Resilience in System Planning

Mark Sims
Manager, Transmission Planning
Planning Committee
September 14, 2017
Resilience - Planning

• Resilience Criteria – Range of Possibilities
  – Do “no harm” (i.e. don’t make an existing problem worse)
  – Opportunistic – incorporate resilience as a factor in RTEP proposal selections
  – Standalone - address resilience as a stand-alone driver

• Resilience Criteria would require new analytical procedures and tools
  – Assess Vulnerabilities
  – Develop Resilience Indices
• Selection and Development of Events
  – NERC TPL-001-4
    • Wide area events
    • Mode of failure / modeling
    • Loss of all lines in a ROW
    • Loss of a substation
    • Loss of two generating stations
    • Severe weather
    • Successful cyber attach
    • Shutdown of nuclear power plant(s)
    • Gas/Electric Interface
• Selection and Development of Events
  – CIP-014-1
    • Assume physical attack
    • Previous targeted events
    • Mode of failure
    • Solution approaches and alternatives

CIP-014-1 — Physical Security

A. Introduction
1. Title: Physical Security
2. Number: CIP-014-1
3. Purpose: To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.
Resilience - Planning

- Sensitivity of Information
- FERC Critical Energy/Electric Infrastructure Information (CEII)
- Sensitivity of Events
- Sensitivity of Consequences
- Sensitivity of Solution Implementation


I. CEII Defined
CEII is defined as information related to or proposed to critical electric infrastructure,
- generated by or provided to the Commission or other Federal agency other than classified national security information,
- that is designated as critical electric infrastructure information by the Commission or the Secretary of the Department of Energy pursuant to section 215A(d) of the Federal Power Act.

CEII is specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure (physical or virtual) that:
1. Relates details about the production, generation, transmission, or distribution of energy;
2. Could be useful to a person planning an attack on critical infrastructure;
3. Is exempt from mandatory disclosure under the Freedom of Information Act; and
4. Gives strategic information beyond the location of the critical infrastructure.

Critical energy/electric infrastructure means a system or asset of the bulk-power system, (physical or virtual) the incapacity or destruction of which would negatively affect:
- national security,
- economic security,
- public health or safety, or
- any combination of such matters.

www.pjm.com
Resilience - Planning

• Resilience Challenges and Next Steps
  – RTEP Approval and Inclusion
    • Transparency & Stakeholder Communication
  – Siting given States historic preferences
  – Cost and cost allocation