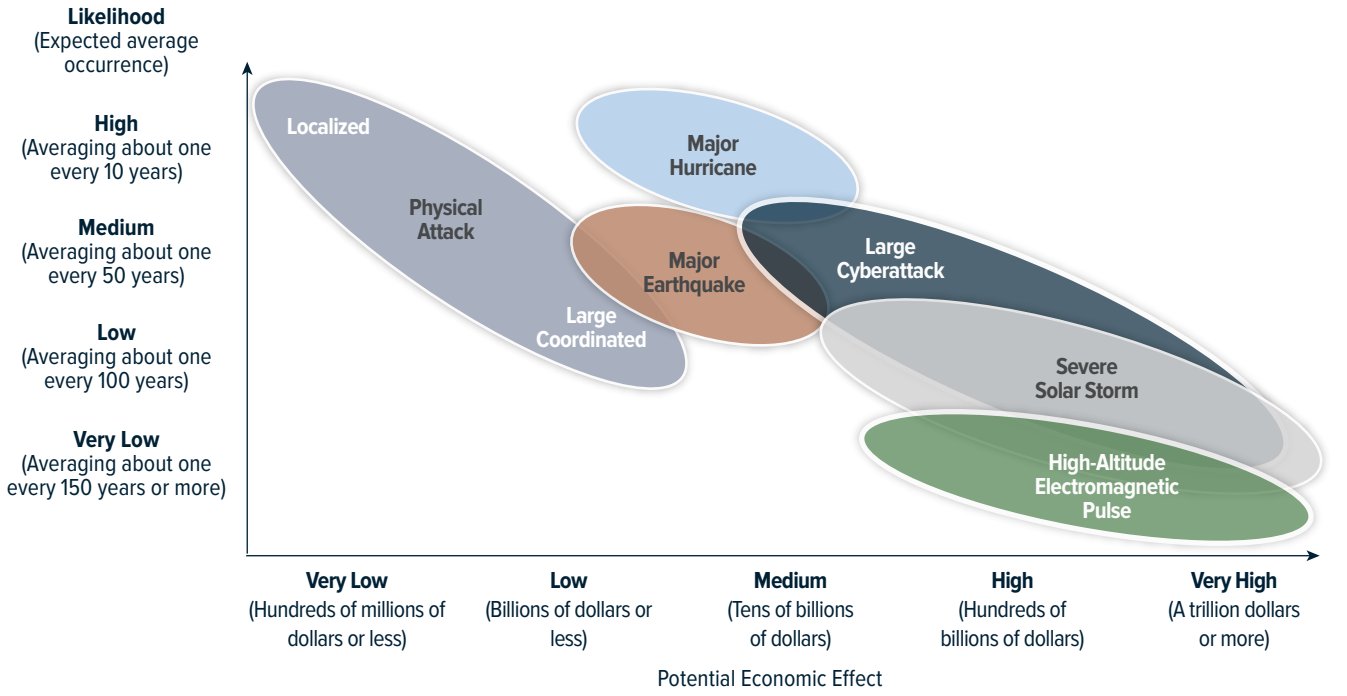
14. See Benjamin L. Preston and others, *Resilience of the U.S. Electricity System: A Multi-Hazard Perspective* (prepared for the Department of Energy, Office of Energy Policy and Systems Analysis, August 18, 2016), https://go.usa.gov/xydU9 (PDF, 4.2 MB).

15. Department of Energy, Office of Electricity Delivery and Energy Reliability, *Large Power Transformers and the U.S. Electric Grid* (June 2012), https://go.usa.gov/xydPm (PDF, 2.2 MB).

16. John G. Kappenman, *Geomagnetic Storms and Their Impacts on the U.S. Power Grid* (prepared for Oak Ridge National Laboratory, January 2010), https://go.usa.gov/xydE9 (PDF, 14.0 MB), and "The Vulnerability of the U.S. Electric Power Grid to Severe Space Weather Events" (presentation at the 2009 Space Weather Enterprise Forum, Office of the Federal Coordinator for Meteorology, May 19–20, 2009), www.ofcm.gov/meetings/swef/2009/; and Department of Energy, Office of Electricity Delivery and Energy Reliability, *Large Power Transformers and the U.S. Electric Grid* (April 2014), https://go.usa.gov/xp2vy (PDF, 2.2 MB).

Figure 3.

Judgments About the Likelihood of Major Threats to the Grid and the Economic Effects From the Loss of Power



Source: Congressional Budget Office.

The location of a bubble reflects a rough estimate of the likelihood and economic cost of each threat if realized, based on a survey of the literature. The length and width of the bubbles reflect the uncertainty that surrounds both the likehood and the costs.

Assessments about the potential economic effect are limited to the costs stemming from the loss of power and not the costs of physical damage more broadly, which could be significant, particularly from hurricanes and earthquakes.

amounts of a certain type of power on the grid—what is called reactive power—that is necessary to maintain the system's voltage levels and stability, resulting in a net shortfall of that power.[17] In that case, although potentially widespread, the power outages would probably be shorter, hours in some cases, potentially days in others.

Although powerful solar storms are rare, millions of people were left without power for about a half-day on March 13, 1989, after a geomagnetic disturbance damaged three transformers and triggered protective relays that disabled Quebec's power grid.[18] Power supplies in the United States and neighboring provinces in Canada were not significantly affected because the Quebec grid is largely separate from the U.S. and other Canadian grids. Other large solar storms have struck Earth, though at times when the grid was less developed or nonexistent. A 1921 storm, for instance, was estimated to have induced electric currents on long transmission lines about 10 times stronger than those affecting the Quebec grid in 1989.[19] The 1859 Carrington Event—named after the amateur astronomer Richard Carrington, who was among the first to document the storm—reportedly

17. See Royal Academy of Engineering, *Extreme Space Weather: Impacts on Engineered Systems and Infrastructure* (February 2013), https://tinyurl.com/u7upaf9 (PDF, 2.7 MB).

18. Government Accountability Office, *Critical Infrastructure Protection: Protecting the Electric Grid From Geomagnetic Disturbances*, GAO-19-98 (December 2018), www.gao.gov/products/GAO-19-98.

19. National Research Council, *Severe Space Weather Events—Understanding Societal and Economic Impacts: A Workshop Report* (National Academies Press, 2008), https://doi.org/10.17226/12507.

created visible auroras as far south as Cuba and caused telegraph lines to spark, starting fires in some telegraph offices. Though the Carrington Event occurred before electricity was produced on an industrial scale, a similarly powerful solar storm missed Earth in July 2012 and was observed by a solar satellite. Experts calculated that Earth would have been in the storm's path had the storm occurred a week earlier.[20]

Hurricane. Damage caused by hurricanes has been the most common cause of wide-ranging power outages in the United States. Particularly large storms like Hurricane Katrina in 2005—the costliest storm in U.S. history—and Hurricane Sandy in 2012 bring wind damage and flooding that can cause power outages lasting days or even weeks over regions spanning several states. Local distribution and long-distance transmission equipment are the parts of the electric grid that are most vulnerable to hurricanes, although generating plants and transformer substations face risks from coastal flooding.

Earthquake. Power outages can be a serious secondary effect of an earthquake. Although the United States has not yet experienced an earthquake that has seriously damaged large portions of the electric grid, the March 2011 Tohoku earthquake off Japan and associated tsunami damaged several coastal nuclear reactors and left 4.5 million households without power.[21] The largest risks of earthquakes for the North American grid center on the New Madrid fault in the five-state region around Memphis, Tennessee; the San Andreas and other faults in California; and the Cascadia subduction zone about 50 miles off the coast of Oregon and Washington. More than other naturally occurring threats, a major earthquake would threaten many components of the electric grid—generating facilities, transmission towers, substations, distribution facilities, and end users' facilities or homes—although such damage is more likely to be local than regional.

20. Daniel N. Baker and others, "A Major Solar Eruptive Event in July 2012: Defining Extreme Space Weather Scenarios," *Space Weather*, vol. 11, no. 10 (October 2013), pp. 585–591, https://agupubs.onlinelibrary.wiley.com/doi/10.1002/swe.20097.

21. Federica Ranghieri and Mikio Ishiwatari, eds., *Learning From Megadisasters: Lessons From the Great East Japan Earthquake* (The World Bank, 2014), https://openknowledge.worldbank.org/handle/10986/18864.

Human-Made Threats That Could Cause Significant Power Losses

As with naturally occurring threats, many of the consequences of human-made threats would probably be limited enough that electricity suppliers and grid operators could manage them within their usual procedures. But a distinguishing aspect of human-made threats is that they could be targeted for maximum impact. A cyberattack could be conducted in several waves, for instance, or a cyberattack and physical attack could be conducted in tandem, boosting their effects. In addition, tactics of human-made threats can be adapted to overcome the protections in place.

Electromagnetic Pulse. A high-altitude detonation of a nuclear weapon can generate an EMP that consists of three distinct periods—often referred to as components. The first component is a pulse that could overload and damage electronics, leaving computer systems and electronic controls at risk. The second is a pulse having effects similar to lightning's, though occurring over a much larger region. Because the grid has lightning protections, it would not face much risk from the second component (unless the first component made the grid more vulnerable to the second). The final component of an EMP—the longest lasting (spanning minutes, potentially)—could create strong electric currents along power lines that could disable large power transformers in much the same way as a severe solar storm might. That final component—alone or in conjunction with the others—could disable the grid over a wide area, although the research is not unanimous in that regard.[22] Because of

22. Charged by the Congress in 2001 to investigate the threat of a high-altitude EMP attack and the potential consequences from one, the EMP Commission found that the damage could be widespread; see John S. Foster, Jr., and others, *Report of the Commission to Assess the Threat to the United States From Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures* (April 2008), www.empcommission.org/reports.php. More recently, the Electric Power Research Institute concluded that an EMP would not overload and disable many large power transformers, and those that it found might become disabled were geographically dispersed. However, the analysis viewed regional outages to be possible in roughly half the cases considered because the EMP would cause a loss of system voltage that—rather than damaging the system—in turn would cause a short-term loss of power. The geographic extent of those outages was estimated to be on the order of several states, and none was judged to be nationwide. See Randy Horton, *Magnetohydrodynamic Electromagnetic Pulse Assessment for the Continental U.S. Electric Grid: Geomagnetically Induced Current and Transformer Thermal Analysis* (prepared for the

the direct risk to electronics from the first EMP component, other critical sectors could also be at risk, including telecommunications, transportation, food distribution, emergency response, and banking.

To cause the most disruption, the nuclear detonation that created the EMP would have to be at high altitude, perhaps 250 miles above Earth, centered over the nation. If such an attack occurred, it would probably be delivered via an intercontinental ballistic missile or possibly a satellite during a war and would most likely occur in conjunction with some other major nuclear attack. In that case, the loss of electric power would be only one of many problems, including the disabling of other critical infrastructure, massive casualties, radiation contamination, and physical destruction. A smaller EMP could be created without using a nuclear weapon, but its effects would be much more localized and easier for electricity suppliers and grid operators to overcome.

Cyberattack. In the context of this study, a cyberattack is an attempt to remotely exploit vulnerabilities in computer systems to affect generating stations, transmission lines, or grid control systems and disable or disrupt power production within a region. A cyberattack could be directed at generating stations to cause physical damage or to disable or hamper their operation. Alternatively, a cyberattack could be used to reset grid controls and reroute power to overload critical lines and equipment.

To date, cyberattacks have not been thought to be a factor affecting the reliability of the electric grid in the United States, but some believe that the grid is becoming more vulnerable to such threats.[23] A recent cyberattack, in March 2019—purportedly the first on record for the U.S. electric grid—was able to disrupt control system communications for a few minutes at several small generating sites located in the western United States, although no losses of power occurred.[24] In December 2015, Ukraine experienced a significant attack. In that case, the power outage was short, about six hours before grid operators were able to manually secure the system. Although the attack is suspected to have originated in Russia, its origin has not been proved, illustrating a clear advantage that cyberattacks have: a degree of anonymity greater than that of other directed threats.

Just how vulnerable U.S. power supplies are to a significant cyberattack is uncertain. The decentralized and dispersed structure of the U.S. electric grid might limit the effectiveness of a cyberattack because it would have to be configured to apply to an array of grid controls. For cyberattackers to disrupt the U.S. electric grid broadly and for a long time, they would need to be technically sophisticated and undertake considerable planning and reconnaissance of the many systems. Some analysts believe that such activities are ongoing.[25]

But modernizations of the electric grid suggest a growing number of vulnerabilities that might be exploited by cyber methods. The increased reliance on digital controls for producing and routing power is one such modernization that could be the target of a cyberattack. Indeed, one proposal before the Congress includes a provision to study the effectiveness of removing the digital controls of certain critical components, despite their many operational advantages, and instead relying on older analog and sometimes manual technologies for their operation, both of which are far less susceptible to cyber threats.[26] Similarly, the growth in renewable sources of electricity increases the number of pathways for intrusions, but those sources can also enhance security by diversifying the types of generating capacity.

Physical Attack. A physical attack is most likely to be a localized threat, unless done in conjunction with a

Electric Power Research Institute, February 2017), www.epri.com/#/pages/product/3002009001/, and *Magnetohydrodynamic Electromagnetic Pulse Assessment for the Continental U.S. Electric Grid: Voltage Stability Analysis* (prepared for the Electric Power Research Institute, December 2017), www.epri.com/#/pages/product/000000003002011969/.

23. See Government Accountability Office, *Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid*, GAO-19-332 (August 2019), www.gao.gov/products/GAO-19-332.

24. See Blake Sobczak, "Report Reveals Play-by-Play of First U.S. Grid Cyberattack," *E&E News* (September 6, 2019), www.eenews.net/energywire/stories/1061111289; and North American Electric Reliability Corporation, *Lesson Learned: Risks Posed by Firewall Firmware Vulnerabilities* (September 4, 2019), www.nerc.com/pa/rrm/ea/Pages/Lessons-Learned.aspx.

25. See Idaho National Laboratory, Mission Support Center, *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector* (August 2016), https://tinyurl.com/yy5podlx.

26. Securing Energy Infrastructure Act, S. 174, 116th Cong. (2019, accessed October 28, 2019), www.congress.gov/bill/116th-congress/senate-bill/174/text.

cyberattack or conducted at a scale difficult to coordinate and implement. Therefore, a physical attack probably would not have a widespread impact on the electric grid simply because the number of different paths through which electric power can be delivered to end users within a highly interconnected network would require disabling many critical components at the same time.

To date, there have been two physical attacks of note on the U.S. grid. One, in California, at the Metcalf Transmission Substation in 2013 resulted in $15 million worth of damage to the grid.[27] The other, in Utah in 2016, left 13,000 customers without power for much of a day.[28] In both cases, gunmen shot and disabled electric transformers. Those experiences probably typify the scale of threat that a physical attack represents: an attack on individual components of the grid rather than on a large number of simultaneous targets. However, a large coordinated attack or, more likely, an insider attack (by an employee or an on-site contractor or by a vendor) on control equipment or system software could cause greater and more costly damage.

Potential Scale of Impacts and Assessments of Likelihood

The costs of a large power outage stemming from a natural disaster or attack can be measured in a number of ways. One measure is the overall business interruption—the forgone goods and services, as measured by the change in GDP.[29] Businesses suffering power outages would be less able to produce, though some unaffected businesses could see their production increase—in part to make up for less output from the affected businesses and in part to accommodate resulting changes in spending. For example, consumers could increase their spending on hotel services or restaurants in less affected regions. The loss of power could also damage machinery and equipment and other forms of the nation's capital stock, reducing the economy's capacity to produce in future years; in other words, the loss of power could destroy wealth. Other measures include expenses incurred in the aftermath of the disaster or attack (for example, costs of temporary housing or of additional transportation) and what are termed hidden costs. Examples of the latter include the loss of schooling, emotional distress, inconvenience or discomfort from the lack of modern services or the loss of power during hot or cold weather. Finally, a resulting lack of food, sanitation, medical care, and potable water, among other problems, could degrade people's health and in some cases cause deaths, particularly among members of at-risk groups: children, the elderly, and the infirm.[30]

Some of the various measures of costs overlap with others, so the overall cost is not the sum of those individual costs. For instance, to the extent that the market cost of replacement capital reflects the value of future business activity generated from it, the business interruption cost and the destruction of capital equipment are different measures of much the same effect, so counting them both would double-count the loss.

The expected costs of potential natural disasters or attacks will inform both private and government decisions to invest in security measures for the electric grid. A proper accounting requires an accurate understanding of an event's likelihood and the range of potential costs. For those threats that are realized frequently, electricity suppliers and grid operators understand the likelihood and scale and have made investments they believe are appropriate. But for threats that are realized only

27. "2013 Attack on Metcalf, California, Power Grid Substation Committed by 'An Insider': DHS," *Homeland Security News Wire* (October 19, 2015), https://tinyurl.com/y4nrdok6.

28. Peter Behr, "Substation Attack Is New Evidence of Grid Vulnerability," *E&E News* (October 6, 2016), www.eenews.net/stories/1060043920.

29. Business interruption is sometimes used in the research literature to measure the contemporaneous reduction in sales of goods and services. But governments and nonprofit companies also produce goods and services, and a change in businesses' sales of goods and services can extend beyond the contemporaneous period. All those effects are captured in a change in GDP.

30. Hurricane Katrina in 2005 caused an estimated 1,800 fatalities, and, more recently, Hurricane Maria, nearly 3,000 or (by some assessments) more. In both cases, the proportion of deaths stemming from the lack of electricity, rather than from direct damage or flooding, is unknown. See Richard D. Knabb, Jamie R. Rhome, and Daniel P. Brown, *Tropical Cyclone Report, Hurricane Katrina, 23–30 August 2005* (National Hurricane Center, December 20, 2005; updated September 14, 2011), www.nhc.noaa.gov/data/tcr/AL122005_Katrina.pdf (PDF, 2.2 MB); George Washington University, Milken Institute School of Public Health, *Ascertainment of the Estimated Excess Mortality From Hurricane Maria and Puerto Rico* (August 2018), https://prstudy.publichealth.gwu.edu/releases-reports; and Nishant Kishore and others, "Mortality in Puerto Rico After Hurricane Maria," *The New England Journal of Medicine*, vol. 379, no. 2 (July 12, 2018), www.nejm.org/doi/pdf/10.1056/NEJMsa1803972.

infrequently or that have never been realized, neither the likelihood nor the potential costs are well understood.

Research on the Cost of Outages From Disasters or Attacks. Relatively few studies have been done that can serve as a basis for reliably judging the cost of outages from large-scale disasters or attacks, and the ones that exist do not all measure the same set of factors. Some estimates describe losses in electricity sales and forgone sales of final goods and services. Others reflect damage to structures and equipment and other capital assets. And still others include estimates of the inconvenience and other less tangible costs of outages affecting consumers' well-being.

Nevertheless, a review of the research suggests that the cost of power losses could be hundreds of billions of dollars, or perhaps more than a trillion dollars, following a severe solar storm, a significant cyberattack, or the detonation of a high-altitude EMP—if the disaster or attack caused widespread, long-lasting damage to the electric grid. One study concluded that a large geomagnetic disturbance resulting from a severe solar storm could cause GDP losses of about $160 billion to $700 billion over the course of about a year—or roughly between 1 percent and 3 percent of GDP.[31] Those figures take into account some offsetting effects in the U.S. economy—changes in prices, interest rates, and other factors that would reallocate production activity and labor and capital inputs and thereby lessen the impact. The magnitude of the cost would depend on the severity of the disturbance, the elements of the grid affected and the extent to which they were damaged, and the rate at which power was restored.

Similarly, an assessment of a large hypothetical cyberattack focused on the East Coast estimated GDP losses of $260 billion to $1.1 trillion over five years, mostly concentrated in the first two years following the attack.[32] Although there has been limited evaluation of the economic effects of a high-altitude EMP, CBO concludes that the losses stemming from such an attack would probably be on par with those from a severe solar storm or a large cyberattack because the potential geographic scope and duration of the outages caused by all three are similar.

A survey of recent hurricanes and estimates of potential impacts from earthquakes suggest that those natural disasters could cause tens of billions of dollars in overall losses depending on the geographic scope and severity. However, costs attributable to the loss of electric power probably account for a small portion of those estimates, which include costs of physical damage to structures and equipment and other capital assets besides the electric grid and the resulting effects on economic activity.

The cost of a physical attack or of a limited cyberattack—targeting transmission system components or a single generating plant, for example—would be smaller, perhaps millions of dollars, possibly billions for a large enough attack. Smaller values in that range would reflect less damage to physical capital (generating plants, industrial machinery, and other equipment), whereas larger values would reflect a combination of more extensive physical damage and a longer outage affecting a wider area. Two studies that considered illustrative versions of those more significant attacks tallied losses of up to $20 billion.[33]

Research on the Likelihood of Disasters or Attacks. Because some historical evidence is available, probability estimates are generally firmer for naturally occurring threats than for human-made ones. For solar storms, a survey of point estimates suggests that the probability of a Carrington-level storm is between 1 percent and 12 percent over a decade's time—or, on average, one such storm every 80 to 1,000 years.[34] That estimate is

31. Edward Oughton and others, *Helios Solar Storm Scenario* (University of Cambridge, Cambridge Centre for Risk Studies, November 2016), https://tinyurl.com/y2n3w63k.

32. Trevor Maynard and Nick Beecroft, *Business Blackout: The Insurance Implication of a Cyber Attack on the U.S. Power Grid* (Lloyd's and University of Cambridge, Cambridge Centre for Risk Studies, May 2015), https://tinyurl.com/y48wspj5 (PDF, 4.1 MB).

33. Adam Rose, Gbadebo Oladosu, and Shu-Yi Liao, "Business Interruption Impacts of a Terrorist Attack on the Electric Power System of Los Angeles: Customer Resilience to a Total Blackout," *Risk Analysis*, vol. 27, no. 3 (2007), pp. 513–531, https://doi.org/10.1111/j.1539-6924.2007.00912.x; and Michael Greenberg and others, "Short and Intermediate Economic Impacts of a Terrorist-Initiated Loss of Electric Power: Case Study of New Jersey," *Energy Policy*, vol. 35, no. 1 (2007), pp. 722–733, https://doi.org/10.1016/j.enpol.2006.01.017.

34. David Morina and others, "Probability Estimate of a Carrington-like Geomagnetic Storm," *Science Reports* (February 20, 2019), https://doi.org/10.1038/s41598-019-38918-8; and Pete Riley, "On the Probability of Occurrence of Extreme Space Weather Events," *Space Weather*, vol. 10, no. 2 (February 2012), https://doi.org/10.1029/2011SW000734.

based on observations of storms that have hit Earth and near misses that have been detected. But the observations are limited to the past 150 years, when solar storms have been documented, leaving a wide swath of uncertainty around the estimate. One study reported a wider range, concluding that the probability (expressed with 95 percent confidence) of a Carrington-level storm over the course of a decade is somewhere between almost zero and 23 percent depending on the analytical methods used, a range so large as to call into question the reliability of any probability estimate.[35]

Estimates of the likelihood of earthquakes have a long geological record to draw on, and hurricanes occur fairly regularly, so probability estimates for both are probably more accurate than they are for severe solar storms. In the United States, California faces the greatest likelihood of a significant earthquake, whereas the most severe earthquake—with strong onshore effects as well as the possibility of destructive coastal flooding from tsunamis—is expected to occur in the Cascadia zone, off the coast of Oregon and Washington. Estimates suggest that, over the course of a decade, California faces a more than 50 percent chance of a magnitude 7 or stronger earthquake (that is, a strong to major earthquake causing a significant economic damage and loss of life) and Cascadia faces about a 2 percent risk of a magnitude 9 earthquake (among the most powerful possible, causing near-total destruction and a large loss of life).[36] Stated differently, those probabilities suggest that, on average, such a California earthquake occurs roughly once every 20 years and such a Cascadia earthquake, about once every 500 years.

Strong hurricanes are more likely than severe earthquakes. Since 1851, about 100 strong hurricanes have made landfall in the United States: about 65 of Category 3 (with sustained winds of up to 130 miles per hour), 25 of Category 4 (with sustained winds of at least 130 miles per hour), and 4 of Category 5 (with sustained winds of at least 157 miles per hour).[37] On the basis of that evidence, the likelihood that a Category 4 or stronger storm will strike the United States over a 10-year period is high—about 85 percent (averaging about one every 6 years); and the likelihood of a Category 5 storm, about 23 percent (averaging about one every 40 years).[38] As climate change is expected to increase the intensity of storms, the likelihood of such storms will probably be greater in the future.[39]

The likelihood of human-made threats is more difficult to assess, and few estimates exist. One group of researchers has provided these estimates: over 10 years, a 20 percent chance of a large cyberattack on the U.S. electric grid affecting 50 generators and causing losses of $260 billion (equivalent to an average of about one such attack every 50 years), and a 5 percent chance of an attack affecting 100 generators and causing losses of about $1.1 trillion (equivalent to an average of about one such attack every 200 years).[40] But the United States has never experienced such an attack, so judging the reasonableness of such estimates is difficult.

Added to the fortunate lack of historical experience with human-made threats is the potential for them to constantly evolve. The chance of a high-altitude EMP or a large cyberattack depends on geopolitical relations, the

35. Jeffrey J. Love, "Credible Occurrence Probabilities for Extreme Geophysical Events: Earthquakes, Volcanic Eruptions, Magnetic Storms," *Geophysical Research Letters*, vol. 39, no. 10 (May 18, 2012), https://doi.org/10.1029/2012GL051431.

36. Edward H. Field and others, "UCERF3: A New Earthquake Forecast for California's Complex Fault System," Fact Sheet 2015-3009 (U.S. Geological Survey, March 2015), https://dx.doi.org/10.3133/fs20153009; and Cascadia Region Earthquake Workgroup, "Cascadia Subduction Zone Earthquakes: A Magnitude 9.0 Earthquake Scenario" (2013), https://crew.org/products-and-programs/earthquake-scenarios/. CBO calculated the 10-year probabilities on the basis of 30-year and 50-year estimates for California and Cascadia, respectively.

37. National Oceanic and Atmospheric Administration, National Research Division, "Continental United States Hurricane Impacts/Landfalls, 1851–2018" (accessed October 17, 2019), www.aoml.noaa.gov/hrd/tcfaq/E23.html.

38. See National Oceanic and Atmospheric Administration, National Research Division, "Continental United States Hurricane Impacts/Landfalls, 1851–2018" (accessed October 17, 2019), www.aoml.noaa.gov/hrd/tcfaq/E23.html; and Colorado State University, Tropical Meteorology Research Project, and Bridgewater State University, GeoGraphics Laboratory, "United States Landfalling Hurricane Project" (accessed October 17, 2019), http://e-transit.org/hurricane/welcome.html.

39. See U.S. Global Change Research Program, *Fourth National Climate Assessment,* vol. II, *Impacts, Risks, and Adaptation in the United States* (2018, revised June 2019), https://nca2018.globalchange.gov/downloads/.

40. Trevor Maynard and Nick Beecroft, *Business Blackout: The Insurance Implication of a Cyber Attack on the U.S. Power Grid* (Lloyd's and University of Cambridge, Cambridge Centre for Risk Studies, May 2015), https://tinyurl.com/y48wspj5 (PDF, 4.1 MB).

abilities of those attempting the attack, and the safeguards in place—with all of those changing over time. Given the uncertainties, a commission formed by the Congress in 2001 that was charged with evaluating the level of threat posed by a high-altitude EMP decided not to address the question of likelihood.[41]

Even without historical experience or a complete set of estimates, a logical assessment of comparative likelihood is possible. Because a cyberattack can originate in distant and remote locations and the source of the attack may be harder to trace than with other deliberate actions, the chances of a large cyberattack are probably greater than the chances of a similarly disruptive physical attack.

The chances of a small physical or insider attack are probably significant given the large number of targets available and the comparatively few resources necessary to conduct one. In contrast, the chances of a large coordinated physical attack—in which many components in the grid are simultaneously targeted—are probably very small because of the logistical complexity necessary to conduct an attack of that scale and remain undetected during the preparation.

A high-altitude EMP is probably less likely than a large cyberattack. Developing a nuclear device and delivering it for high-altitude detonation are almost certainly possible only for established nation-states that have the motivation, resources, and technical ability. Any nation intending to use a nuclear weapon against the United States would then run the risk of inviting a nuclear reprisal. Consequently, such an attack would probably occur only during a crisis serious enough and with the stakes high enough that the attacker would take such a great risk.

Uncertainty Surrounding the Estimates

Estimates of the likelihood and costs of disasters and attacks affecting the electric grid are uncertain for several reasons. First, as discussed above, for some events there is little or no historical experience to draw upon to estimate either the likelihood or the economic impact.

Second, the likelihood of an event is not the same as the chance of a major failure of the electric grid. A severe solar storm, for instance, might damage some transformers, though too few to cause a widespread outage. Some of the studies CBO considered evaluated the chance that the operations of the grid would be affected, but others—most notably the investigations of natural disasters—are assessments only of the likelihood of the event's occurrence, not of the consequences for the grid. For the studies that take into account the effects on the grid, many of the estimates of economic damage reflect extreme-case scenarios, so losses would probably be less in most cases.

Third, outages of similar geographic scope and duration can have different economic consequences depending on the types of customers and industries affected. Outages would tend to be more costly if, for example, they affected businesses that are more dependent on electricity as an input (banks, rather than farms, for instance) or businesses that are a key component of a supply chain (such as energy producers).

Fourth, relying on the experience of small outages to estimate the effects of large outages—as studies must do because historical experience with large outages is limited—might not capture the outcomes of those longer, bigger outages well. Many of the interdependencies between the electric grid and other critical infrastructure, such as communications, financial services, water treatment and sanitation, and public health, and the consequent economic feedback might be apparent only if and when a longer, bigger outage occurs.

Fifth, the limited number of studies available often lack detail on the types of costs that are included (such as business interruption costs, the destruction of wealth, and hidden costs). And even if the costs of various types are detailed, many of the studies do not clearly account for some broader feedback in the economy or interdependencies among critical industries that could positively or negatively affect the ultimate cost of an outage.

Finally, few of the studies detail the extent to which existing protections and procedures are accounted for in the estimates of damage. Because such strategies are routinely used to manage power flows, they may be

41. See John S. Foster, Jr., and others, *Report of the Commission to Assess the Threat to the United States From Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures* (April 2008), www.empcommission.org/reports.php; and Michael Frankel, James Scouras, and Antonio De Simone, *Assessing the Risk of Catastrophic Cyber Attack: Lessons From the Electromagnetic Pulse Commission* (Johns Hopkins Applied Physics Laboratory, 2015), https://tinyurl.com/y5nhgffq (PDF, 12.3 MB).

included, but if those strategies have implicitly been excluded, the economic effects would probably be smaller than the studies estimate, though by how much is unknown.

Approaches to Reduce the Cost of Major Outages

The utility industry has, in addition to physical protections, a number of operational and procedural protections to improve the security of the electric grid. Given advance warning of an impending threat, grid operators could act to minimize the impact by, for instance, boosting generation in some areas and reducing it in others to reroute flows of power or, if the threat seemed severe enough, even temporarily shutting down portions of the grid to reduce damage. Following a major disaster or attack that reduced capacity, grid operators might ration power by using rolling blackouts. And for prolonged outages, mobile generating units—diesel generators or natural gas combustion turbines—might be used to provide localized power or to power certain critical sectors, such as water treatment, sanitation, public health, and emergency services, among others.

Beyond those and other operational and procedural protections already in place, CBO identified a range of possible approaches to address threats facing the North American grid, along with their applicability to the range of threats considered in this report (see Table 1). Those approaches do not represent an exhaustive list of the strategies possible. Rather, they are meant to illustrate how approaches can differ. Some constitute strategies to prevent or limit effects of a disaster or attack, whereas others would improve or hasten recovery. Similarly, some approaches are widely applicable to a range of threats, but others are more narrowly focused.

Approaches That Would Prevent or Mitigate Damage

Among approaches that would prevent or mitigate damage, hardening grid components—that is, building protective barriers around power plants or transformers, upgrading the transmission system to protect it, or building new control centers to better withstand natural disasters or physical attacks—would apply to a range of threats to different degrees, depending on the specific approach implemented. For instance, protecting the transmission system (by, say, installing equipment that can absorb an influx of power or circuit breakers that isolate elements of the grid when power surges occur) would apply most to the threats of a severe solar storm or a high-altitude EMP, for which the potential for power surges is greatest. Certain other ways of hardening the grid (for instance, installing protective barriers or flood controls) could offer some protection against the physical damage that a hurricane, earthquake, or physical attack could bring. But such improvements would not protect against a cyberattack, which would most likely target plant operations or grid controls through communication networks. Similarly, satellites that would provide early warning of an impending solar storm would help grid operators prevent damage to large power transformers but would not provide any protection against an EMP.

Improving information sharing and developing microgrids—that is, areas of the grid that may be electrically isolated from the surrounding larger grid and remain fully functional—are other examples of approaches that might prevent or mitigate damage across a wide range of threats. Improving information sharing—reporting and sharing knowledge of threats, system vulnerabilities and corrective actions, and best practices, among other information—could help address the threat of a cyberattack, which is continually evolving. Developing microgrids could contain damage and insulate other areas from being affected, thereby potentially reducing the impact of a wide range of disasters and attacks. Indeed, some consider the development of microgrids as a potential protection against power outages that have stemmed from California wildfires in recent years. Microgrids would allow communities at lower risk from power outages to continue receiving service and isolate themselves from other areas at higher risk. But because the development of microgrids is in its infancy and is currently best suited for protecting smaller facilities, such as hospitals and military facilities, or, potentially, individual communities, the approach is unlikely to be used as a broad grid security measure for the foreseeable future.

Enhancing cyber protections and improving the physical security of grid components would represent more narrowly focused approaches, specifically addressing the threats of a cyberattack and a physical attack. Enhancing cyber protections includes continually improving the monitoring and assessment of global threats, identifying vulnerabilities and measures to safeguard systems, and promoting best practices, among other activities. In addition to the protective barriers around critical components discussed above, improving physical security

Table 1.

Possible Approaches to Address Large Threats to the North American Grid

		Approaches That Would Prevent or Mitigate Damage						Approaches That Would Improve Recovery			
	Type of Threat	Build More Early-Warning Satellites	Harden Grid Components	Improve Information Sharing	Develop Microgrids	Enhance Cyber Protections	Improve Physical Security	Increase the Number of Transformers Stockpiled	Improve Security of Blackstart Generators	Increase Backup Power for Critical Infrastructure	Provide More Disaster Response Training
Naturally Occurring	Severe Solar Storm (Geomagnetic disturbance)[a]	●	●	◐	○			●	◐	◐	●
	Major Hurricane (Category 4 or 5)		◐	○	○		○	○	○	◐	●
	Major Earthquake (Magnitude 7+)		◐	○	○		○	○	○	◐	●
Human-Made	High-Altitude Electromagnetic Pulse		●	◐	○			●	◐	◐	●
	Large Cyberattack[b]		○	●	○	●		○	◐	◐	●
	Physical Attack[c]		◐	○	○		●	○		○	○

● High Applicability to the Threat ◐ Medium Applicability to the Threat ○ Some Applicability to the Threat

Source: Congressional Budget Office.

a. A severe geomagnetic disturbance resulting from a powerful, fast-moving coronal mass ejection.

b. An attack that simultaneously targets a large number of critical grid systems or controls.

c. Although targeting a significant enough number of elements of the grid to affect power supplies regionally might be possible, doing so would be difficult. Accordingly, CBO expects that the most likely form of physical attack would be much more limited in nature.

includes activities such as improving personnel screening and increasing security staffing.

Approaches That Would Improve Recovery

Among approaches that would improve recovery once power is lost, one is improving the security of certain types of power plants necessary to help bring the grid back into operation—referred to as blackstart generators. Unlike most power plants, which require power to begin operations, blackstart generators—usually diesel generators, hydroelectric facilities, and certain types of natural gas generators—effectively require no outside power. Consequently, they can be employed to start a sequence of using smaller plants to progressively restart larger plants, ultimately returning power to the grid as a whole. A recent investigation concluded that there is sufficient blackstart capacity in place in the United States, but some analysts have noted the possibility that cyberattacks could specifically target the controls of those types of plants, thereby limiting their availability for repowering the grid.[42]

Similarly, increasing the availability of backup power for critical infrastructure—that is, maintaining a supply of diesel generators and other power supplies not dependent

42. See Federal Energy Regulatory Commission and North American Electric Reliability Corporation, *Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans: Blackstart Resources Availability* (May 2018), https://go.usa.gov/xdwJV (PDF, 704 KB); testimony of Andrew L. Ott, President and Chief Executive Officer, PJM Interconnection, before the Senate Committee on Energy and Natural Resources, *An Examination of Blackstart, the Process for Returning Energy to the Power Grid After a System-Wide Blackout, and Other System Restoration Plans in the Electric Utility Industry* (October 11, 2018), https://go.usa.gov/xyuj7; and testimony of Juan Torres, Associate Laboratory Director for Energy Systems Integration, National Reviewable Energy Laboratory, before the Senate Committee on Energy and Natural Resources (October 11, 2018), https://go.usa.gov/xyuj7.

on the grid's being operational—and providing more disaster response training could boost the recovery from a wide range of disasters and attacks. Both approaches are currently used to a degree. For example, hospitals and other medical services, some government facilities, and certain telecommunications services have backup power in place. The availability of backup power provides a degree of protection against any threat that can cause widespread outages. But unless accompanied by advances in microgrid or other technologies, backup power will probably remain a targeted, smaller-scale protection.

Disaster response training occurs at the plant and local levels and at the national level, where simulation exercises—like the Grid Security Exercise (or GridEx) sponsored by NERC—test the industry's ability to respond to threats such as a coordinated cyberattack and physical attack. Those exercises also help identify additional risks and interdependencies that may otherwise become apparent only after a significant loss of power.[43] GridEx is a recurring exercise, but it is voluntary and takes place every other year, suggesting that more comprehensive or more frequent exercises could provide additional security.

Two Illustrative Approaches That CBO Examined

To illustrate the considerations for policymakers as they decide how to address threats to the electric grid, CBO chose two approaches to analyze in some detail: deploying of a set of space-based sensors that would continue to provide (and in some cases improve) reliable early warning of a solar storm, and increasing reserves of large power transformers and related equipment.

CBO examined those approaches because they could address, at least in part, the potential long-term disruptions from some of the most consequential threats to the grid. Providing grid operators time to implement protections, space-based sensors would be intended to reduce the wide-ranging threat that a large solar storm could pose to large power transformers and, to a lesser extent, generating facilities. Large power transformers are vulnerable to such threats and, because they take many months to manufacture and install, greatly affect recovery times if they are damaged or disabled. Consequently, increasing reserves of transformers, along with related equipment, could address, at least in part, the security of a critical aspect of the grid against a range of the threats—including a severe solar storm, a high-altitude EMP, and possibly a cyberattack or physical attack—that could result in billions of dollars or, by some estimates, even more than a trillion dollars of economic damage.

In addition, the two approaches that CBO examined focus on improving the grid's security during different phases of an event. Spaced-based sensors are a before-the-fact approach that would allow procedures to be implemented to prevent or mitigate damage to the grid. A larger reserve of transformers and critical grid components, in contrast, is an after-the-fact approach that could enhance the pace of recovery if they were damaged or became inoperable.

Deploy New Space-Based Sensors to Detect Solar Storms

One approach to reducing the economic and social harm that would result from a large-scale disruption of the electric grid would be to deploy new, dedicated systems in space to provide early warning of solar storms by detecting them before they reach Earth. Similar systems exist in space today, but they are aging and were not designed to be the reliable source of data that is needed for uninterrupted forecasting of space weather. NOAA has formulated a program to deploy new satellites, but lawmakers have yet to commit to fully funding it.

Warned of a solar storm soon enough, operators can, depending on the expected severity, take a number of actions to protect the grid, minimize damage, and maximize the availability of power once the threat has passed. To the extent that the protections prevent damage (particularly to elements of the grid that would take many months to replace) or a power outage, they would avoid the costs of repairs and lost electricity sales and economic and social costs to customers affected by an outage. Moreover, other industries also facing significant risk from the effects of solar storms (such as the telecommunications and airline industries) could act on the warnings and take preventive action.

Existing Capabilities for Detecting Solar Storms. Solar storms can affect Earth in a variety of ways. Most consequential for the electric grid are coronal mass ejections, which send large quantities of charged particles and their associated magnetic fields into space. If those particles

43. See The President's National Infrastructure Advisory Council, *Surviving a Catastrophic Power Outage: How to Strengthen the Capabilities of the Nation* (December 2018), www.hsdl.org/?abstract&did=819354.

hit Earth, they can disturb its magnetic fields and disrupt currents in power lines and other equipment essential for the grid to function.

Currently, to prepare for such a geomagnetic disturbance that might result from a solar storm, utilities rely on early notifications from space weather forecasts provided by NOAA's Space Weather Prediction Center. The center processes data from existing satellites and uses computer models to predict the severity of the effects that a solar storm will have on systems on Earth, aircraft in the air, and satellites in orbit. It issues watches, warnings, and alerts. Smaller solar storms are relatively common, notifications occur, and grid operators are practiced at responding in ways that protect their ability to deliver power to their customers.

Just as there are categories for classifying hurricanes, there are space weather scales for communicating the expected severity of solar storms. Electricity suppliers, telecommunications providers, providers of precision navigation services, airlines, and other industries monitor the space weather forecasts and take preventive action as needed. Grid operators, for example, can delay critical maintenance, bring in reserve power, and, if necessary, temporarily shut down sections of the grid to ensure continued delivery of power to critical self-contained areas or to contain losses in other areas. But preventive actions themselves can have costs (such as preventive evacuations and business closures in a broad area in anticipation of a hurricane that misses that area), so more accurate space weather warnings reduce the unnecessary actions that industries otherwise would take.

The warning system depends on data that NOAA receives from instruments on a patchwork of satellites (see the appendix for a discussion of the sensors and satellites used to detect solar storms). Almost all of those satellites were designed for research purposes and not for providing reliable continuous data for early notifications of solar storms, and most of the satellites are well past their design life and could stop functioning without warning. If any of the existing instruments fail, NOAA's ability to provide such notifications will be reduced, possibly severely. Moreover, after such a failure, building a replacement satellite and placing it in orbit to restore NOAA's ability would take years, and in the interim, the agency would have little ability to forecast solar storms.

Two types of instruments are essential for providing early warning of coronal mass ejections: a coronagraph that takes images of the sun to detect solar activity and a set of instruments that measure the stream of particles from the sun (the solar wind) to estimate the timing and size of the storm and the severity of its effects on Earth. Coronagraphs can provide early warning if they are in certain orbits around Earth or the sun, but measurements of the solar wind must be taken in orbits between Earth and the sun. Data from other types of instruments that measure ultraviolet radiation or other phenomena emanating from the sun are important for detecting solar flares and radiation storms (which affect satellites and communications) and can provide complementary information about coronal mass ejections.

The Solar and Heliospheric Observatory (SOHO) is the only source of coronagraph images of the sun from the direction of Earth. Built by the National Aeronautics and Space Administration (NASA) and the European Space Agency (ESA) as a research mission, it was launched in 1995 and is already more than 20 years past the end of its planned service life. SOHO's solar panels are degrading and are expected to stop providing enough power for operations by 2026. The Deep Space Climate Observatory (DSCOVR) is the primary instrument used by space weather forecasters to measure the solar wind. Launched in 2015, it was expected to operate for at least five years. Both satellites are in orbits between Earth and the sun and were built for solar science missions, not to provide reliable solar data for space weather forecasters. Both satellites (along with another aging satellite, the Advanced Composition Explorer (ACE), which provides a backup source of data on the solar wind) are expected to stop operating by the mid-2020s.

Options for Sustaining or Improving Space Weather Monitoring. CBO examined three options that would sustain and, in some cases, improve capabilities to monitor solar activity in space:

- The first option would improve on today's capabilities by deploying better and more reliable satellites. NOAA would build two new satellites, one deployed in 2024 and another deployed about five years later, when the first reached the end of its planned service life. Both satellites would carry a coronagraph and instruments to measure the solar wind in an orbit between Earth and the sun. The equipment would be more modern, reliable, and accurate than what is now

in space. NOAA would also build a ground system to receive and process data.

- The second option would place a coronagraph on each of the next generation of meteorological satellites (those used for forecasting weather on Earth) that orbit Earth, but it would not deploy new solar wind instruments.

- The third option would be like the second except that it would place the coronagraph on the International Space Station—a stopgap approach if the satellites deployed today fail sooner than expected.

Both the second and third options would be less costly but would provide less accurate and less useful forecasts.

NOAA already has under way a program to implement half of the first two options as part of its Space Weather Follow On program: The agency would acquire the first of the two satellites in the first option and deploy a coronagraph on only one meteorological satellite. To date, the Congress has funded a small fraction of the costs of NOAA's program and has not yet committed to full funding. The agency has also considered the third option as a stopgap measure but currently has no plans to pursue it because it would not meet NOAA's requirements for reliable continuous data.

NOAA's strategy would change the U.S. approach to the space weather satellite program from one that relies on satellites designed for other purposes to one that establishes those satellites as part of a dedicated infrastructure for detecting space weather—echoing the approach that NOAA has used for meteorological satellites for decades.

The private sector has not demonstrated that it would invest in monitoring and forecasting space weather on its own and is probably unlikely to do so. Forecasts of solar conditions and warnings of impending storms amount to a public good. Thus, for matters of public safety and economic stability, among others, the benefits of early detection and warnings would probably be shared with entities providing no funding for the spaced-based sensors. That broad availability of the information limits the incentive for the private sector to fund the services. In addition, the benefits of solar storm warnings extend well beyond the U.S. electricity sector. Such warnings could preclude widespread disruptions in telecommunications, GPS (global positioning system) navigation, and transportation that could impose costs on many U.S. households and businesses. The diffuse nature of those benefits makes it even more unlikely that the private sector alone would fund solar monitoring.

Deploy a New Dedicated Space Weather Satellite Between Earth and the Sun. Under this option, NOAA would get the funding that it estimates it would need to develop and build the new satellite that it is currently planning, the Space Weather Follow On-L1 (SWFO-L1), which would provide continuous data after SOHO and DSCOVR stop operating. NOAA would also get the funding it has requested to build the ground system planned for collecting and distributing the data from the satellite. This option would go one step further than NOAA's plan: It would also fund a second satellite to replace the first at the end of its service life. Because building a satellite takes several years, NOAA would start constructing the second satellite and its instruments after the first satellite was launched and would launch it about five years after the first, or later if the first lasted longer than anticipated. The first satellite would be launched in 2024 and would have an expected life of five years.

The new space weather satellite would be placed in orbit at the same location as SOHO, DSCOVR, and ACE, around a point known as the Lagrange 1 point, or L1, between Earth and the sun, about 1 million miles from Earth, where the satellite would maintain a fixed position relative to those two much larger bodies. The satellite would include a coronagraph, specifically, the compact coronagraph that the U.S. Naval Research Laboratory is currently developing for NOAA.[44] Other sensors on the satellite—a magnetometer, a solar wind plasma detector, and an ion spectrometer in a package called the Space Weather Instrument Suite—would monitor the solar wind and measure the intensity and timing of storms headed toward Earth.

Like the satellites currently in service, the new satellite would provide between 15 and 60 minutes of warning time about the severity of an incoming solar storm. Compared with the existing satellites (which were designed for research), the instruments on the new

44. See Elsayed R. Talaat, Director, Office of Projects, Planning, and Analysis, National Oceanographic and Atmospheric Administration, "NOAA's Current and Future Space Weather Architecture" (presentation to the 2019 Space Weather Workshop, April 4, 2019), https://go.usa.gov/xdQPc (PDF, 2.0 MB).

satellites would be designed to provide better data, be more reliable, and be better suited to the needs of space weather forecasters. For example, the coronagraph would be designed to better operate in the high-radiation environment associated with a severe solar storm, conditions that can overwhelm the existing coronagraph. In addition, the magnetometer on the new satellite would be designed to provide better resolution for measurements of the strength and direction of the magnetic field headed toward Earth, which are key factors in predicting the effects that a storm will have on Earth and the electric grid.

The Congress appropriated about $7 million for the new satellite in 2019, and the Administration requested about $11 million in its 2020 budget.[45] (Those totals exclude the cost of developing the coronagraph for the new satellite). Altogether, NOAA expects to need about $500 million over the next 10 years to acquire the first satellite with its coronagraph, launch it in 2024, build the ground system, and operate and support the satellite and ground system for five years.[46]

Overall, CBO estimates that the cost of a dedicated space weather satellite program similar to NOAA's proposed SWFO-L1 program (but including a second satellite and its launch costs) would be about $1 billion (in 2020 dollars) over a 10-year period (2020 through 2029):[47]

- Developing and building the two satellites and their coronagraphs would cost almost $500 million.
- Launching the satellites into their orbits would cost about $200 million. For the first satellite, NOAA plans to share a ride to L1 on the rocket that will carry a NASA research satellite, the Interstellar Mapping and Acceleration Probe (IMAP), into orbit around L1.[48] Thus, the launch would be essentially free to NOAA. Launching the second satellite on its own would cost about $200 million, although costs could be lower if the second satellite could also share a ride. In addition, commercial providers are currently developing lower-cost launch services that might be available when the second satellite was ready to launch, but their costs are not yet known.
- By NOAA's estimates, building the ground system for the satellites would cost almost $200 million.
- Operating the system and providing technological support would cost about $30 million a year, or $150 million over five years, from 2024 through 2029, CBO estimates.

Those estimates are based on data from NOAA and may change as it continues to refine its plans. Moreover, CBO's estimates cover the next 10 years, but if the United States remains committed to providing accurate and timely space weather forecasts, many of those costs (such as building replacement satellites and operating the system) would continue at roughly the same level beyond 2029. Other costs, such as building the ground system, would be onetime costs.

A recent investigation of a hypothetical once-per-century severe solar storm affecting the United Kingdom concluded that current satellite capabilities would reduce GDP losses by about 80 percent relative to a case in which no satellites are available to monitor solar conditions, which will be the situation if current satellites become disabled and are not replaced.[49] Though existing satellites are currently in use, new satellites would have to

45. For 2020, the Congress provided a larger appropriation than NOAA requested for the overall SWFO program, which includes the SWFO-L1 satellite as well as the ground system and a coronagraph that would go on a future meteorological satellite. As of this writing, NOAA has not determined how that increase will be distributed among the elements of the program, including the new satellite.

46. CBO's analysis of costs is drawn primarily from National Oceanic and Atmospheric Administration, *Space Weather Follow-On: Space Weather Observation Needs and Plans, Including and Beyond a Solar Coronagraph* (March 2019), Appendix D.

47. That figure differs from one provided in Congressional Budget Office, cost estimate for S. 881, the Space Weather Research and Forecasting Act (May 31, 2019), www.cbo.gov/publication/55322. That earlier estimate covered 5 years, rather than the 10 covered here, and did not include building and launching a second satellite.

48. Although IMAP is designed for other purposes, it will provide measurements of the solar wind that will be useful for predicting space weather. Those data would complement rather than duplicate what DSCOVR provides and SWFO-L1 would provide. If SWFO-L1 failed or was not developed and deployed, IMAP could provide at least a partial alternative source of data on the solar wind.

49. Edward J. Oughton and others, "A Risk Assessment Framework for the Socio-Economic Impacts of Electricity Transmission Infrastructure Failure Due to Space Weather: An Application to

be deployed by the mid-2020s to ensure continued monitoring. The SWFO-L1 satellite and its ground system would offer a number of improvements over the existing configuration, including better and more reliable sensors and a faster transmission of the data to Earth. Those capabilities would probably help reduce losses further (that is, by more than 80 percent) by providing faster and more accurate forecasts of solar storms.[50]

Translated for the U.S. economy, that study's findings suggest that the new satellite would help avoid GDP losses ranging from $128 billion to $560 billion (that is, 80 percent of the costs of a severe solar storm without any monitoring based on one study's estimated range of $160 billion to $700 billion, as discussed above).

Those estimates of avoided losses can be coupled with the aforementioned survey of point estimates of the likelihood of a severe (Carrington-level) geomagnetic disturbance affecting the United States (1 percent to 12 percent over a decade) to yield two estimates spanning a broad range of expected losses of GDP that might be prevented by a dedicated space weather satellite and its replacement. Specifically, those estimates would be about $1.3 billion (0.01 x $128 billion) and about $67 billion (0.12 x $560 billion) over 10 years.

Even though those estimates are imprecise, they do not convey the extent of the uncertainties. The GDP losses that a Carrington-level event would impose could be higher or lower than the estimated range of $160 billion to $700 billion. In addition, the estimated likelihood of a 1 percent to 12 percent chance of such an event over a decade does not capture the full range of possibilities; the actual likelihood could be even closer to zero than the bottom of the range or substantially higher than the top of it.

Beyond those uncertainties, other factors could positively or negatively affect a decision to fund the satellites. Avoiding or lessening a disaster stemming from a solar storm would do more than protect the economy's output; it could protect against, among other things, loss of life, damage to public health, and the destruction of wealth. For the federal government, it could protect tax revenues and avoid or reduce the spending that follows from disasters. Factors working in the opposite direction are the possibility that false alarms raised by the satellite could create new costs and the possibility that the avoided losses could apply only far in the future (and a dollar in the future is worth less than a dollar today, even after being adjusted for inflation).

Install Coronagraphs on New Weather Satellites. In addition to asking for funding for the SWFO-L1 satellite, in its 2020 budget request NOAA proposed deploying a compact coronagraph on the next weather satellite that it plans to deploy in a geostationary orbit around Earth. That geostationary weather satellite, the Geostationary Operational Environmental Satellite (GOES-U), would be launched in 2024. (Three GOESs are currently in orbit—two in use and one as a spare.)

NOAA's motivation for adding a coronagraph to GOES-U is twofold: to deploy a coronagraph as soon as possible to provide a hedge against the loss of SOHO (the only other coronagraph in space between Earth and the sun) and to provide a long-term backup for the coronagraph that it plans to deploy on SWFO-L1. That approach is consistent with NOAA's goal of creating a robust capability for predicting space weather (like the approach the agency takes for its meteorological forecasting mission) that will continue to function during large solar storms and that includes backups for the most important instruments in case they fail.

Under CBO's option, NOAA would get the funding it estimates that it will need to place a compact coronagraph on GOES-U, but this option would go one step further and provide funding to place another compact coronagraph on the satellite that follows GOES-U,

the United Kingdom," *Risk Analysis*, vol. 39, no. 5 (November 2018), https://doi.org/10.1111/risa.13229.

50. By one estimate, enhancing the capabilities of space weather satellites relative to those in space today—including better sensors and faster transmission of data from a satellite at L1 (as this option would do) and the positioning of an additional satellite at the L5 Lagrange point to provide even earlier monitoring of solar conditions—could reduce GDP losses from a solar storm by another 70 percent relative to those that could occur with current capabilities. Taken together with the protections afforded by the current capabilities, satellites with enhanced capabilities might reduce losses by about 95 percent relative to those that could arise from not having a space weather satellite at all. The option assessed in this report would provide only part of that enhancement because it would not include a satellite at L5, although the European Space Agency is considering such a system. See Edward J. Oughton and others, "A Risk Assessment Framework for the Socio-Economic Impacts of Electricity Transmission Infrastructure Failure Due to Space Weather," *Risk Analysis*, vol. 39, no. 5 (November 2018), https://doi.org/10.1111/risa.13229.

which could be launched in the late 2020s. If combined with the first option, this option would provide a redundant system (which NOAA plans) for detecting and forecasting the effects of solar storms, because a coronagraph in geosynchronous orbit would provide data of about the same quality and as quickly as a coronagraph in orbit closer to the sun does.

This option would cost almost $150 million over 10 years, CBO estimates, if NOAA's budget documents prove to be accurate. Completing the development of the first sensor would require about $15 million, and completing the integration with GOES-U, about $40 million. (Building the coronagraph and integrating it into the next GOES would cost about $50 million more.) There would be no additional launch costs because the coronagraphs would be placed on satellites that NOAA is already planning to launch. Operating costs would be about $5 million a year after GOES-U is launched, CBO estimates. No new ground system would be necessary; instead, the solar weather instruments would rely on the ground system that NOAA uses for the GOES system.

Mounting a coronagraph on GOES-U and a successor satellite would cost almost $900 million less over 10 years than building and launching the dedicated satellite and a spare, as in the first option. By itself, however, this option would lead to far less accurate forecasts than NOAA can make today: When the DSCOVR satellite stops operating, NOAA will lose the ability to measure the particles associated with a solar storm, and its forecasts will provide significantly less warning time and far less accurate estimates of the likely effects on Earth than it can provide today.

Another, albeit transitory, concern with placing a coronagraph on a geostationary satellite is that there are times during the year when Earth would block the coronagraph's view of the sun for several minutes during the day. Having a coronagraph on both of the GOESs that NOAA keeps in geostationary orbit (one over the East Coast of the United States and one over the West Coast), which could occur as soon as 2030 under this option, would eliminate that problem because only one satellite would be in Earth's shadow at a time.

Install a Coronagraph on the International Space Station. Another option that has been proposed is placing a coronagraph on the International Space Station.[51] Such a program would cost almost $100 million over 10 years, CBO estimates. Of that total, about half would fund completing the development of the sensor and integrating it on the space station. Operating costs would make up the other half of the total and would be similar to those for GOES-U, CBO estimates, about $5 million a year. Launch costs are not included, because the instrument would share a launch vehicle with other equipment headed to the space station. Altogether, mounting a coronagraph on the space station would cost more than $900 million less over 10 years than launching a dedicated satellite.[52] It would also cost about $50 million less than deploying coronagraphs on future GOESs because that option would place two coronagraphs in orbit at a time.

The primary motivation for installing a coronagraph on the International Space Station would be to get an instrument in space as quickly as possible if SOHO failed earlier than NASA now estimates. In theory, that task could be done as early as 2022, or about one or two years before GOES-U and SWFO-L1 are scheduled to be launched. Although it could be deployed sooner, a coronagraph on the space station would have a serious shortcoming: It would be able to observe the sun for only about 12 hours a day because the space station, which orbits close to Earth, spends half of each day in the shadow of Earth. Consequently, it would provide a poor substitute for either of the first two options, in which the coronagraphs would be able to observe the sun continuously. But being able to observe the sun even half the time would be better than nothing if SOHO failed before one of those satellites could be placed in orbit.

Increase the Stockpile of Transformers

Another approach to reducing the economic and social effects that would result from a large-scale disruption of the electric grid would be to enact federal policies or programs to increase the number of large power

51. See, for example, Kyung-suk Cho, "Toward a Next Generation Solar Coronagraph: Development of a Compact Diagnostic Coronagraph for the ISS," *Journal of the Korean Astronomical Society*, vol. 50, no. 5 (October 2017), pp. 139–149, https://doi.org/10.5303/JKAS.2017.50.5.139.

52. NASA has said that a coronagraph installed on the space station could be retrieved and used later on a dedicated satellite. In that case, the development and purchase cost of the coronagraph would be avoided for one of the dedicated space weather satellites.

transformers, along with related equipment, held as replacements in inventory. Large power transformers handle about 90 percent of electric power generated, and because they allow power to flow throughout the grid, they are potentially vulnerable to the strong electric currents that could be caused by a severe solar storm or a high-altitude EMP.[53] Such an event could lead to widespread and sustained outages of electricity if spare transformers were not available because electricity suppliers might have to wait more than a year for new transformers to be manufactured.

Existing Transformer Reserve Programs. A number of private-sector efforts have been undertaken to protect the electric grid. For large power transformers and related equipment, a number of private reserve programs have been developed in recent years. One effort, the Spare Transformer Equipment Program (STEP), is an arrangement in which participating electricity suppliers are contractually bound to maintain a certain number of spares and make them available to other participants in the case of a terrorist attack (so a solar storm and other naturally occurring threats would not automatically be covered). STEP is designed so that participating electricity suppliers could restore their system to at least a minimally working order after a loss of up to five substations (transmission facilities each containing one or more transformers).[54]

Another effort has been the formation of a private company, Grid Assurance, by a collection of electric utilities. Rather than obligate individual utilities to purchase or maintain a certain number of spare transformers, Grid Assurance buys and maintains spare transformers on behalf of participating utilities with the intent of lowering costs by pooling purchases. Other private programs include SpareConnect (a less formal, nonbinding sharing arrangement), Wattstock (a program of smaller, more rapidly deployable spares for short-term use), the Spare Equipment Database Program (a centralized catalog of spare equipment held by participants that may be available on a nonbinding basis), and the Regional Equipment Sharing for Transmission Outage Restoration program (a voluntary program in which utilities identify spares available for sale to other participants in the event of a regional disaster or an attack).

However, little information is available about the coverage of those existing programs, in part because of security concerns about exposing potential weaknesses of the grid. By one estimate, about 200 electric utilities participate in STEP, SpareConnect, and the Spare Equipment Database Program—the most developed programs. Together, they may hold as many as 300 spare large power transformers, which would cover at least two-thirds of the power provided in the United States.[55] However, that estimate is uncertain because it is based in part on information provided in regulatory filings made before the programs were fully operational and because it may reflect some double-counting owing to utilities' overlapping memberships in the programs. For many of the more common scenarios, those reserves may be sufficient. But for the most extreme scenarios, they may fall short of what would be required to avoid widespread, long-term outages.

Options for Increasing the Number of Replacement Transformers. CBO examined three options for increasing the number of replacement transformers beyond the number that the private sector might invest in without federal intervention.

Subsidize Purchases. One option for increasing the stock of replacement transformers is to provide subsidies to electricity suppliers to purchase transformers and hold them in reserve. That arrangement could be accomplished either by appropriating funds or by establishing a tax credit for that purpose. Private-sector investment in additional spare transformers is at least partially determined by the cost of purchasing them and the benefits the utility would receive from having the additional units. Federal subsidies would reduce utilities' purchase costs, thereby increasing the number of spare transformers that they would find it worthwhile to purchase.

One advantage of subsidizing private purchases is that it would leave decisions about the types of transformers'

53. Electric Power Research Institute, *Considerations for a Power Transformer Emergency Spare Strategy for the Electric Utility Industry* (prepared for the Department of Homeland Security, September 30, 2014), https://go.usa.gov/xp9Qg (PDF, 1.3 MB).

54. See Department of Energy, Office of Electricity Delivery and Energy Reliability, *Strategic Transformer Reserve: Report to Congress* (March 2017), https://go.usa.gov/xyu8U (PDF, 9.0 MB).

55. ICF, *Assessment of Large Power Transformer Risk Mitigation Strategies* (prepared for the Department of Energy, Office of Energy Policy and Systems Analysis, October 2016), https://go.usa.gov/xyu8D (PDF, 809 KB).

designs and site-specific factors in the hands of the electricity suppliers.

A disadvantage of such a program is the difficulty the government would face in setting the appropriate subsidy level. Ideally, doing so would entail determining the optimal total reserve, the reserve the utility industry would build without any subsidy, and the effects of different subsidy levels. In addition, because federal authorities would be unable to determine precisely what investments electricity providers would have made in the absence of a subsidy, the subsidies could not be restricted to only those transformers that increased the total reserve stock; a significant share of the federal costs—perhaps the majority—would serve only to reduce the utilities' net cost of units that they would have purchased even in the absence of the federal program.

Invest in a Federal Stockpile. A second option for increasing the stock of replacement transformers is the creation of a federally owned stockpile. Under this option, the federal government would buy transformers and hold them in one or more secure locations that would not be vulnerable to the risks faced by transformers that are connected to the electric grid. Then, in the event of damage to the transformers in operation, the government could either sell the spares to electricity suppliers or provide them without charge.

The cost of a federal stockpile would depend in part on the number of transformers and their cost (between an estimated $2 million and $9 million each).[56] The Department of Energy estimates that at least 100 units would be necessary for a federally operated reserve, though that number could be higher depending on how extensive a reserve program was desired and the degree to which it displaced private investment.[57]

The cost of the program also would depend on the costs of transporting and installing replacement transformers (estimated by the Department of Energy to boost individual costs by about 30 percent) and storing them until they were needed for use.[58] The cost of storage would depend partly on the number of storage facilities selected, a choice involving some trade-offs. Locating the transformer stockpile in a few central locations would probably reduce capital costs because fewer storage facilities would be necessary, but it would increase the time required to put the reserves into service when needed and would probably make the stockpile more vulnerable to a physical attack. Greater decentralization, perhaps including some on-site storage, would reduce transportation costs between the storage and service locations and would reduce the chance that the stockpile would be targeted for an attack but could increase capital costs, as more reserve units would be necessary for replacements to be available locally. Implementing a federal reserve program would require assessing those trade-offs and other technical details, probably in extensive consultation with the utility industry.

One argument against having the federal government create and hold a stockpile of transformers is that it could displace a large amount of private investment and result in little change in the overall number of replacements available. CBO expects that electricity suppliers would regard transformers in a federal stockpile as substitutes for privately held stockpiles and reduce their own efforts to build reserves. Such substitution might not reduce privately held reserve transformers one for one, because differences in transformers' designs and site-specific factors could mean that transformers in federal reserves might not be considered perfect substitutes in all instances. But federal spending for a public-sector reserve could displace a large amount of private investment and result in little change in the overall number of replacements available.

Set a Federal Requirement. A third option for increasing the number of spare transformers would be for the federal government to require that electricity suppliers hold private reserves of a specified size. That option would have negligible costs to the government and could be implemented in a way that did not undercut cost-effective investments the private sector would have made on its own to avoid the most likely types of outages.

56. Department of Energy, Office of Electricity Delivery and Energy Reliability, *Large Power Transformers and the U.S. Electric Grid* (April 2014), https://go.usa.gov/xyu8R.

57. Department of Energy, Office of Electricity Delivery and Energy Reliability, *Strategic Transformer Reserve: Report to Congress* (March 2017), https://go.usa.gov/xyu8U (PDF, 9.0 MB).

58. Department of Energy, Office of Electricity Delivery and Energy Reliability, *Large Power Transformers and the U.S. Electric Grid* (April 2014), https://go.usa.gov/xyu8R.

However, the feasibility of such a mandate is unclear. One issue is the government's ability to hold the utility industry as a whole responsible for the mandate. Although FERC has jurisdiction over the reliability of bulk power, by law FERC can only review and approve standards set forth by NERC. FERC itself has no legal authority to propose standards. So mandating the private sector's participation in a reserve program is outside FERC's jurisdiction. However, the Congress has the option of amending the Federal Power Act to provide that authority to FERC.[59]

Another issue is that the federal government has less expertise about the operations of energy suppliers than do the suppliers themselves, which raises the possibility that a federal mandate would not efficiently reflect the public interest as intended. For example, the government would probably be less equipped to determine the appropriate number of spare units required, their size, and other technical characteristics.

Some Key Considerations for Policymakers

Decisions about federal actions can often require policymakers to answer three key questions:

- What is the rationale for federal intervention?
- What factors should be weighed when contemplating such intervention?
- How should the advantages and disadvantages of intervention be compared amid great uncertainty?

CBO's catalog of major threats to the electric grid and its examination of approaches to addressing those threats, including its consideration of two approaches in detail, illuminate the challenges in addressing those three questions. The rationale for federal intervention will vary for different approaches. A variety of factors, sometimes noneconomic ones, can come into play. And the possibilities for accurately assessing advantages and disadvantages of individual approaches will range from being relatively straightforward to being extremely uncertain.

Gauging the Rationale for Federal Intervention

In many cases, the private sector's decisions about what to produce, and how to produce it, will both maximize profits and be consistent with an allocation of resources that is best for society as a whole. That coincidence of private and public benefits is most likely to occur when all of the societal costs and benefits associated with producing and consuming goods are fully reflected in the prices that households and businesses pay for them.

A rationale for federal intervention is to address a "market failure," that is, when some of the costs or benefits associated with producing or consuming a good are not reflected in the prices paid. In such cases, federal intervention may help correct the failure. For example, a company that invests in basic science research may generate knowledge that is widely beneficial, but because the knowledge may be of a form that it is freely available, the company cannot fully capture the benefits of the research in the form of profits. Thus, absent intervention, there will be too little investment in that basic research from a societal point of view.

Another rationale for government intervention is to address underinvestment when the social benefits can exceed the private benefits. For instance, to help mitigate the financial risks of terrorism, the federal government provides catastrophic federal reinsurance through the Terrorism Risk Insurance Act (TRIA) program, which provides federal payments to private insurers to reimburse them for a portion of their terrorism-related losses on commercial policies after an attack. Without TRIA, the supply of terrorism insurance would be smaller—rates would be higher and policy limits could be lower—and commercial developers in higher-risk areas might have difficulty finding financing for their projects.[60] As a result, new construction and job creation could lessen and economic growth could slow, even with the likelihood that some of the development that occurs in higher-risk areas under TRIA would occur in lower-risk areas if the law did not exist. With TRIA, commercial construction in major urban areas is greater, which helps preserve economic benefits resulting from the concentration of related businesses. But that continued construction also increases possible losses from a terrorist event.

The two approaches CBO examined in detail reflect potential differences in the rationale for federal intervention. Sensors dedicated to monitoring solar conditions are unlikely to be funded by the private sector acting

59. Federal Power Act, 16 U.S. Code § 824o.

60. See Congressional Budget Office, *Federal Reinsurance for Terrorism Risk: An Update* (January 2015), www.cbo.gov/publication/49866.

alone because the advantages of improved warnings would be so widely shared and the information would be available to entities choosing not to provide funding. In contrast, having access to spare components—transformers and other equipment—is in the business interest of electricity suppliers, so they would be more likely to invest in having them in reserve. However, to the extent that spare components enhance general safety and economic stability following a power loss, the private sector may purchase fewer reserves than might be best from a societal perspective.

Other approaches also reflect that difference in the rationale for federal intervention. Increased hardening of facilities and equipment and improvements in the physical security of individual grid components are arguably in the business interest of individual power suppliers, so government intervention might not be necessary. In contrast, improvements in information sharing or in wide-scale disaster response training—though imparting benefits to individual power suppliers—might require a degree of coordination beyond what private industry would be able to conduct acting on its own.

Deciding Which Factors to Weigh When Considering Federal Intervention

CBO's analysis has focused on potential losses of GDP and the federal budgetary and private costs of policies. Those are two among many factors that policymakers may want to take into account when choosing among policies to secure the electric grid. Just which factors play a role in the decisions and what weight they are given will matter.

Loss of GDP does not account for all the costs of an outage. For instance, power outages will cause inconvenience, personal discomfort, and possibly even loss of life. Other such factors include the potential effects on national security and public health. Policymakers might wish to pursue specific measures even if the loss of GDP might be relatively small or the cost of the policy might be high if the measures maintain military preparedness or the ability to address acute medical needs for affected populations.

Another factor is the possibility that the intervention will impart additional costs to society that go beyond federal budgetary and private costs. For example, subsidies and regulations alter decisions about what to produce and how to produce it in ways that can cause economic inefficiencies—outcomes in which the combined well-being of consumers and producers is not maximized—so that the total costs of additional security measures extend beyond the actual expenses of purchasing them.

Still another factor to weigh could be the distributional effects of the risks to the electric grid and the costs of actions to mitigate those risks. For instance, the costs of disruptions to the grid and the benefits of avoiding them might fall more heavily on people with lower income because they have fewer resources to draw upon, such as the money to purchase backup power supplies for their homes or to relocate to areas less likely to experience outages. Similarly, certain areas of the country, such as urban locations, might be less able to sustain a lengthy loss of power than other areas.

Comparing the Advantages and Disadvantages of Federal Intervention Amid Uncertainty

Another consideration is how to compare the advantages and disadvantages of government intervention when estimates of them are highly uncertain. Avoiding a loss of GDP is one benefit of improving the security of the grid and reducing the chance of a widespread, enduring power outage, but estimates of the extent of the potential loss are often highly uncertain. Estimates of the likelihood of a potential loss have the same limitation. So a large range of possible outcomes complicates decisions about efficient investment in security measures for the electric grid.

Some naturally occurring threats, such as hurricanes, have occurred frequently enough that relatively reliable estimates of their likelihood and impact have been formed. But others, such as solar storms, have rarely occurred, leaving uncertain just how likely they are and whether their effects would be large. And so little information is available about some threats, particularly some human-made threats, that only judgments about general trends of likelihood or effects may be possible.

Individual approaches for improving the security of the electric grid also involve a number of uncertainties about either their cost or their effectiveness. For new space-based sensors for solar monitoring, the budgetary costs of building and deploying them are broadly known and suggest a relatively small expense in exchange for some protection from solar storms. But less is known about some of the potential costs for the private sector—for

instance, the costs of false positive warnings, which could prompt the private sector to take precautions against storms that ultimately do not affect the grid's operations.

Moreover, the additional protection that new sensors would provide is not certain. Existing satellites are aging and may be nearing their end of life, so they could become less effective or cease operating altogether. In such cases, the extent of the additional protection from replacing sensors is relatively clear. The improvements are less clear in the case in which existing satellites are in operating condition, although CBO expects that new sensors—either through more accurate monitoring or longer operating lives—would offer additional protection.

The effects of increasing the number of replacement transformers are similarly difficult to evaluate, as are the additional costs to the government and private sector of doing so. Although transformer stockpiles might address many threats, the reserves do not prevent outages but merely shorten them. How much so depends on the severity of the disaster or attack and the damage incurred by the grid. And even then, outages of different lengths and geographic scope will have different economic consequences. Furthermore, federal options aimed at increasing the reserve would be complicated by uncertainty about the appropriate number of units to stockpile, the number of units already stockpiled by the private sector, and the policy's effect on the private sector's holdings, among other factors. Should policymakers wish to increase the reserve of replacement transformers, CBO expects that subsidizing purchases by the private sector would be more likely to increase the overall size of the reserve than having the government do the purchasing. Subsidies would cause the private sector to purchase more than it otherwise would have and leave decisions about the type and location of reserve transformers in the hands of the private sector. In contrast, direct federal purchases probably would cause the private sector to reduce its purchases.

The uncertainty involved in decisions to protect the electric grid against severe threats can work in two directions. It can argue for policies to guard against extreme events beyond those that would be supported by estimates of the avoided loss of GDP and the cost of the policies. Or it can argue for fewer measures precisely because the benefits and costs are not well known.

Appendix: How Satellites Monitor Space Weather Today

Space weather is determined primarily by solar activity and the flow of the solar wind, the stream of highly ionized gas that flows continuously outward from the sun through the solar system. When the sun ejects a large amount of radiation or material rapidly in an event such as a solar flare or a coronal mass ejection, the solar wind becomes intensified. If the shock wave and particles associated with that solar activity strike Earth, they can cause problems. Having advance warning of an impending solar storm allows operators of different systems (including the electric grid, GPS [global positioning system] satellites, communications satellites, airlines, and spacecraft) to take steps to reduce those effects.

The United States uses a variety of sensors based on a collection of existing satellites to provide warnings of solar storms. Some of the most important of those satellites were not intended for that task. The sensors look for unusual solar activities and measure the radiation and particles, and their associated magnetic fields, coming from the sun. The space weather forecasters at the National Oceanic and Atmospheric Administration (NOAA) use those data in models to forecast space weather.

Essential Features of Space Weather Sensors and Satellites

Three primary types of instruments are used to detect a solar storm headed toward Earth, determine its strength and magnetic field, and estimate its arrival time. Perhaps the most important sensor for detecting a storm is a coronagraph. That instrument images the sun's corona (the outermost part of the sun's atmosphere) so that solar flares and coronal mass ejections can be observed.

A coronagraph can provide one to four days' notice that a solar storm might be approaching, but forecasters need data from another set of instruments to determine its size and speed and the direction of its magnetic field so that they can predict when it will reach Earth and what effects it might have. To estimate the possible severity of a storm's effects on Earth, they need estimates of the strength and direction of the magnetic field created by the charged particles. Those estimates cannot be made until the particles pass over a monitoring satellite equipped with sensors for measuring the solar wind. The closer that satellite is to the sun (and the farther it is from Earth), the more warning time it can provide. Satellites that monitor the solar wind are usually placed in orbit around the L1 Lagrange point, a location about a million miles from Earth directly between it and the sun. There, the gravitational pull of Earth and the sun create conditions so that a satellite can orbit around that point throughout the year as that point revolves around the sun.[1] At that location, the satellite can provide a good estimate of a solar storm's size and severity 15 minutes to one hour before the storm hits Earth, depending on its speed.

A different set of instruments, x-ray and ultraviolet solar imagers, can provide an earlier indication of the potential severity of a storm because those forms of radiation travel at the speed of light. But the estimates of severity of a coronal mass ejection from those sensors are less accurate than what can be learned by directly measuring the solar wind.

Coronagraphs and the x-ray and ultraviolet sensors can be located closer to Earth without affecting warning time much because the energy they detect is moving at the speed of light, much faster than the particles. However, to be effective in monitoring the sun, they need to be located outside Earth's atmosphere so that their view of the sun is not blocked by the Earth.

1. There are five known Lagrange points in the Earth-sun system. Like L1, L2 is about a million miles away from Earth on the Earth-sun axis, though in the opposite direction away from the sun; L3 is located behind the sun, opposite Earth's orbit and always hidden from Earth; and L4 and L5 are located along Earth's orbit but ahead of and behind that orbit, respectively, by about 100 million miles.

Satellites Currently Used for Predicting Space Weather

Several solar monitoring satellites are currently in operation, each with different types of instruments, though they are aging, and none of them was designed for predicting space weather. They include the Solar and Heliospheric Observatory (SOHO), the Advanced Composition Explorer, the Deep Space Climate Observatory (DSCOVR), the Geostationary Operational Environmental Satellite series of weather satellites, and the Solar Terrestrial Relations Observatory (STEREO).

SOHO

A cooperative effort between the European Space Agency and the National Aeronautics and Space Administration (NASA), SOHO carries the only coronagraph located between Earth and the sun. It is therefore one of the most important satellites for monitoring coronal mass ejections. It carries 12 instruments, including the coronagraph, and is in orbit around the L1 Lagrange point. NOAA's Space Weather Prediction Center relies on the coronagraph images from the observatory to detect solar storms that are heading toward Earth. Launched in December 1995 and designed to operate for two years, the satellite has been so successful that its mission has been extended several times. Because the satellite is well past its planned lifetime, it is experiencing age-related problems, including the deterioration of its solar panels, and is projected to lose power by 2026. How much longer it will continue to function is unclear.

Advanced Composition Explorer

NASA designed the Advanced Composition Explorer as a science mission, but the spacecraft has also provided NOAA with data about the solar wind streaming toward Earth past the L1 point, where the satellite is in orbit. It was launched in 1997 and is well past its design life but still in service as a backup to DSCOVR; it is expected to run out of fuel in 2026.

DSCOVR

When functioning, DSCOVR is space weather forecasters' primary source of data about the solar wind and is intended to succeed the Advanced Composition Explorer. It was launched in 2015 with a planned life span of five years.

DSCOVR was not originally intended as a primary source of data for solar weather predictions but is acting as one to provide an interim solution. NASA designed DSCOVR as a low-cost satellite, so it lacks the redundant systems that NOAA needs for reliable continuous operations and is subject to failure if any one critical system fails. Indeed, in June 2019, DSCOVR experienced a malfunction and has been silent since. NOAA has a plan to restart it sometime in 2020 and in the interim has been relying on data from the Advanced Composition Explorer to fill the gap in solar wind measurements.

Geostationary Operational Environmental Satellite Series

NOAA has also placed x-ray and ultraviolet sensors for monitoring space weather on its most recent terrestrial weather satellites, the Geostationary Operational Environmental Satellite-N and -R series, which operate in geostationary orbits that are about 22,000 miles above Earth. The series consists of three satellites in orbit, of which two are in operation and one is a spare. That series is planned to stay in service through the 2030s.

STEREO

NASA's STEREO consists of two satellites, which were launched in 2006: one ahead of Earth in its orbit, the other trailing behind, and each carrying a coronagraph. Providing views from two different perspectives, they were designed to analyze the structure and evolution of solar storms as they travel from the sun, in order to better understand the structure of the sun and its corona. In 2014, the trailing satellite stopped functioning, but the other is still in service, well past its planned lifetime. The European Space Agency has proposed deploying another satellite to trail Earth in its orbit at the L5 Lagrange point, which would also carry a coronagraph that could help provide earlier warning of coronal mass ejections. Although a compact coronagraph at L5 would be a useful complement to a coronagraph at L1 or in geostationary orbit, it would not be a good substitute.

List of Tables and Figures

Tables

Figures

About This Document

This report was prepared in response to a request from the Chairman of the House Committee on Oversight and Government Reform in the 115th Congress. In keeping with the Congressional Budget Office's mandate to provide objective, impartial analysis, the report makes no recommendations.

Ron Gecan, Bernard Kempinski (formerly of CBO), and David Mosher prepared the report with guidance from Terry Dinan, Edward Keating, Joseph Kile, and Chad Shirley. Perry Beider, Sebastien Gay, Kathleen Gramp, Kim Kowalewski (formerly of CBO), and David Torregrosa provided helpful comments. Fritz Hirst of the North American Electric Reliability Corporation, William Murtagh of the National Oceanic and Atmospheric Administration, David Ortiz of the Federal Energy Regulatory Commission, and Adam Rose of the University of Southern California also provided helpful comments. The assistance of external reviewers implies no responsibility for the final product, which rests solely with CBO.

Jeffrey Kling, Wendy Edelberg, and Robert Sunshine reviewed the report, the editor was John Skeen, and the graphics editor was Jorge Salazar. This report is available on CBO's website (www.cbo.gov/publication/56083).

CBO continually seeks feedback to make its work as useful as possible. Please send any comments to communications@cbo.gov.

Phillip L. Swagel
Director
March 2020