Low Impact BES Cyber Systems
Implementation and Issues

2017 MIPSYCON
Michael Brytowski - Great River Energy

November 7, 2017
Talking Points

- About Great River Energy
- Quick CIP Time-line
- Low Impact BES at GRE
  - Plans
  - Identify facilities
  - Physical Security
  - Cyber Security
  - Time-Line
  - Shared Facilities
- Wrapping it all up
About Great River Energy

- 28 member cooperatives – 665,000 member accounts
- 4th largest G&T in the U.S.
  - $4 billion total assets
  - $1 billion revenue
- 940 employees (MN & ND)
- 8 Generator Stations
  - 710 MW renewables
- 4,771 miles transmission
Cyber Security Standards (CIP)

- November 2013: FERC Approves Version 5 CIP Standards (FERC Order 706)
- June 2016: FERC Approves Version 6 CIP Standards (FERC Order 791)
- July 2016: CIP effective date for High & Medium BES Assets
- April 2017: Medium Transient assets & Low Impact BES Plans due.
- September 2018: Low Impact Implementation
### Bulk Electric System Classification

<table>
<thead>
<tr>
<th>High Impact</th>
<th>Medium Impact</th>
<th>Low Impact</th>
<th>No Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Large control centers</td>
<td>Critical substations and generation sites</td>
<td>Remaining sites with a BES Cyber System (≥ 100 kV)</td>
<td>Sites without a BES Cyber System</td>
</tr>
<tr>
<td>2 Facilities</td>
<td>2 Facilities</td>
<td>88 transmission sites 8 generation sites</td>
<td>Remaining sites without a BES Cyber System</td>
</tr>
</tbody>
</table>

All BES Facilities are to be considered for inclusion into CIP!
Security Management Controls

- Cyber Security Awareness
- Physical Security Controls
- Electronic Access Controls
- Cyber Security Incident Response
Keep It Simple
Integrated into already existing CIP Policies, Plans and Procedures
Cyber Awareness & Incident Response

- Integrated into current Cyber Awareness program
- Posters at substations
  - Generation Stations
  - Switching stations
- Email to utility partners
- Included in contractor safety briefing
Physical Security

- Surveyed surrounding entities
- Low Impact Asset Physical Security Plan V1.0
  - Attachment 1, Section 2
    - Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity
  - Physical Security Controls
    - GRE will control access to their Low Impact assets or the locations of the low impact BES Cyber Systems within the assets using controls to prevent unauthorized access in a manner that is commensurate with the classification of those assets.
Physical Security

Where to control access?
What about stuff in the yard?
IT infrastructure limitations

Deterrence strategies
• Signage - Who to call
• Motion lighting
• Door contact alarm
• Vegetation management
• “High security” locks with strict key control
• Minimal IT comm support
• Low cost
Physical Security Implementation

- **Type of Security?**
  - Keys
  - Card access
  - Combination locks

- **Re-key all substation buildings**
  - Assa Abloy Protec2 Key System
  - $100 per site plus labor
  - Total Cost ~$50,000
Electronic Security Controls

- Electronic Security Perimeters V 4.0
  - Integrated Low Impact into existing document
  - Low-impact BES Transmission facilities connect to the larger GRE network via a centralized firewall at a datacenter location.
Electronic security controls
# Timeline

<table>
<thead>
<tr>
<th>Milestone</th>
<th>Task</th>
<th>Completion Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Initial wave of remotely accessible devices put in service in CrossBow.</td>
<td>Sept. 2017</td>
</tr>
<tr>
<td>2</td>
<td>Final wave of remotely accessible devices put in service in CrossBow.</td>
<td>Spring 2018</td>
</tr>
<tr>
<td>3</td>
<td>Decommission Relay Call Up.</td>
<td>Spring 2018</td>
</tr>
<tr>
<td>4</td>
<td>Move communications for low impact sites over to the Ops Network, put access lists on routers and set firewall rules.</td>
<td>Spring 2018</td>
</tr>
<tr>
<td>5</td>
<td>Install new key cylinders at low impact sites and badge readers at sites $\geq$ 300kV.</td>
<td>Summer 2018</td>
</tr>
</tbody>
</table>

All low impact sites must be fully compliant by Sept. 1, 2018
Key impacts

- **Cyber security awareness**
  - Receive quarterly security awareness emails
  - Security awareness [posters](#) at low impact sites

- **Incident response**
  - Low impact sites have formally been added to our Incident Response Plan.
  - If you see something, say something.

- **Electronic security controls**
  - Interactive remote access for **ALL** sites will be through CrossBow.
  - Relay Call Up will be decommissioned.

- **Physical security controls**
  - New high security keys for low impact control houses and cabinets
  - Badge readers on control houses for low impact sites $\geq$ 300kV
Shared Facilities

GRE Cooperatives – 28!
Issues – Shared Facilities

- Who is responsible?
  - The Entity with the BES Cyber Asset

- Site Ownership
  - Controlling physical access
  - Electronic access

- Who has control of the BES asset?
  - Other entity has control
  - Dual control

- Compliance!
MRO Position on shared facility agreements:

- Any agreement between multiple entities can describe shared responsibility for shared facilities, and can be used to support an entity’s position regarding compliance responsibility. In the case of a noncompliance or possible violation, MRO may use the agreement as a basis to determine responsibility, but MRO will not preemptively interpret agreements and is not responsible for enforcing these agreements.

- In general, if a noncompliance has been discovered, responsibility for the noncompliance is generally assigned to the entity responsible for the BES Cyber System. However, there are scenarios where a noncompliance caused by one entity may become a noncompliance for all entities that are associated with a given shared facility.

  — MRO Low Impact Workshop 3/1/17
Memorandum of Understanding (MOU)

An MOU is not a NERC-specific document, but more of a document that can be crafted and agreed upon between two different entities to state what responsibilities will be shared between them (Section 3.5.3 CEIWG* draft)

Ask yourself three questions...
- What needs to be protected?
- Who is responsible?
- How is responsibility documented?
Suggested Elements of an MOU

- Preferred tool for shared facilities
- Positive identification of all Cyber Assets
- Identification of all routable connectivity (LEAPs)
- Identification of physical access responsibility
- Understanding and agreement of cooperation during audits
- Agreement on responsibility for fines for any enforcement actions taken by the ERO
- Inclusion of, or access to, Cyber Incident Response Plans
- Cyber Awareness that includes notifying other entities
- Non-disclosure agreement
Wrap it up

- Keep It Simple
  - Plans
  - Integrate into existing plans & policies

- Shared Facilities
  - What needs to be protected
  - Who is responsible
  - How is responsibility documented

- September 1, 2018 is coming fast!
Discussion and Questions
Contacts

- Michael Brytowski - Compliance
  - mbrytowski@grenergy.com
  - 763-445-5961

- Richard Fitzpatrick – CIP-003 Lead Engineer
  - rfitzpatrick@grenergy.com
  - 763-445-5974

- Mark Lucas – Manager Facilities Services
  - mluucas@grenergy.com
  - 763-445-5407
Resources

- NERC CIP Standards
- Standard Application Guide CIP-003-6 R2 (MRO)
- MOU Template (draft) - CEIWG
- MRO Shared Facilities and Mixed Ownership of Cyber Assets - (3/1/17 CIP workshop)