

# GRID MODERNIZATION

## Security and Resilience—Overview

Recent weather events, physical attacks, and cyberattacks on the nation's electrical grid have led to Presidential Policy Directives and an Executive Order to secure the grid.

The “Security and Resilience” focus area has five main activities, based on the NIST cybersecurity framework, that are in alignment with DOE strategies in the Infrastructure Security and Restoration Program and the Cybersecurity for the Energy Delivery Systems Program. Each activity has specific goals and target achievements to be completed by 2020.



### ***Activity 1: Improve the Ability to Identify Threats and Hazards***

**Goal:** Anticipate threats and hazards to the grid, while gaining an understanding of the vulnerabilities to all hazards, as well as their potential consequences.

#### **Target achievements:**

- Expand the existing cybersecurity model (C2M2) to anticipate threats and include all hazards, such as physical hazards, and perform on-site pilot assessments.
- Create enhanced sensors for information-sharing devices in the Cybersecurity Risk Information Sharing Program and create a security data repository.

### ***Activity 2: Increase the Ability to Protect Against Threats and Hazards***

**Goal:** Provide effective protection and resilience of the grid by developing standards for analyzing component and system resilience, creating and disseminating tools for resilient planning, hardening components against attacks, and instituting an inherently resilient communications system.

#### **Target achievements:**

- Develop standards, methods, testing, and evaluation procedures for grid designs that are resilient to physical and cybersecurity attacks.
- Develop and demonstrate communications for emerging energy technologies, as well as control system models and logistical optimization techniques to minimize outage durations.
- Develop grid components that are inherently protective of grid services during any hazardous event.

### ***Activity 3: Increase the Ability to Detect Potential Threats and Hazards***

**Goal:** Proactively call out system vulnerabilities or attacks by applying system status characterization, machine learning, and high-throughput analytics for the entire grid lifecycle,

from planning and design to operations. Also address the human cognitive components of responding to threats identified through such a process.

**Target achievements:**

- Build modeling and simulation capabilities to approximate the operating profiles of grid operations from a cyber and physical security standpoint for the full system lifecycle.
- Develop real-time cyber and physical data analytics and cognitive learning across the grid system lifecycle and demonstrate the ability to detect potential threats in two regional exercises.



**Activity 4: Improve the Ability to Respond to Incidents**

**Goal:** Improve the power grid’s ability to predict, respond, and adapt to all hazards and threats by developing methodologies and frameworks that assess system degradation, advance utility preparations based on predictions, and transform the grid to keep operating during hazardous events.

**Target achievements:**

- Develop and deploy prototypes that assess infrastructure degradation, identify cyber and physical attacks, and adapt the behavior of grid technologies to maintain critical grid operations.
- Develop methodologies and frameworks that provide diverse attack recognition and a mixed response on multiple timescales, optimizing the operational priorities to reduce the grid’s response time.

**Activity 5: Improve the Grid’s Recovery Capacity and Time**

**Goal:** Maintain plans for grid resilience and the restoration of electric sector capabilities and services following an all-hazards event.

**Target achievements:**

- Develop designs and standards for advanced substations, transformers, and support technologies that facilitate improved portability and rapid recovery from natural disasters.
- Develop hardened, fail-safe, wireless communications for grid control systems that resist cybersecurity attacks and electromagnetic disturbances.