Physical Security Analysis of Substations

Carl Herron, Senior Manager Physical Security Analyst
NPCC Fall Workshop
November 8, 2017 Hartford Connecticut
• Substation Review
• Vulnerabilities and characteristics
• Security Countermeasures Implementation
• Case Studies – Threats
• Strategic Security Initiatives
Substations Review

- Initial CIP-014-02 Outreach NERC and Regions
- OE-417 Electric Disturbance Event Reports
- EOP-004 Event Report Forms
- Regional Physical Security Working Groups
- Physical Security Advisory Group
- Assistance Visits
Vulnerabilities Consideration

- Security gaps physical/human
- Budget
- Subject Matter Expertise
- Policy and procedures
- Substation Design
- Geographic challenges
- Property Maintenance
Geographic Challenges
Vulnerabilities Consideration

Substation design
Vulnerabilities Consideration

Substation Maintenance
Physical Security Characteristics

• Common physical security characteristics observed:
  - Substations located near or adjacent to other sectors (i.e., natural gas pipelines)
  - Substations located in high crime areas
  - Substations located in remote rural areas with limited law enforcement support
  - Geographical challenges in implementing physical security measures
  - Support of other critical infrastructure or national assets
  - Proximity of the facility to unique threats
  - Proximity of roadways and highways for easy vehicular access and egress
  - Multiple transmission lines entering into a substation
  - Substation located close to other substations not owned by critical substation owner
Some of the security countermeasures being implemented:

- Intrusion detection systems
- Video surveillance and analytics
- Thermal cameras
- Anti-climb/anti-cut fencing
- Ballistic resistant fencing
- Ballistic panels or walls
- Electronic Key/Management
- Additional lighting
- Vehicle barriers/bollards/crash gates
- Use of natural environment
- Gun shot detection
• Security Plans should address identified threats and vulnerabilities
• Two-part plan - security response and security measures
• Detection and response
Bolt Removal Incidents

- One incident in the United States.
- Two incidents in Canada.
- One group has implied credit for one of the incidents.
- All incidents are currently under investigation.
- Conference call between the two Entities.
Bolt Removal Incidents

- Citizen discovered bolts, reported to environmental education center who then reported to Utility.
- Two towers affected. One tower (closest to roadway) had approximately 36 bolts and 2 splice plates missing. The second tower had approximately 60 bolts removed and 4 splice plates missing.
- Significant effort was required to remove the bolts as they were torqued to 60 pounds.
- Weeds and brush were growing through the holes.
- Some of the missing bolts were found in the surrounding area.
Bolt Removal Incidents

Tower 5-5

Tower 5-6
Bolt Removal Incidents
• September 12, 2016 Humboldt County

• September 25, 2016 Garkane Energy Utah

• September 29, 2016 Mt. Wheeler Power
Escalante man accused of shooting at substation, knocking out power faces federal charges

By McKenzie Romero | Posted Feb 16th, 2017 @ 4:16pm

SALT LAKE CITY — A federal grand jury handed down an indictment Wednesday for an Escalante man accused of shooting at a southern Utah substation, knocking out power to two counties.
• April 2017, DGR has implied that the Metcalf incident was a sophisticated assault an example of the groups strategy of Decisive Ecological Warfare.

• May 2017, DGR reposted the Garkane incident stating that targeting infrastructure is an effective tactic and an effective means of resistance.

• August 2017, DGR tweeted about the Metcalf incident
New group will be responsible for managing emerging security risks, coordinating security efforts between NERC business units, the EISAC and industry.
Strategic Security Initiatives

- CIP 2025 Plan
- Security Metrics
- Supply Chain
- Mexico
- Cloud
- CIP Website
- CIPC
- UAS/Drones
- Insider Threat Programs
- Key Management
Questions and Answers