

Sources	E&E News	Date	May 2021		
Potential scale of impact	★★★★★	Certainty of outcome	★★★★★		
		Impact horizon	H1	H2	H3

The demand for public grid data to spur renewable energy development in the US has raised a challenge: Can utilities and regulators shield sensitive information from hackers while speeding up the transition to clean power?

The U.S. grid is undergoing a shift to digitisation to accommodate millions of smart technologies but cybersecurity experts are warning that the wave of accompanying data — including publicly available tools renewable developers use to find project sites — can also be abused by hackers looking for vulnerabilities in the grid.

[A recent report](#) by the National Association of Regulatory Utility Commissioners noted that distribution utilities are struggling with the notion that potentially millions of consumer-based devices will be linking up with the grid.

"The growing connectivity between the grid and customer devices increases cybersecurity vulnerabilities and broadens the threat landscape by expanding the number of potential entry points through which malicious cyberattacks can be launched," the report said.

Meanwhile, the Government Accountability Office warned that the increasing cyberthreats to distribution energy companies are not being adequately addressed by the federal government.

The government watchdog said that the increasing digitalisation and reliance on monitoring technologies and internet-facing consumer devices can open additional weak points that can be used to attack the grid. Additionally, the vulnerabilities "are compounded for distribution systems because the sheer size and dispersed nature of the systems present a large attack surface."

