The Cybersecurity Challenge

As the use of solar and other DER expands, the electric grid is increasingly comprised of independently owned, interconnected cyber-physical devices that rely on two-way data communications and power flows to operate safely and reliably.**The inherently sophisticated communications capabilities built into each of those devices expose potential cyber security vulnerabilities.For example, to perform their grid-enabled functions, smart inverters communicate with DER aggregators and utility operators, typically over the internet.**A cyberattack aimed at disrupting or manipulating DER communications at any point along the communications path could affect electricity delivery on the grid.9 **Similarly, software vulnerabilities could allow malicious actors to gain access to a smart inverter and change settings that affect the voltage or electrical current delivered to the grid.With the increasing prevalence of DER devices, common-mode vulnerabilities run the risk of simultaneously disconnecting massive quantities of generation, which could lead to power disruption**.10

Although updating is underway, **current versions of IEEE 1547-2018 and CA Rule 21 offer little guidance on cybersecurity, opting to focus on operational and interoperability requirements instead.Nonetheless, the security of the electric grid now and in the future remains a high priority for utilities, the solar industry, and state and federal agencies alike.The desired end state, suggest researchers from Sandia National Laboratory, is one where grid operators, PV owners, and aggregators communicate with interoperable, secure-by-design systems using safe, resilient networks with high availability, data integrity, and confidentiality**.11 Standards alone, however, may not be enough to achieve this end state amid rapidly evolving technology advances and increasingly sophisticated cyber threats.