

Low Impact BES Cyber Systems Implementation and Issues

2017 MIPSYCON

Michael Brytowski - Great River Energy



November 7, 2017

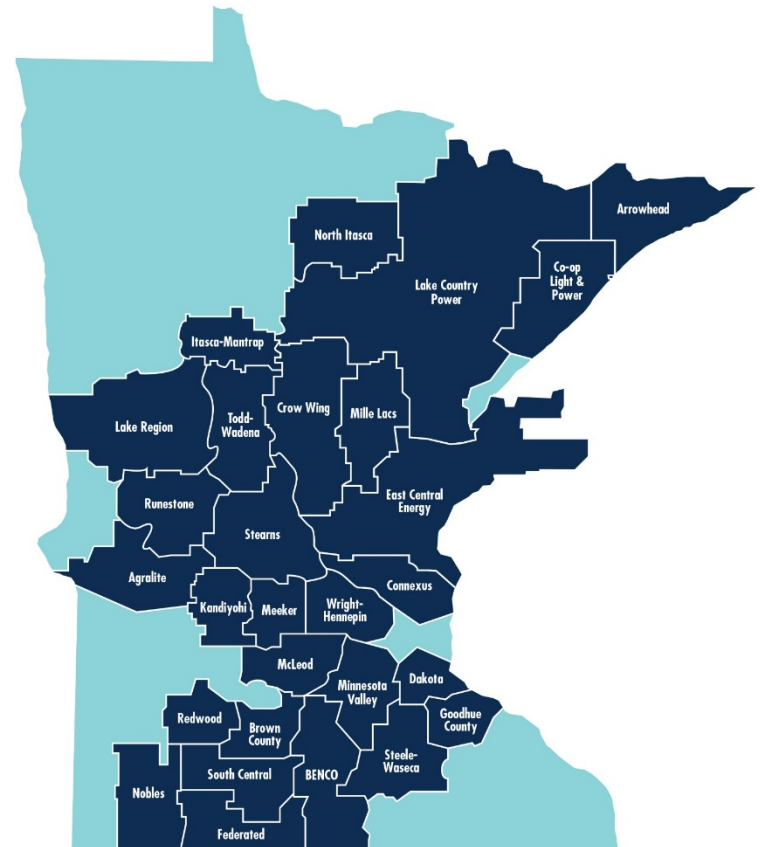
Talking Points

- ▶ 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

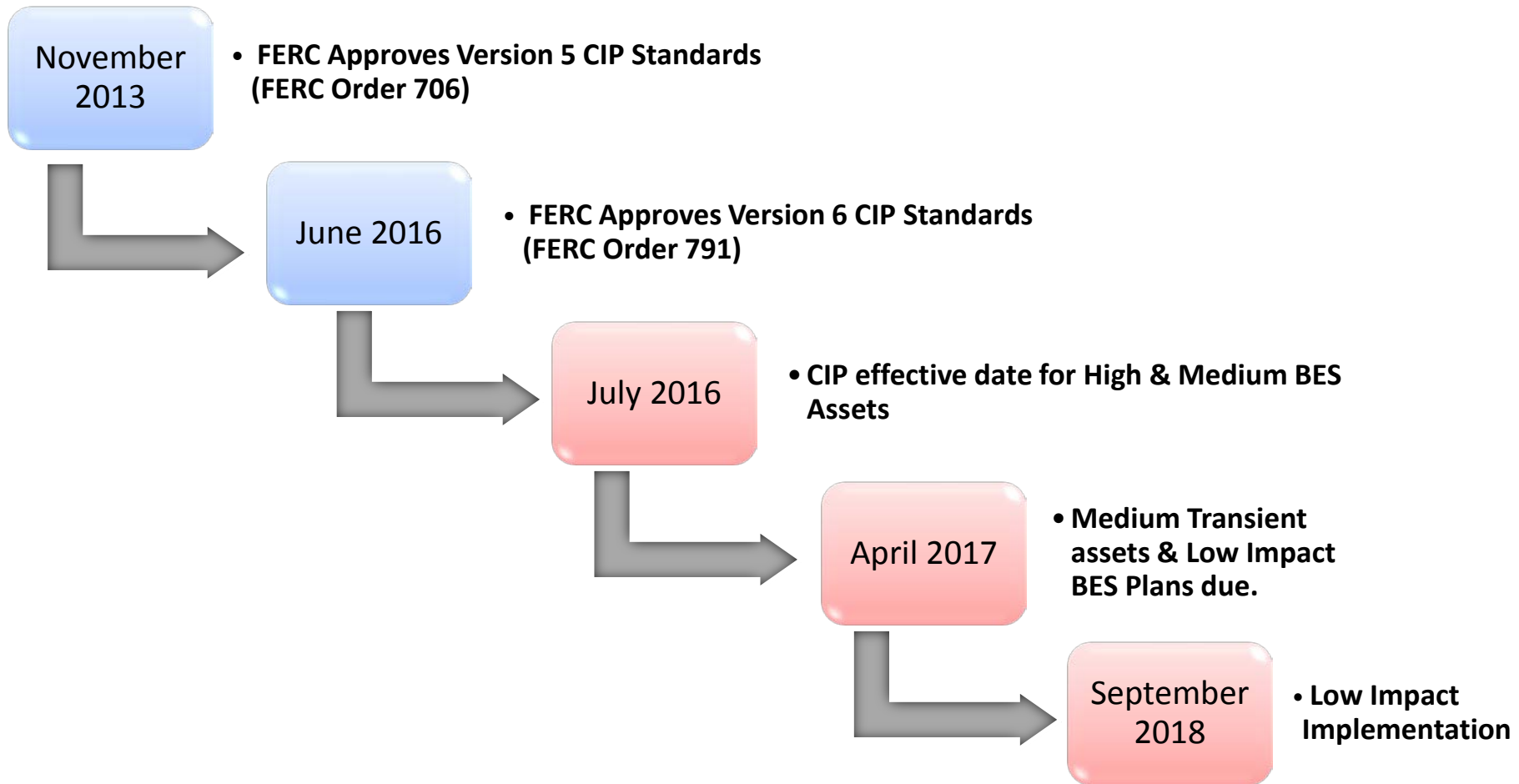


About Great River Energy



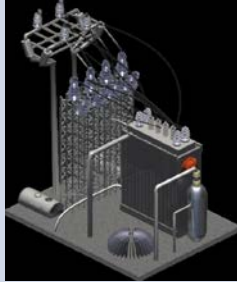
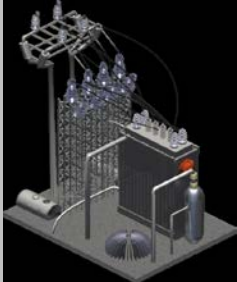
- ▶ 28 member cooperatives – 665,000 member accounts
- ▶ 4th largest G&T in the U.S.
 - \$4 billion total assets
 - \$1 billion revenue
- ▶ 940 employees (MN & ND)
- ▶ 8 Generator Stations
 - 710 MW renewables
- ▶ 4,771 miles transmission



Cyber Security Standards (CIP)



Bulk Electric System Classification

High Impact	Medium Impact	Low Impact	No Impact
<p data-bbox="112 425 372 518">Large control centers</p>  <p data-bbox="208 996 411 1032">2 Facilities</p>	<p data-bbox="537 425 913 575">Critical substations and generation sites</p>  <p data-bbox="633 996 836 1032">2 Facilities</p>	<p data-bbox="967 425 1319 575">Remaining sites with a BES Cyber System (≥ 100 kV)</p>  <p data-bbox="987 996 1338 1089">88 transmission 8 generation sites</p>	<p data-bbox="1392 425 1769 518">Sites without a BES Cyber System</p>  <p data-bbox="1431 996 1744 1146">Remaining sites without a BES Cyber System</p>

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



GRE Low Impact BES Plans

- ▶ Low Impact Cyber Security Plan V 1.0
 - Due April 1, 2017
 - Addresses the four security management controls

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

Bulk Power System Security

Great River Energy believes in a culture of security to complement our already-strong culture of safety for our employees and contract workers. You play a key role in protecting our part of this nation's critical electricity infrastructure, and your diligence is appreciated.

Security policy statements

- GRE will be compliant to all NERC cybersecurity and physical security requirements
- All GRE bulk electric system facilities are designated 'in-scope' for NERC cybersecurity and physical security requirements
- Security policy exceptions must be reported to a supervisor immediately

Cybersecurity

- Personnel may be required to comply with certain elevated procedures for electronic access
- Sharing of personal credentials is forbidden
- Certain information related to bulk electric system configurations cannot be shared with third-parties

Physical security

- Personnel may be required to comply with certain elevated procedures for physical access
- Visitor access controls are in place for all designated bulk electric system facilities
- See your supervisor for site-specific security protocols

Incident response

- All incidents (cyber or physical) shall be reported
- See your supervisor for site-specific security protocols
- Report physical incidents to the GRE Security Hotline at 763-241-2222
- Report suspected cybersecurity incidents to the GRE Service Desk at 763-241-2252



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

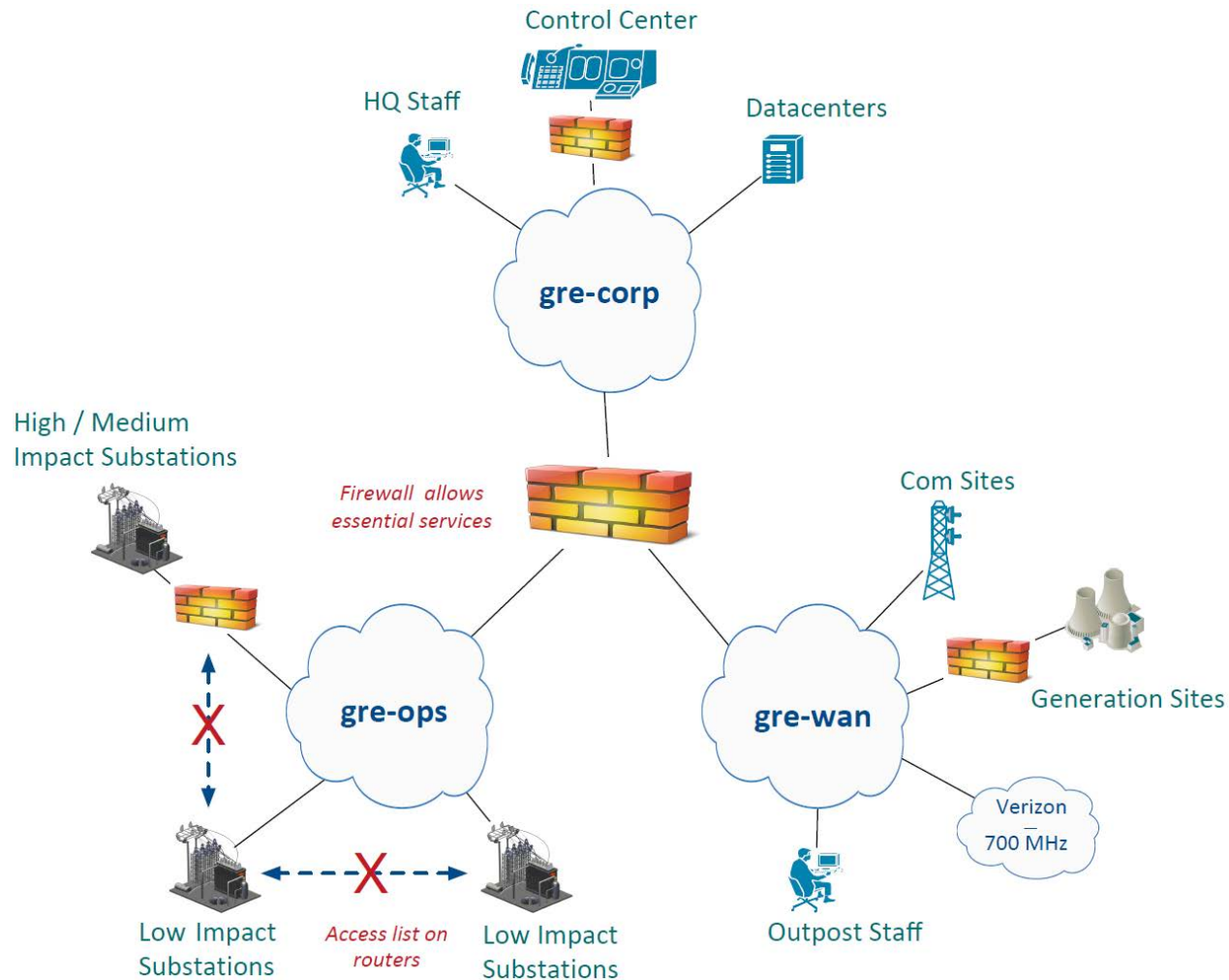


Electronic Security Controls

- ▶ 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

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

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 $\geq 300\text{kV}$

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!



Shared Facility Agreements

- ▶ 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@greenergy.com
 - 763-445-5961
- ▶ Richard Fitzpatrick – CIP-003 Lead Engineer
 - rfitzpatrick@greenergy.com
 - 763-445-5974
- ▶ Mark Lucas – Manager Facilities Services
 - mlucas@greenergy.com
 - 763-445-5407

Resources

- ▶ NERC CIP Standards
- ▶ Standard Application Guide CIP-003-6 R2 (MRO)
 - <https://www.midwestreliability.org/MRODocuments/CIP%20003-6%20R2%20Standard%20Application%20Guide.pdf>
- ▶ Critical Infrastructure Protection Committee Guidance Document – Shared Facilities, (Draft 3/30/17), Compliance Enforcement and Input Working Group (CEIWG)
- ▶ MOU Template (draft) - CEIWG
- ▶ MRO Shared Facilities and Mixed Ownership of Cyber Assets - (3/1/17 CIP workshop)