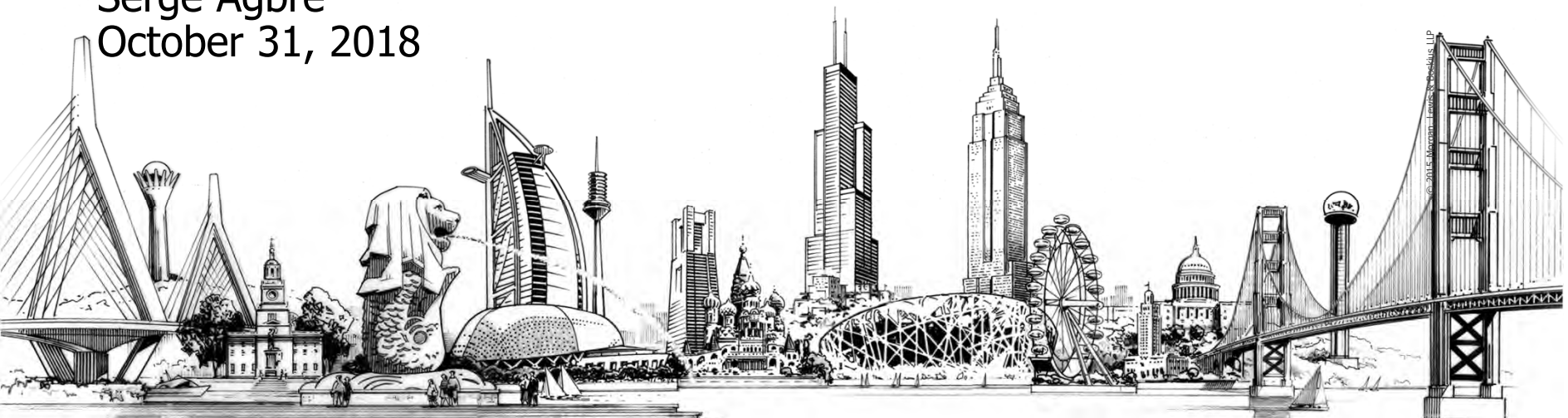
Morgan Lewis

PROPOSED CIP STANDARD FOR CONTROL CENTER COMMUNICATIONS, RELIABILITY STANDARD CIP-012-1

J. Daniel Skees
Arjun Ramadevanahalli
Serge Agbre
October 31, 2018



Agenda

- Need for Reforms
- Overview of Standard
- Challenges to Implementation
- Questions

NEED FOR REFORMS

FERC Directive

- FERC order adopting Version 6 standards (Order No. 822) highlighted risk to communication links and data communicated between BES Control Centers
  - FERC found that there was a reliability gap in CIP-006-6 (Physical Security of BES Cyber Systems)
- Directed NERC to develop modifications to the CIP Standards to protect those communication links and sensitive data
- Controls should:
  - Be commensurate with the risks posed by the protected assets (*i.e.*, impact rating under CIP-002-5.1a);
  - Identify the scope of the sensitive BES data to be protected; and
  - Specify how the "confidentiality, integrity, and availability" of each type of BES data should be protected while in transit or at rest.

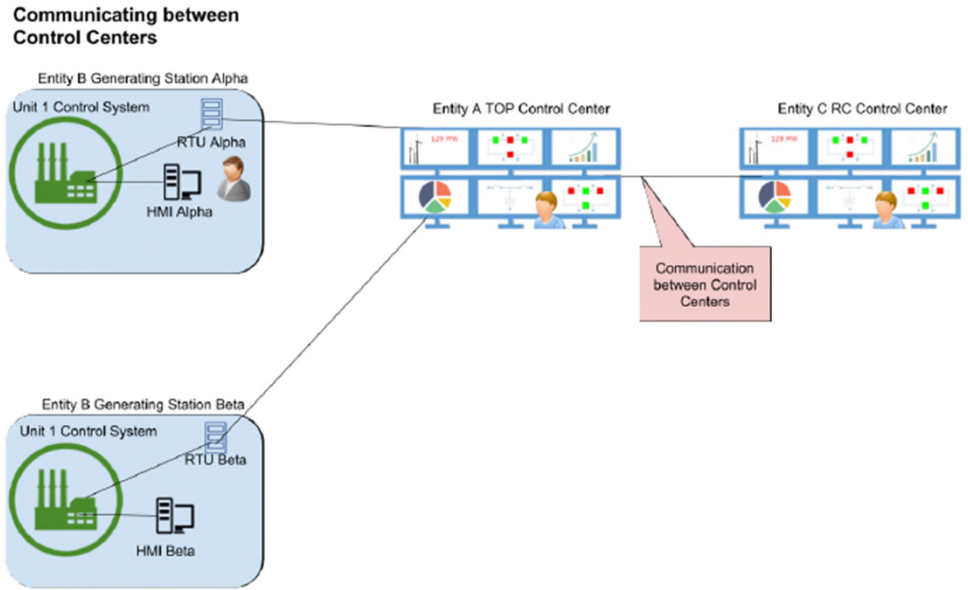
Security Concerns

- Inter-Control Center communications are crucial to maintaining BES reliability
- Control Centers must be capable of receiving and storing a variety of sensitive BES data from interconnected entities
- Data is used to support:
  - Immediate situational awareness and real-time operations
  - Communications needed to complete essential reliability functions

Example: Under TOP-003-3, the TOP dictates the schedule and format for the data it needs to perform Operational Planning Analyses, Real-time Monitoring, and Real-time Assessments.

Risks to Data in Transit

- Wide variety of communicated data (and formats) could be prone to targeted attacks
  - Eavesdropping
  - Data manipulation
  - "Man-in-the-middle" traffic interception



OVERVIEW OF PROPOSED RELIABILITY STANDARD CIP-012-1

NERC's Petition

- **CIP-012-1 Requirements**
  - Develop and implement a plan to mitigate the risks posed by unauthorized modification (integrity) and unauthorized disclosure (confidentiality) of assessment and monitoring data. Plans must include:
    - (1) The security protection used to mitigate the risks posed by unauthorized modification and unauthorized disclosure of real-time assessment and real-time monitoring data;
    - (2) The identification of where the utility applied the security protection; and
    - (3) The split of responsibilities for these protections when different utilities control the communicating control centers.

Who Must Comply with the Standard?

- **Responsible Entities** - Functional entities that own or operate a Control Center. Those entities include:
  - Balancing Authorities,
  - Generator Operators & Generator Owners,
  - Reliability Coordinators,
  - Transmission Operators & Transmission Owners.

- **Other Exceptions/Caveats**
  - Facilities that would otherwise qualify as a control center, but only communicate real-time data with other control centers regarding a "co-located field asset."
  - Oral communications

Implementation Schedule

- Under NERC's Implementation Plan, CIP-012-1 would become effective on the first day of the first calendar quarter two years after FERC issues an order approving the standard.

- FERC has placed this petition in a rulemaking docket, indicating that FERC will issue a Notice of Proposed Rulemaking, providing an opportunity for public comment before acting on the filing.
  - Typically, interested persons may submit comments on a NOPR for 60 days after its issuance.
  - After consideration of the comments FERC may issue an order approving its NOPR likely with modifications based on the comments submitted.
  - Only then will the 2 year clock begin.

CHALLENGES TO IMPLEMENTATION

Challenges to Implementation

- Identifying the data to be protected
  - Control Center-to-Control Center, with exception for Control Centers co-located at and only providing data for a substation or generation resource
  - Data exchanged between Control Centers (e.g. TOP-003, IRO-010) likely to be broader than what is protected under CIP-012
- Identifying Control Centers
- Choosing the method(s) of protection
  - Logical protection, physical protection, or a combination. Examples include:
    - VPN using Internet Protocol security with encryption (protects the communication)
    - Physical conduit (protects the communication)
    - Secure ICCP (protects the data integrity)
  - Determining whether the chosen protection is sufficient to "mitigate the risks posed by unauthorized disclosure and unauthorized modification" in light of Commission suggestion that protections should be commensurate with the risk
  - Avoiding protections that will adversely affect reliability, such as by increasing latency

Challenges to Implementation

- Identification of the location where the security control is applied
  - For physical protections, will need to demonstrate continuous physical barrier
  - Where encryption begins/ends
  - The application or service applying the security (e.g. Secure ICCP) where protection is applied at the application layer
- Sorting out arrangements with other Responsible Entities
  - Same plan as internal communications or bespoke plans?
  - Shared responsibility, or one entity assuming most responsibility
  - Cautions on accepting responsibility for both ends of a communication where one link is within another Responsible Entity's CIP environment
  - Determining who will manage the certificate authority if digital certificates are used
  - The unique problems of shared Control Centers

Potential Issues of Concern at the Commission

- Exclusion of data at rest: Are the existing CIP protections for this data adequate as NERC claims?
- Exclusion of Operational Planning Analysis data: Is the manipulation of information used for next-day operational planning sufficiently unlikely to have a reliability impact?
- Exclusion of oral communications: Are existing methods to detect and defend against compromised oral communications sufficient?

Biography

J. Daniel Skees
Washington, D.C.
T +1.202.739.5834
F +1.202.739.3001

J. Daniel Skees represents electric utilities before the Federal Energy Regulatory Commission (FERC) and other agencies on rate, regulatory, and transaction matters. He handles rate and tariff proceedings, electric utility and holding company transactions, reliability standards development and compliance, and FERC rulemaking proceedings. The mandatory electric reliability standards under Section 215 of the Federal Power Act are a major focus of Dan’s practice. He advises clients regarding compliance with reliability standards, and helps them participate in the development of new standards.

Biography

Arjun Ramadevanahalli
Washington, D.C.
T +1.202.739.5913
F +1.202.739.3001

As the US energy business continues to evolve, Arjun Prasad Ramadevanahalli represents key industry participants in regulatory, transactional, and litigation matters, including investigations and enforcement proceedings. Arjun represents electric power, natural gas, and other energy industry participants before the Federal Energy Regulatory Commission (FERC), the US Commodity Futures Trading Commission (CFTC), and the North American Electric Reliability Corporation (NERC). When necessary, his representations extend to court appeals.

Biography

Serge Agbre
Washington, D.C.
T +1.202.739.5633
F +1.202.739.3001

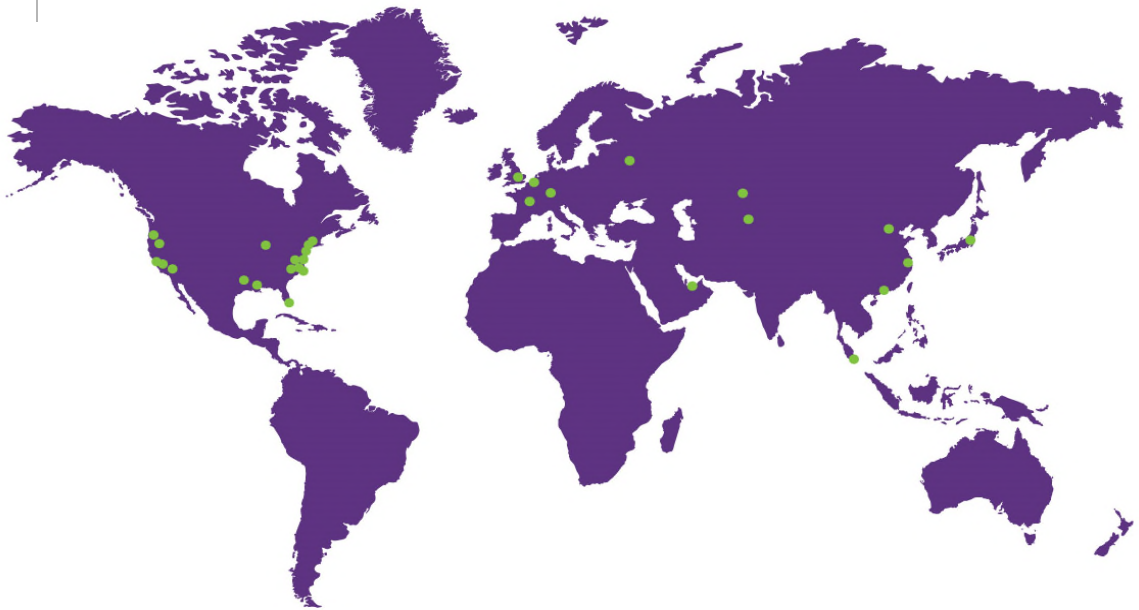
Serge Agbre represents electric, natural gas, and other energy industry participants in a variety of regulatory, transactional, and litigation matters before the Federal Energy Regulatory Commission (FERC). His practice includes related court appeals. Serge represents clients in enforcement matters, rate proceedings, certificate proceedings, and National Environmental Policy Act (NEPA) matters connected to gas infrastructure projects. He also represents electric utilities in rate proceedings, tariff proceedings, and reliability standard compliance and enforcement matters.

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Almaty	Chicago	Houston	Orange County	Shanghai*
Astana	Dallas	London	Paris	Silicon Valley
Beijing*	Dubai	Los Angeles	Philadelphia	Singapore
Boston	Frankfurt	Miami	Pittsburgh	Tokyo
Brussels	Hartford	Moscow	Princeton	Washington, DC
Century City	Hong Kong*	New York	San Francisco	Wilmington



Morgan Lewis

*Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan Lewis operates through Morgan, Lewis & Bockius, which is a separate Hong Kong general partnership registered with The Law Society of Hong Kong as a registered foreign law firm operating in Association with Luk & Partners.

THANK YOU