



Cyber Security: A Consequence Based Approach

David DeFalaise
Critical Infrastructure Protection Advisor
Federal Energy Regulatory Commission

Nuclear Regulatory Commission
28th Regulatory Information Conference
March 8, 2016

General Purpose Disclaimer



The contents of this presentation reflect my personal views only, they do not represent the views of the Federal Energy Regulatory Commission, its Commissioners or any other members of Federal Energy Regulatory Commission Staff.

02/16/2016 4:19 PM

2

What is the Federal Energy Regulatory Commission (FERC)?

- Similar to the NRC
 - An independent Federal regulatory agency
 - 5 Commissioners
 - Chairman serves as administrative head
- FERC responsibilities include:
 - Regulating the interstate transmission of electricity, natural gas, and oil
 - Reviewing proposals to build liquefied natural gas (LNG) terminals and interstate natural gas pipelines
 - Reviewing licensing of hydropower projects
 - Protecting the reliability of the high voltage interstate transmission system through mandatory reliability standards
 - Monitoring and investigating energy markets

02/16/2016 4:19 PM

3

Electric Reliability Regulatory Model

- Energy Policy Act (EPA) 2005 laid the groundwork for the current Regulatory Model.
- Commission has authority to certify an Electric Reliability Organization (ERO), approve or remand ERO developed Reliability Standards, ensures compliance with the approved mandatory standards by the users, owners, and operators of the bulk electric system.
- The North American Electric Reliability Corporation (NERC) was certified by the Commission as the ERO for the United States in 2006.
- The ERO delegated authority to 8 Regional Entities to enforce Reliability Standards.

02/16/2016 4:19 PM

4

Regional Entities



02/16/2016 4:19 PM

5

Two Types of Reliability Standards

- Operation & Planning (O&P)
 - Established by Order No. 693
Mandatory Reliability Standards for the Bulk-Power System (issued: March 16, 2007)
 - Focuses on natural disasters and misoperation
- Critical Infrastructure Protection (CIP)
 - Established by Order No. 706
Mandatory Reliability Standards for Critical Infrastructure Protection (issued: January 18, 2008)
 - Focuses on intentional man-made threats

02/16/2016 4:19 PM

6

Mandatory Reliability Standards

(with the number of standards in each family)

- BAL Resource and Demand Balancing (10)
- CIP **Critical Infrastructure Protection (9..., soon to be 11)**
- COM Communications (3)
- EOP Emergency Preparedness and Operations (8)
- FAC Facilities Design, Connections, and Maintenance (9)
- INT Interchange Scheduling and Coordination (5)
- IRO Interconnection Reliability Operations and Coordination (15)
- MOD Modeling, Data, and Analysis (17)
- NUC Nuclear (1)
- PER Personnel Performance, Training, and Qualifications (4)
- PRC Protection and Control (21)
- TOP Transmission Operations (9)
- TPL Transmission Planning (1)
- VAR Voltage and Reactive (4)

02/16/2016 4:19 PM

7

Two Types of CIP Standards

- Cyber Security
 - Reliability Standards CIP-002 through CIP-011
 - Two Generations of Security Control Implementation
 - 1st Generation: Urgent Action Cyber Security Standard 1200 (UA-1200) to CIP version 4
 - 2nd Generation: CIP version 5 and its revisions
- Physical Security
 - Reliability Standard CIP-014

02/16/2016 4:19 PM

8

1st Generation of Mandatory Cyber Security Standards

- CIP version 1, Order No. 706 (issued: January 18, 2008)
 - Commission issued 103 directives to NERC to modify the CIP Standards
 - Most directives were to better align the CIP Standards to “applicable features of the NIST framework.” (see Order No. 706 P 25)
- CIP version 2 & 3 addressed “low hanging” directives
 - CIP version 2: 128 FERC ¶ 61,291 (issued: 9/30/2009)
 - CIP version 3: 130 FERC ¶ 61,271 (issued: 3/31/2010)
- CIP version 4, Order No. 761 (issued: 4/19/2012), only changed the applicability of the CIP Standard
 - i.e., how which assets were determined to have mandatory standards applied to them
 - Change from a risk based approach to a bright line methodology

02/16/2016 4:19 PM

9

2nd Generation of Mandatory Cyber Security Standards

- Order No. 791 *Version 5 Critical Infrastructure Protection Reliability Standards*
 - Issued 11/22/2013
 - NERC started development in 2008
 - Prior to CIP version 3 & 4
 - Filed with FERC on 1/31/2013
 - Addressed all 103 directives from Order No. 706
 - Staff led technical conference on CIP Communication Security on 4/29/2014
- Order No. 822 *Revised Critical Infrastructure Protection Reliability Standards*
 - Issued January 21, 2016
 - Staff led technical conference on Supply Chain Risk Management on 1/28/2016

02/16/2016 4:19 PM

10

Risk Management (Simplified)*

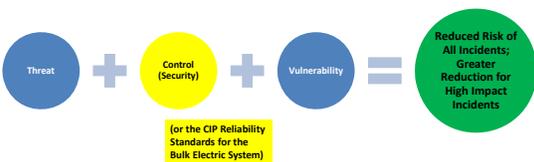


*Although there are many ways to represent risk in a formula, this approach somewhat mirrors an approach used by the Electricity - Information Sharing and Analysis Centers (E-ISAC), which is component of NERC.
See: <http://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx>

02/16/2016 4:19 PM

11

Goal of Mitigating Vulnerabilities (Simplified)



02/16/2016 4:19 PM

12

Risk-Based Compliance Monitoring and Enforcement (or Risk-Based CME)

- Originally a NERC project called “Reliability Assurance Initiative” (RAI)
 - Completed in 2014
- FERC Approved Risk-Based CME in Order 150 FERC ¶ 61,108
 - Issued February 19, 2015
 - Introduced Two Components
 - Compliance Exceptions
 - Self Logging
 - Qualified registered entities to “self-log” minimal risk issues as “compliance exceptions”
 - » Log periodically reviewed by the relevant Regional Entity

02/16/2016 4:19 PM

13

Risk-Based CME Risk Categories*

- Minimal
 - nothing serious could have occurred
 - there were complete or significant protections in place to reduce the risk
- Moderate
 - something serious could have occurred
 - there were only some protections in place to reduce risk
- Serious and Substantial
 - instance of noncompliance is related to a serious event

*See: 150 FERC ¶ 61,108
http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/FERC_Order_Approving_Risk-Based_CMEP.pdf

02/16/2016 4:19 PM

14

Risk-Based CME Enforcement Mechanisms*

- Compliance Exception
 - minimal-risk noncompliance that does not warrant a penalty
 - recorded and mitigated without triggering an enforcement action
- Find, Fix, Track and Report (FFT)
 - option for minimal and moderate risk non-compliances
 - Approved by FERC in order 138 FERC ¶ 61,193
 - Issued March 15, 2012
- Notice of Penalty

*See: 2016 ERO Enterprise Compliance Monitoring and Enforcement Program Implementation Plan Version 2.3
http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/2016%20CMEP%20IP_v_2_11172015_ForPosting.pdf

02/16/2016 4:19 PM

15

Risk-Based CME Enforcement Mechanism Timeline

| Mechanism | Order Approving | Approval Date |
|----------------------|-------------------|-------------------|
| Notice of Penalty | Order No. 672 | February 3, 2006 |
| Find, Fix, Track | 138 FERC ¶ 61,193 | March 15, 2012 |
| Compliance Exception | 150 FERC ¶ 61,108 | February 19, 2015 |

02/16/2016 4:19 PM

16
