**Roadmap to Achieve Solar Cybersecurity**

**Introduction**

* Solar energy technologies can be vulnerable to cyberattack through inverters and control devices that are designed to help manage the electric power grid. Operating-technology (OT) devices like solar photovoltaic inverters, when connected to the Internet, are at higher risk relative to stand-alone OT devices. They must be able to prevent, detect, and respond to unauthorized access or attack.
* social engineering is a type of manipulative, fraudulent practice and failure to recognize such deceptions is the entry point into many systems.
* A cyberattack on a cyber-physical system is different from one on an enterprise IT system. Cyber-physical systems are engineered systems that are built from, and depend upon, the seamless integration of computation and physical components.

**Background**

Cybersecurity is the protection of interconnected electric power systems from digital attacks. Solar is one of the many electric generation technologies used on the grid, contributing to large-scale generation in the form of solar farms and utility-scale installations, as well as small-scale distributed energy resource (DER) generation in the form of rooftop installations.

In 2017, SETO funded Sandia National Laboratory’s [Roadmap for Solar Cybersecurity](https://www.researchgate.net/publication/322568290_Roadmap_for_Photovoltaic_Cyber_Security), which helps to guide research in this area in SETO and other DOE offices. In 2020, DOE Energy Efficiency and Renewable Energy (EERE) Office published a [Multi-Year Program Plan](https://www.energy.gov/eere/articles/doe-releases-plan-improving-cybersecurity-renewable-energy-manufacturing-buildings-and) that includes strategies to improve cybersecurity in renewable energy, manufacturing, buildings, and transportation research and development.

* [Solar Energy Technologies Office Lab Call FY2022-24](https://www.energy.gov/eere/solar/solar-energy-technologies-office-lab-call-fy2022-24-systems-integration)

in this lab, they Secure Solar for the Grid project

* [Solar Energy Technologies Office Fiscal Year 2019](https://www.energy.gov/eere/solar/seto-fy2019-advanced-solar-systems-integration-technologies)

They create strategic plans and decision-making tools for enhancing cybersecurity solutions and developing technologies that protect power electronic devices from cyberattacks

* [Solar Energy Technologies Office Lab Call FY19-21](https://www.energy.gov/eere/solar/solar-energy-technologies-office-lab-call-fy2019-21-systems-integration)

they improve analysis of grid integration challenges to allow the solar industry to develop new tools

* [Enabling Extreme Real-time Grid Integration of Solar Energy](https://www.energy.gov/eere/solar/enabling-extreme-real-time-grid-integration-solar-energy-energise)

They fund programs to develop distribution planning and managing of distributed sources, like solar, onto the grid.

* [Advanced Systems Integration for Solar Technologies](https://www.energy.gov/eere/solar/advanced-systems-integration-solar-technologies-assist-situational-awareness-and)

They fund programs to improve situational awareness of solar energy systems

**Technology Gaps /drivers/Chalenges**

* Cyber-incidents will continue to increase in sophistication and number
* Effective cybersecurity practices are difficult to establish, maintain, and trace:

construction ⇒ repowering ⇒ decommissioning

* solar energy technologies and deployments are highly diverse
* Limited number of established cybersecurity standards specific to solar energy
* practical and available cybersecurity options may be costly
* Information sharing is limited among solar energy stakeholders
* Lack of solar-specific cybersecurity services, products, and strategies
* Stakeholders have few incentives for Prioritizing the cyber security

**Objectives**

* Release the Roadmap for Solar System Cybersecurity, which will motivate the need for Solar energy cybersecurity through technology and threat analysis
* Contextualize the roadmap within national energy cybersecurity efforts
* Provide recommendations for improving solar cybersecurity

**Methodology/ Strategies**

* Develop solar system Cyber-Culture

Promote cybersecurity culture and information sharing among solar energy community

* Identify and Protect

Managing cybersecurity risk to solar assets, data, and grid infrastructure and developing cyber-safeguards regarding delivery of solar energy

* Detect

identifying malicious or unintentional cybersecurity events impacting solar technologies and networks

* Respond and Recover

**References**

[**https://www.energy.gov/eere/solar/solar-cybersecurity-basics**](https://www.energy.gov/eere/solar/solar-cybersecurity-basics)

[**https://www.osti.gov/biblio/1402553**](https://www.osti.gov/biblio/1402553)

[**https://www.energy.gov/sites/default/files/2021-10/fy21peerreview-gridintegration-inl-gentle2.pdf**](https://www.energy.gov/sites/default/files/2021-10/fy21peerreview-gridintegration-inl-gentle2.pdf)

[**https://www.energy.gov/eere/solar/solar-cybersecurity**](https://www.energy.gov/eere/solar/solar-cybersecurity)