# Security and Resilience

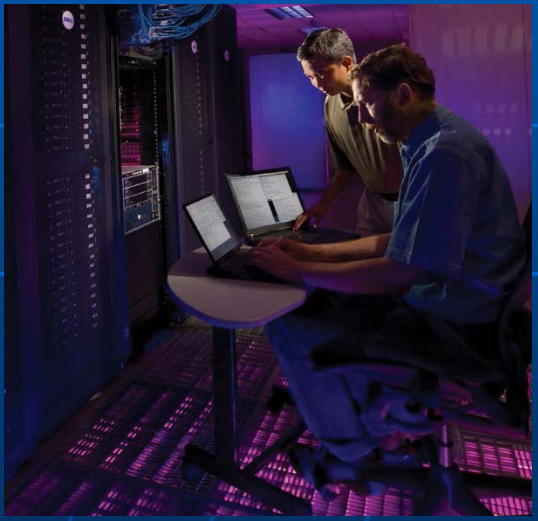
Juan Torres, SNL

April 21, 2016

# Overview

The "Security and Resilience" focus area has five main activities, based on the NIST cybersecurity framework, but expanded to all-hazards.

- Improve the Ability to **Identify** Threats and Hazards
- Increase the Ability to **Protect** Against Threats and Hazards
- Increase the Ability to **Detect** Potential Threats and Hazards
- Improve the Ability to **Respond** to Incidents
- Improve the Grid's **Recovery** Capacity and Time



# New Jersey TransitGrid

Sandia National Laboratories BPU NJTRANSIT The Way To Go.

## CHALLENGE ADDRESSED

Major tropical storms pose a high risk to east coast critical infrastructure, impacting the economy and safe transport of the population.

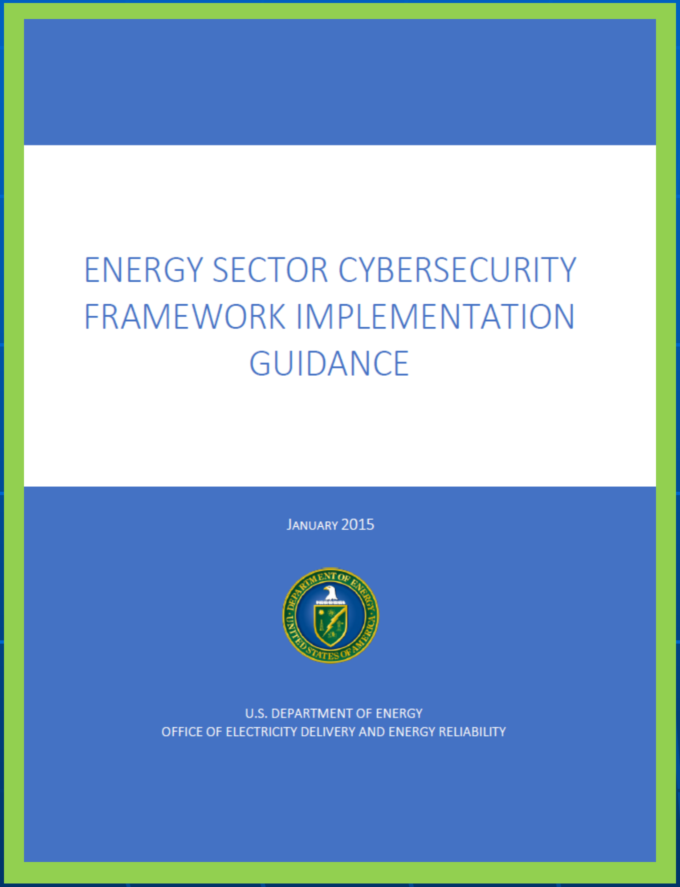
## R&D STRATEGY

Develop a resilient transportation microgrid (NJ TransitGrid) capable of providing power during a grid outage.

## IMPACT

When completed, the NJ TransitGrid will generate more than 100 MW to service critical transportation assets operated by the NJ Transit Corporation and Amtrak. It will also supply energy and ancillary services to the grid during normal conditions and provide enhanced energy resilience during localized or regional grid outages.

# Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)



ENERGY SECTOR CYBERSECURITY FRAMEWORK IMPLEMENTATION GUIDANCE

January 2015

U.S. DEPARTMENT OF ENERGY
OFFICE OF ELECTRICITY DELIVERY AND ENERGY RELIABILITY

## CHALLENGE ADDRESSED

There is a need to improve electricity subsector cybersecurity capabilities and to understand cybersecurity posture.

## STRATEGY

Provide a mechanism to evaluate, prioritize, and improve cybersecurity capabilities using the NIST Cybersecurity Framework.

## IMPACT

- Provides a common set of industry-vetted cybersecurity practices.
- Allows organizations to evaluate their cybersecurity practices against industry’s.
- Scores compared with each organization’s desired risk tolerance.

# Artificial Diversity and Defense Security (ADDSec)

Sandia National Laboratories · Lawrence Livermore National Laboratory · Washington Gas Energy Systems · Chevron · GRIMM · Ft. Belvoir / Night Vision & Electronic Sensors · SEL Schweitzer Engineering Laboratories

## Extend Software Defined Networking (SDN)

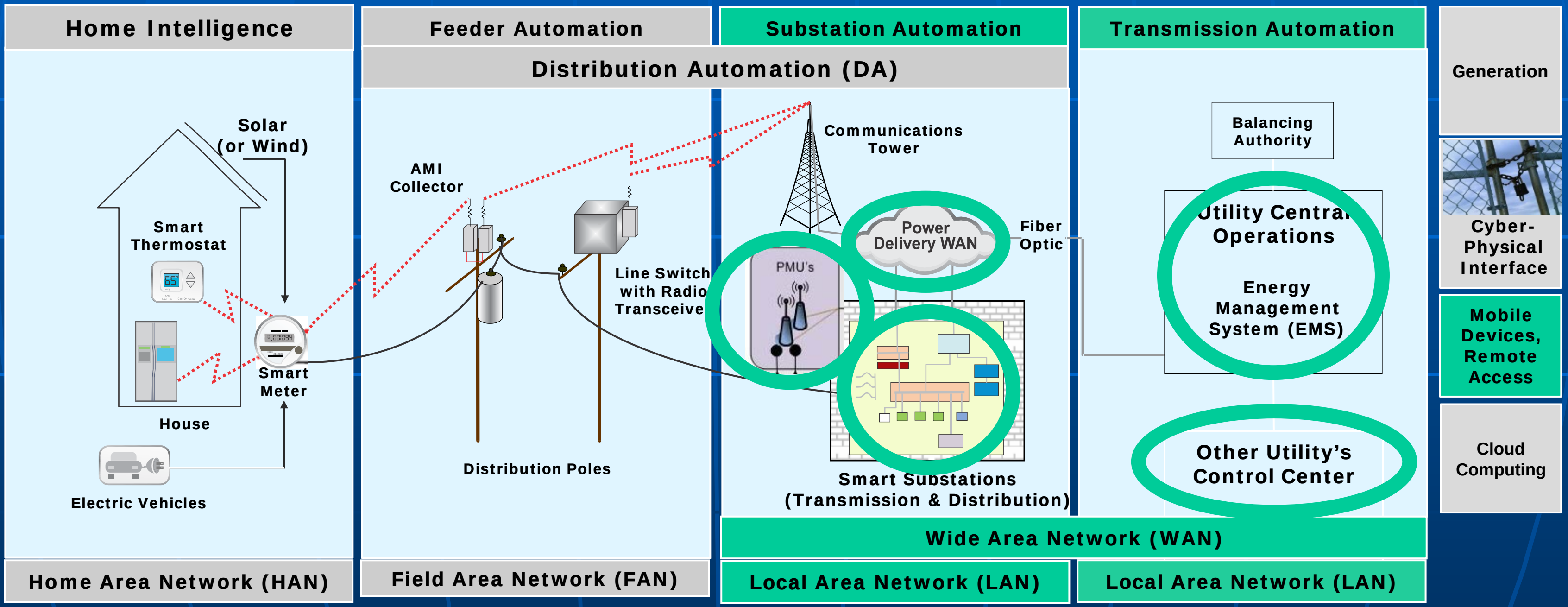
- Research the extension of SDN from the local area network to wide area networks
- Enable network randomization transparency to end devices within an SDN setting to yield a scalable solution

## Moving target security architecture

- Develops a framework to automatically detect and defend control systems
- Converts static control systems into moving targets

## Applicable to existing and future energy delivery systems

- Provides improved situational awareness
- Addresses NERC CIP-007-5 R3 (Malicious Code Prevention), R4 (Security Event Monitoring), CIP-008-5 R1 (Cyber Security Incident Response)



# Future Work

- 1.3.4 - Industrial Microgrid Analysis and Design for Energy Security and Resiliency (ORNL, SNL)
- 1.3.11 - Grid Analysis and Design for Energy and Infrastructure Resiliency for New Orleans (SNL, LANL)
- 1.4.23 - Threat Detection and Response with Data Analytics (LLNL, LBNL, INL, ORNL, PNNL, SNL)