



Presidential Policy Directive 21 established national policy on critical infrastructure and resilience in February 2013. The directive defines resilience as the ability to prepare for and adapt to changing conditions and to withstand and recover rapidly from disruptions. Such disruptions include naturally occurring threats or incidents, deliberate attacks, and accidents.

This brief draws from recent GAO reports on natural and human-caused risks to the electricity grid. It also highlights GAO recommendations that had not been implemented as of September 2021.

### Context and Federal Role


The nation’s grid delivers electricity that is essential for modern life. However, the grid faces risks from events that can damage electrical infrastructure (such as power lines) and communications systems, resulting in power outages. These outages can threaten the nation’s economic and national security. They can also disproportionately affect low-income groups, in part because such groups have fewer resources to invest in backup generators and other measures to minimize the impact of outages.

Even though most of the electricity grid is owned and operated by private industry, the federal government plays a key role in enhancing grid resilience.

- The Department of Homeland Security (DHS) is responsible for coordinating the overall federal effort to promote the security and resilience of the nation’s critical infrastructure sectors.
- The Department of Energy (DOE) leads federal efforts to support electricity grid resilience, including research and technology development by national laboratories.
- The Federal Energy Regulatory Commission (FERC) reviews and approves standards developed by the North American Electric Reliability Corporation, the federally designated U.S. electric reliability organization.

### Key Issues

The electricity grid faces multiple risks that can cause widespread power outages.

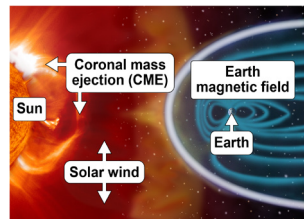
Risk	Example
<b>Extreme weather and climate change</b> 	More frequent and intense extreme weather and other risks due in part to a changing climate, can affect electricity generation, transmission, and distribution. For example, in February 2021, extreme cold weather that spread from the Canadian border as far south as Texas caused record winter demand for electricity and left about 4.5 million customers in Texas, along with about 376,000 customers in Louisiana and Oklahoma, without power. In September 2017, Hurricanes Irma and Maria caused widespread power outages in Puerto Rico and the U.S. Virgin Islands. As a result, the chronically ill often did not have access to electricity to power their medical devices, such as ventilators (see <a href="#">GAO-21-346</a> and <a href="#">GAO-21-274</a> ).

### Cyber- and physical attacks



The electricity grid is vulnerable to cyberattacks, particularly on the systems that control electric power generation, transmission, and distribution. These systems were once isolated from the internet but now are increasingly connected, which poses opportunities for attackers. In March 2019, a cyberattack on an electric utility serving parts of California, Utah, and Wyoming resulted in a communications outage that prevented utility staff from monitoring and controlling the system. A cyberattack could also seek to disable a security system to facilitate a physical attack (e.g., damaging electric grid components) against a utility’s infrastructure (see [GAO-21-81](#), [GAO-19-332](#) and [GAO-11-117](#)).

### Electromagnetic events



Electromagnetic events, which can result from natural phenomena (e.g., geomagnetic disturbances from solar storms) or a weapon that creates an electromagnetic pulse, can disrupt computers and harm electronics. They can also cause significant damage to critical electrical infrastructure, such as transformers, which facilitate the efficient transfer of electric power. For example, in 1989, an extreme solar storm caused wide-scale damage to the Hydro-Quebec power system in Canada. Although such effects are rare, the damage left 6 million customers without power for up to 9 hours (see [GAO-19-98](#), [GAO-18-67](#), and [GAO-16-243](#)).


Sources: Prior GAO work (text); Federal Emergency Management Agency (top image); Song\_about\_summer/stock.adobe.com (second photo from top); National Aeronautics and Space Administration (bottom image). | GAO-21-105403

## Key Opportunities

Agencies have implemented several of GAO's recommendations for improving electricity grid resilience. For example, in March 2016, we recommended that DHS designate roles and responsibilities within the department for addressing electromagnetic risks, which DHS did in 2017. However, as of September 2021, agencies had not yet implemented a number of GAO recommendations that represent key opportunities to mitigate risks in the following areas.

Risk	Key opportunities
<b>Extreme weather and climate change</b> 	<p><b>Prioritize efforts and target resources effectively.</b> DOE should develop a department-wide strategy to enhance the resilience of the grid to climate change, as we recommended in <a href="#">GAO-21-346</a>. Such a strategy could help DOE better prioritize its climate resilience efforts to ensure that resources are targeted effectively.</p> <p><b>Enhance grid resilience efforts.</b> DOE should create (1) a plan to guide development of resilience-planning tools and (2) a mechanism to better inform utilities about grid resilience efforts at its national laboratories, as we recommended in <a href="#">GAO-21-274</a>.</p> <p><b>Better manage climate-related risks.</b> FERC could better manage climate-related risks to the grid by identifying, assessing, and planning for these risks, as we recommended in <a href="#">GAO-21-346</a>.</p>

## Cyberattacks

	<p><b>Assess all cybersecurity risks.</b> DOE should develop a plan to implement the federal cybersecurity strategy, as we recommended in <a href="#">GAO-19-332</a>. The plan, which DOE is now working on, should include a full assessment of all cybersecurity risks to the grid. Such a plan could help guide decision makers in allocating resources to address cybersecurity risks.</p> <p><b>Address risks to distribution systems.</b> DOE should ensure its plans being developed to implement the federal cybersecurity strategy more fully address risks to the grid's distribution systems—which carry electricity to consumers—as we recommended in <a href="#">GAO-21-81</a>.</p> <p><b>Consider changes to current standards.</b> FERC could address current and projected cybersecurity risks, and more fully align its cybersecurity standards with leading practices, by considering changes to its standards, as we recommended in <a href="#">GAO-19-332</a>.</p> <p><b>Evaluate potential risks of a coordinated attack.</b> FERC should evaluate the potential risks to the grid from a coordinated attack on geographically distributed targets, as we recommended in <a href="#">GAO-19-332</a>. Doing so could provide FERC assurance that the approved threshold for mandatory compliance adequately responds to that risk.</p>
---	--

Sources: Prior GAO work (text); Federal Emergency Management Agency (top image); Song\_about\_summer/stock.adobe.com (second image from top). | GAO-21-105403

## GAO SUPPORT

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. This document is based on GAO audit products.

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#). Subscribe to our [RSS Feeds](#) or [Email Updates](#). Listen to our [Podcasts](#). Visit GAO on the web at <https://www.gao.gov>.

Nikki Clowers, Managing Director, Congressional Relations, [ClowersA@gao.gov](mailto:ClowersA@gao.gov), (202) 512-4400

Chuck Young, Managing Director, Public Affairs, [YoungC1@gao.gov](mailto:YoungC1@gao.gov), (202) 512-4800

U.S. Government Accountability Office, 441 G Street NW, Washington, DC 20548

## Key Issues (continued)

In addition to the risks described in the prior page, the electric utility industry faces complex challenges and transformations, including

- aging infrastructure;
- adoption of new technologies, such as information and communication systems to improve the grid's efficiency; and
- a changing mix of power generation.

The traditional model of large, centralized power generators is evolving as retiring generators are replaced with variable wind and solar generators, smaller and more flexible natural gas generators, and nontraditional resources. Such resources include demand-response activities which encourage consumers to reduce their demand for electricity when the cost to generate electricity are high, and various technologies (e.g., solar panels) that generate electricity at or near where it will be used—known as “distributed generation.”

## Selected References

- Zamuda, et al. “Energy Supply, Delivery and Demand.” In *Impacts, Risks, and Adaptation in the United States: Fourth National Climate Assessment*, Vol. 2. Washington, D.C.: United States Global Change Research Program, November 2018.
- National Academies of Sciences, Engineering, and Medicine. *Enhancing the Resilience of the Nation's Electricity System*. July 2017.
- Quadrennial Energy Review Task Force. *Transforming the Nation's Electricity System: The Second Installment of the QER*. January 2017.

For more information about this brief, contact:

Frank Rusco, Director, Natural Resources and Environment, [RuscoF@gao.gov](mailto:RuscoF@gao.gov)

Key Contributors: Janice Ceperich (Assistant Director), Celia Rosario Mendive (Analyst in Charge), Cynthia Norris, and Dan Royer.

Source: ABCDstock/stock.adobe.com (cover image).

**GAO@100**  
A Century of Non-Partisan Fact-Based Work