ABB NERC CIP v5 Special interest group

Low Asset Discussion and Future CIP Versions & Compliance Activity

November 5, 2014

Today's Panel

- Tim Conway, EKC Consulting and Technical Director, ICS and SCADA programs at. conwaytimothyj@gmail.com
- Joseph "Joe" Baxter, NERC CIP Lead, ABB HV/DC - Before coming to ABB. joseph.baxter@us.abb.com
- Joe Doetzl, CISO and Head of Cyber Security, ABB Ventyx. Joe.Doetzl@ventyx.abb.com
- Mike Radigan, Senior Advisor, Cyber Risk Management, ABB PSPG
  - Mike.Radigan@us.abb.com (614) 398-6241

Additional NERC CIP educational webinars

NERC CIP Education Webinar Series - http://new.abb.com/us/about/nerc-cip-education

- **Cyber asset grouping for Power Generation – Tim Conway**
  Thursday, October 23, 2014 at 12:00 p.m.
  (Power generation specific) Learn process approaches to CIP-002-5.1 R1 as it pertains to BES cyber asset categorization.
  Register now: https://www1.gotomeeting.com/register/774616816
- **Access management and malicious software controls – Joe Baxter**
  Wednesday, October 29, 2014 at 2:00 p.m.
  Learn how to access control fits with CIP-004-5 and why account management is not effortless.
  Register now: https://www1.gotomeeting.com/register/448008129
- **Low assets and future CIP versions – Tim Conway & Joe Baxter**
  Wednesday, November 5, 2014 at 2:00 p.m.
  (Power generation specific) Learn the compliance requirements for entities with low assets and audit worksheets as well as future standard activities.
  Register now: https://www1.gotomeeting.com/register/872327665
- **Identification and review of critical transmission assets - Martin Shalhoub**,
  Wednesday, November 12, 2014 at 2:00 p.m.
  Learn how to approach the guidelines and criteria highlighted by NERC to fulfill the risk assessment goal.
  Register now: https://www1.gotomeeting.com/register/639963169

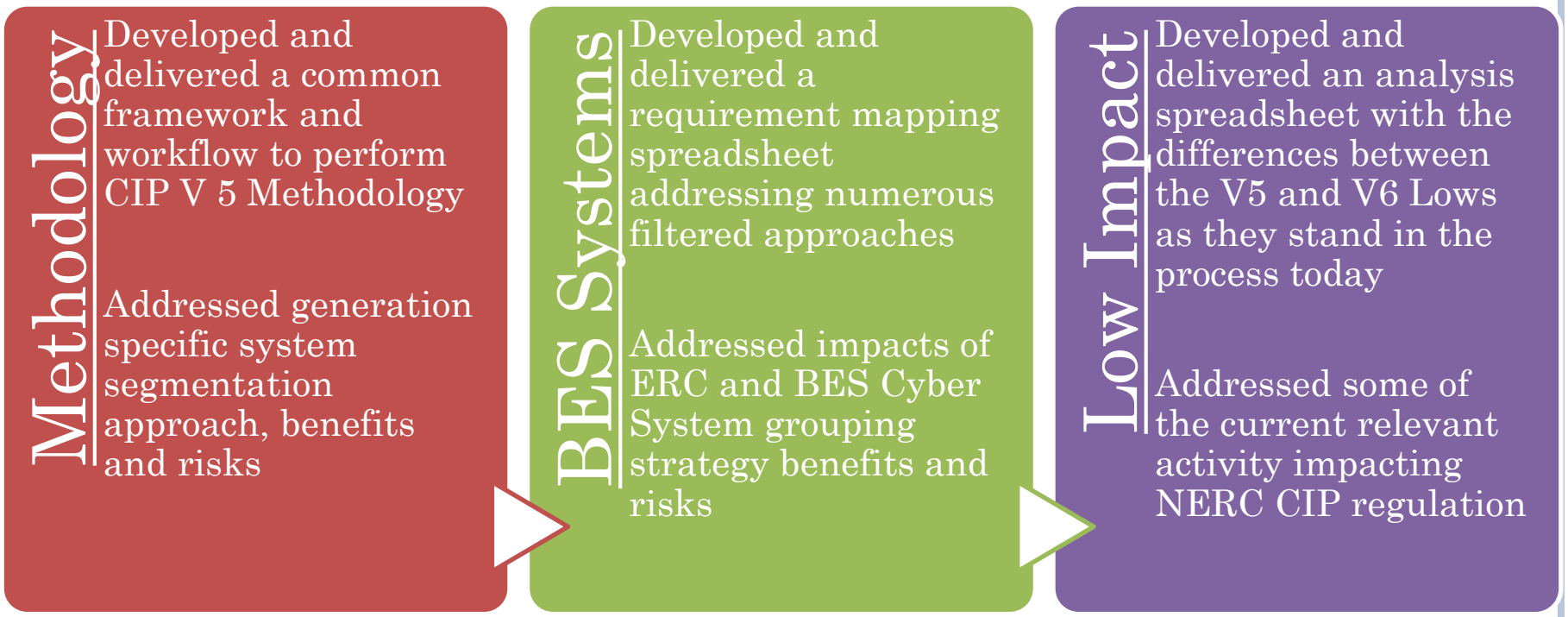
Agenda

- What Have we Covered
- CIP V5 Low Requirements
- SDT Activity
- Top 5 Items to Track
  - FERC Response
  - RAI
  - Lessons learned
  - RFI Process
  - Transition Plan

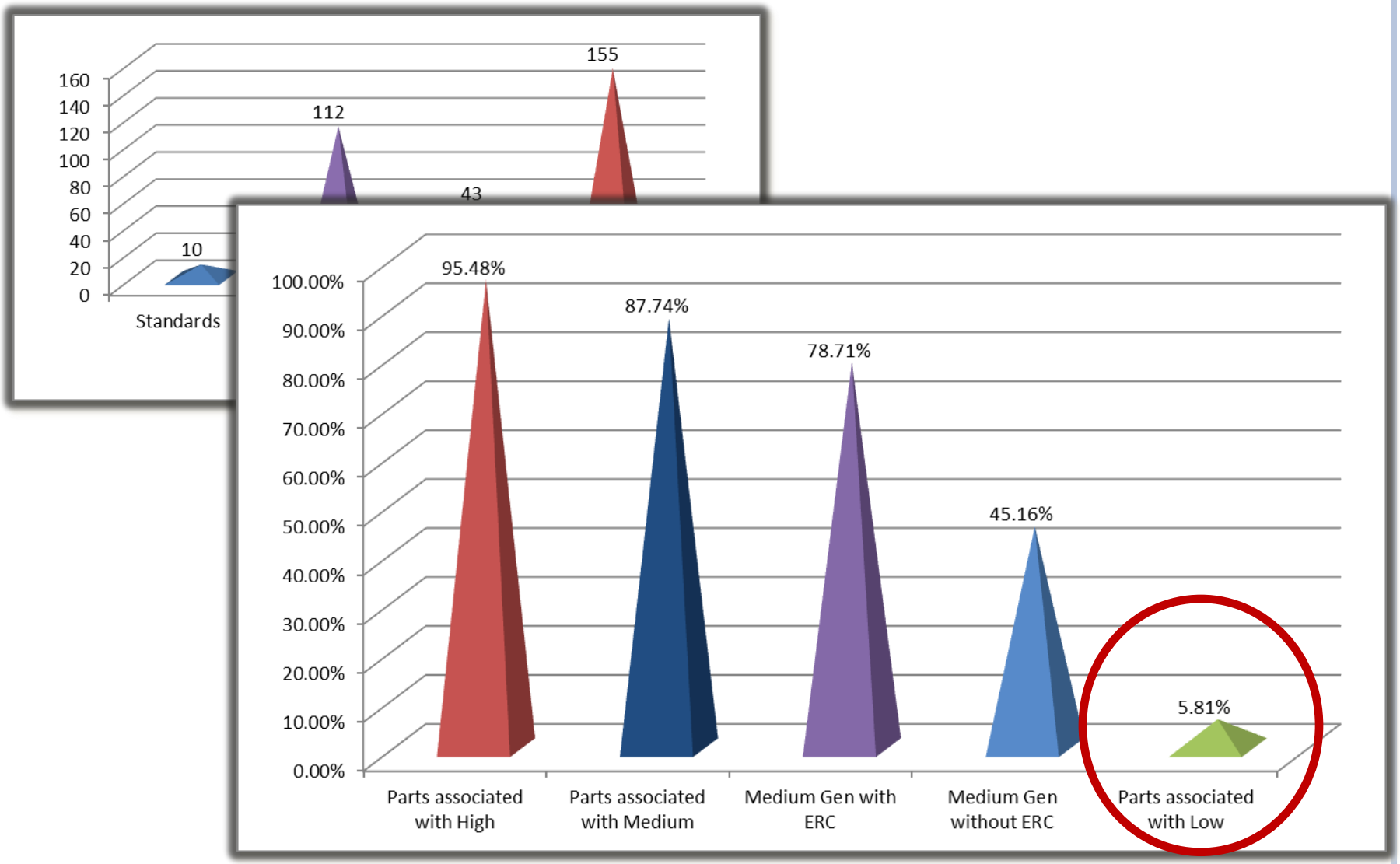
What Have we covered

Session 1 and Session 2

CIP V5 Special Interest Group



Data


160
140
120
100
80
60
40
20
0
10
112
43
155
Standards
100.00%
90.00%
80.00%
70.00%
60.00%
50.00%
40.00%
30.00%
20.00%
10.00%
0.00%
95.48%
87.74%
78.71%
45.16%
5.81%
Parts associated with High
Parts associated with Medium
Medium Gen with ERC
Medium Gen without ERC
Parts associated with Low

CIP V5 Low Requirements

Requirement Mapping

CIP-002-5.1			
	R1 - 1.3		x
	R2 - 2.1		x
	R2 - 2.2		x
CIP-003-5			
	R2 - 2.1		x
	R2 - 2.2		x
	R2 - 2.3		x
	R2 - 2.4		x
	R3		x
	R4		x

Summary of Low Requirements

- CIP-002-5.1
  - Attachment 1 Section 3
  - Update every 15 calendar months
  - Have CIP Senior Manager approve every 15 months
- **3. Low Impact Rating (L)**

  BES Cyber Systems not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

  3.1. Control Centers and backup Control Centers.

  3.2. Transmission stations and substations.

  3.3. Generation resources.

  3.4. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.

  3.5. Special Protection Systems that support the reliable operation of the Bulk Electric System.

  3.6. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

SDT Activity

FERC Order 791

Feb 3 2015

- Modify or Remove IAC
- Define and protect communication networks

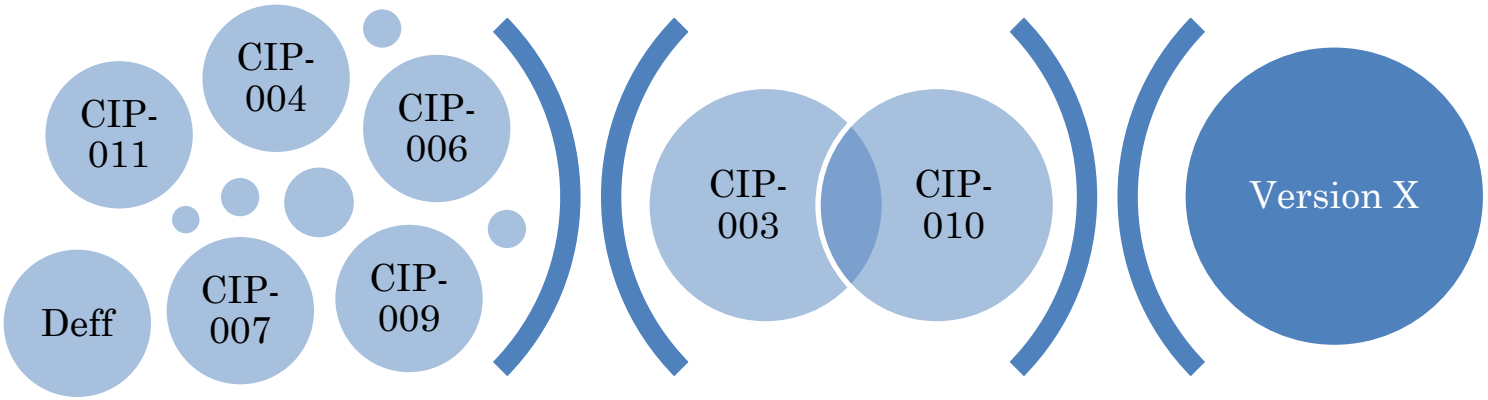
Open End

- Address security controls for Low
- Requirements for transient electronic devices

July Comment and Ballot

Standard	Quorum	Weighted Segment Vote
CIP-003-6	80.49%	35.72%
CIP-004-6	80.24%	80.71%
CIP-006-6	79.76%	76.20%
CIP-007-6	80.00%	78.35%
CIP-009-6	80.00%	85.29%
CIP-010-2	80.24%	49.48%
CIP-011-2	80.00%	82.51%
Definitions	78.05%	78.52%

CIP Version X Ballot



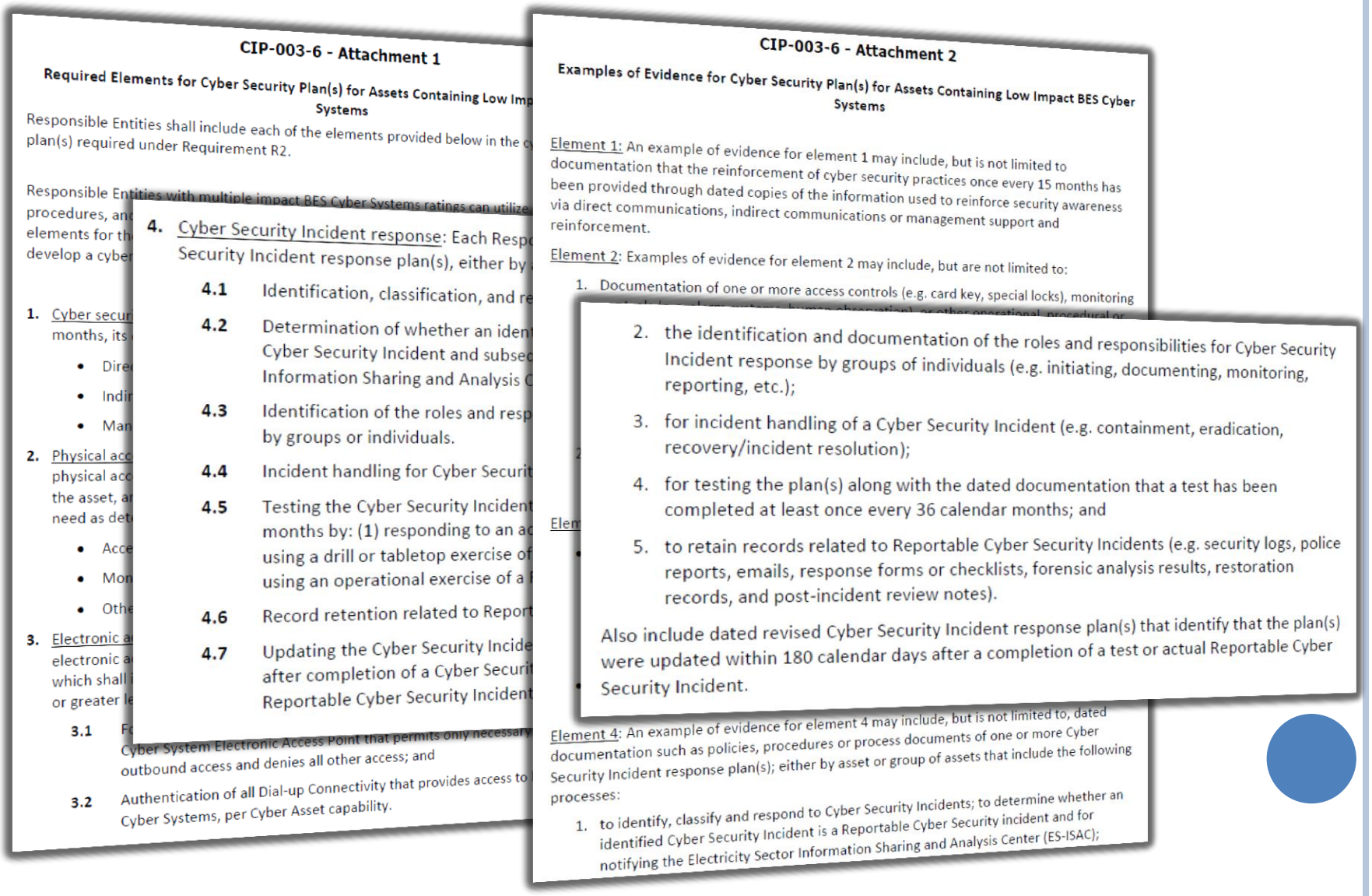
CIP-003-6

Develop modifications to the CIP standards to address security controls for assets containing low impact BES Cyber Systems.

CIP-010-2

Develop requirements that protect transient electronic devices.

Low and Transient Ongoing Activity



CIP-003-6 - Attachment 1

Required Elements for Cyber Security Plan(s) for Assets Containing Low Imp Systems

Responsible Entities shall include each of the elements provided below in the cy plan(s) required under Requirement R2.

Responsible Entities with multiple impact BES Cyber Systems ratings can utilize procedures, an elements for th develop a cyber

1. Cyber secur months, its
   - Dire
   - Indi
   - Man
2. Physical acc physical acc the asset, a need as det
   - Acce
   - Mon
   - Othe
3. Electronic a electronic a which shall or greater le

   3.1 F Cyber System Electronic Access Point that permits only necessary outbound access and denies all other access; and

   3.2 Authentication of all Dial-up Connectivity that provides access to Cyber Systems, per Cyber Asset capability.

4. Cyber Security Incident response: Each Resp Security Incident response plan(s), either by

   4.1 Identification, classification, and re

   4.2 Determination of whether an iden Cyber Security Incident and subsec Information Sharing and Analysis C

   4.3 Identification of the roles and resp by groups or individuals.

   4.4 Incident handling for Cyber Securit

   4.5 Testing the Cyber Security Incident months by: (1) responding to an ac using a drill or tabletop exercise of using an operational exercise of a

   4.6 Record retention related to Report

   4.7 Updating the Cyber Security Incide after completion of a Cyber Securit Reportable Cyber Security Incident

CIP-003-6 - Attachment 2

Examples of Evidence for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems

Element 1: An example of evidence for element 1 may include, but is not limited to documentation that the reinforcement of cyber security practices once every 15 months has been provided through dated copies of the information used to reinforce security awareness via direct communications, indirect communications or management support and reinforcement.

Element 2: Examples of evidence for element 2 may include, but are not limited to:

1. Documentation of one or more access controls (e.g. card key, special locks), monitoring

2. the identification and documentation of the roles and responsibilities for Cyber Security Incident response by groups of individuals (e.g. initiating, documenting, monitoring, reporting, etc.);

3. for incident handling of a Cyber Security Incident (e.g. containment, eradication, recovery/incident resolution);

4. for testing the plan(s) along with the dated documentation that a test has been completed at least once every 36 calendar months; and

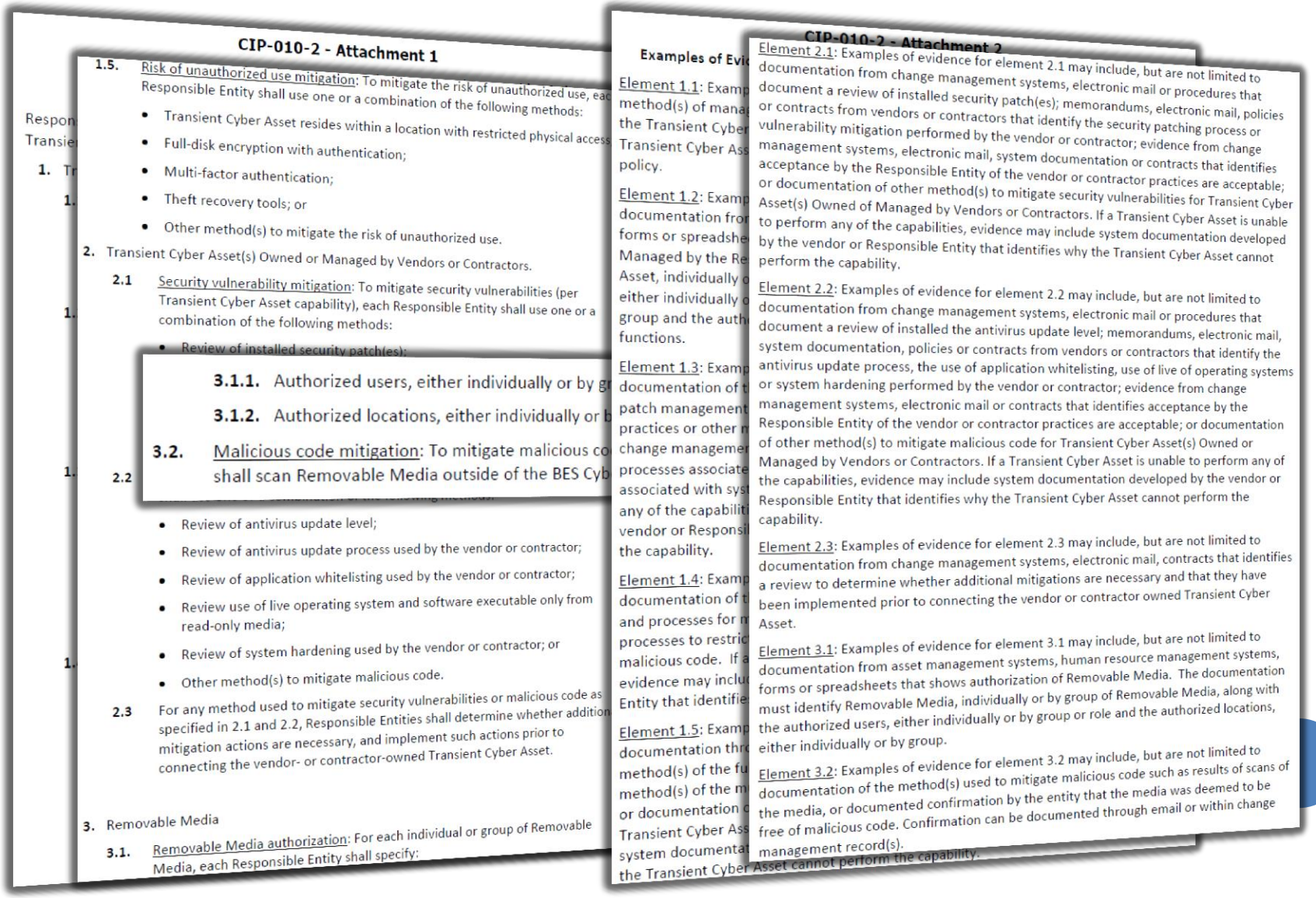
5. to retain records related to Reportable Cyber Security Incidents (e.g. security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes).

Also include dated revised Cyber Security Incident response plan(s) that identify that the plan(s) were updated within 180 calendar days after a completion of a test or actual Reportable Cyber Security Incident.

Element 4: An example of evidence for element 4 may include, but is not limited to, dated documentation such as policies, procedures or process documents of one or more Cyber Security Incident response plan(s); either by asset or group of assets that include the following processes:

1. to identify, classify and respond to Cyber Security Incidents; to determine whether an identified Cyber Security Incident is a Reportable Cyber Security incident and for notifying the Electricity Sector Information Sharing and Analysis Center (ES-ISAC);

Low and Transient Ongoing Activity



CIP-010-2 - Attachment 1

1.5. Risk of unauthorized use mitigation: To mitigate the risk of unauthorized use, each Responsible Entity shall use one or a combination of the following methods:

- Transient Cyber Asset resides within a location with restricted physical access
- Full-disk encryption with authentication;
- Multi-factor authentication;
- Theft recovery tools; or
- Other method(s) to mitigate the risk of unauthorized use.

2. Transient Cyber Asset(s) Owned or Managed by Vendors or Contractors.

2.1 Security vulnerability mitigation: To mitigate security vulnerabilities (per Transient Cyber Asset capability), each Responsible Entity shall use one or a combination of the following methods:

- Review of installed security patch(es);

3.1.1. Authorized users, either individually or by g

3.1.2. Authorized locations, either individually or b

3.2. Malicious code mitigation: To mitigate malicious co

2.2 shall scan Removable Media outside of the BES Cyb

- Review of antivirus update level;
- Review of antivirus update process used by the vendor or contractor;
- Review of application whitelisting used by the vendor or contractor;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the vendor or contractor; or
- Other method(s) to mitigate malicious code.

2.3 For any method used to mitigate security vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether addition mitigation actions are necessary, and implement such actions prior to connecting the vendor- or contractor-owned Transient Cyber Asset.

3. Removable Media

3.1. Removable Media authorization: For each individual or group of Removable Media, each Responsible Entity shall specify:

Examples of Evi

Element 1.1: Examp method(s) of mana the Transient Cyber Transient Cyber Ass policy.

Element 1.2: Examp documentation fro forms or spreadshe Managed by the Re Asset, individually either individually group and the auth functions.

Element 1.3: Examp documentation of t patch management practices or other n change manageme processes associate associated with syst any of the capabiliti vendor or Responsi the capability.

Element 1.4: Examp documentation of t and processes for n processes to restric malicious code. If a evidence may inclu Entity that identifie

Element 1.5: Examp documentation thro method(s) of the fu method(s) of the m or documentation o Transient Cyber Ass system documentat the Transient Cyber Asset cannot perform the capability.

CIP-010-2 - Attachment 2

Element 2.1: Examples of evidence for element 2.1 may include, but are not limited to documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memorandums, electronic mail, policies or contracts from vendors or contractors that identify the security patching process or vulnerability mitigation performed by the vendor or contractor; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity of the vendor or contractor practices are acceptable; or documentation of other method(s) to mitigate security vulnerabilities for Transient Cyber Asset(s) Owned of Managed by Vendors or Contractors. If a Transient Cyber Asset is unable to perform any of the capabilities, evidence may include system documentation developed by the vendor or Responsible Entity that identifies why the Transient Cyber Asset cannot perform the capability.

Element 2.2: Examples of evidence for element 2.2 may include, but are not limited to documentation from change management systems, electronic mail or procedures that document a review of installed the antivirus update level; memorandums, electronic mail, system documentation, policies or contracts from vendors or contractors that identify the antivirus update process, the use of application whitelisting, use of live of operating systems or system hardening performed by the vendor or contractor; evidence from change management systems, electronic mail or contracts that identifies acceptance by the Responsible Entity of the vendor or contractor practices are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) Owned or Managed by Vendors or Contractors. If a Transient Cyber Asset is unable to perform any of the capabilities, evidence may include system documentation developed by the vendor or Responsible Entity that identifies why the Transient Cyber Asset cannot perform the capability.

Element 2.3: Examples of evidence for element 2.3 may include, but are not limited to documentation from change management systems, electronic mail, contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the vendor or contractor owned Transient Cyber Asset.

Element 3.1: Examples of evidence for element 3.1 may include, but are not limited to documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users, either individually or by group or role and the authorized locations, either individually or by group.

Element 3.2: Examples of evidence for element 3.2 may include, but are not limited to documentation of the method(s) used to mitigate malicious code such as results of scans of the media, or documented confirmation by the entity that the media was deemed to be free of malicious code. Confirmation can be documented through email or within change management record(s).

October Comment and Ballot

Ballot	Quorum	Weighted Segment Vote
CIP-003-6	82.68%	68.77%
CIP-010-2	82.68%	74.67%
CIP Version X	83.17%	93.65%
CIP-003-6 Definitions	82.44%	79.97%
CIP-010-2 Definitions	81.95 %	85.64 %
CIP Implementation Plan	82.20%	89.07%

Final Ballot

- 10 day final ballot closes 8 PM Eastern 11/6/2014
- Standards under Version X are being balloted in the final ballot not the CIP-003-6 and CIP-010-2 with Low and Transient
- If final ballot passes – these V6 standards without Low and Transient will be submitted to the NERC BOT and then filed with FERC by Feb 3, 2015
- This means continued work will proceed with the remaining 791 directives and CIP-003-7 and CIP-010-3 will eventually need to be industry approved and NERC approved for submittal to FERC

Mapping

Standard	Requirement Part	Communication Network Change	Identify Assess and Correct Removal	New Requirement
CIP-003-6	R2		x	
	R4		x	
CIP-004-6	R2		x	
	R3		x	
	R4		x	
	R5		x	
CIP-006-6	R1		x	
	R1.10	x		x
	R2		x	
CIP-007-6	R1		x	
	R1.2	x		
	R2		x	
	R3		x	
	R4		x	
	R5		x	
CIP-009-6	R2		x	
CIP-010-2	R1		x	
	R2		x	
CIP-011-2	R1		x	
Summary	19	2	17	1

Top 5 Items to Track

FERC Response

- FERC Order 791
  - The Version 6 Standards submitted will directly address the directive to remove IAC
  - They directly address the modifications to VRF's and VSL's
  - They indirectly address the directive for a definition of Communication Network, by modifying the standards to address the reliability gap in protection identified by NERC
  - NERC also has proposed a modified plan to conduct the industry survey that was directed by FERC on the 15 min impact
- Await approval order and next steps for remaining 791 directives

Reliability Assurance Initiative (RAI)

- Zero Tolerance and Zero Deficiency = Bad
- SDT developed a controls based approach in which entities implement requirements in a manner that Identifies, Assess, corrects deficiencies = Industries Awesome, FERC = Nice, but difficult to enforce
- FERC recommended NERC develop a compliance and enforcement approach that would empower NERC and the Regional Entities to exercise risk-based enforcement discretion (RAI) = Awesome

RAI Terms

- **Inherent Risk Assessment (IRA)** - An IRA is a review of potential risks posed by an individual registered entity to the reliability of the BPS.
- **Internal Control Evaluation (ICE)** - the process by which an evaluation of entity internal controls takes place
- **Monitoring Tools** – RE determination of type and frequency of compliance monitoring tools warranted for a particular registered entity, determined by IRA and ICE processes.

http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Public_Final_Application_Risk-Based_CMEP_Concepts_to_CIPV5_%2810-22-2014%29.pdf

http://www.nerc.com/pa/comp/news/Documents/RAI_Spotlight_Agenda%20Now%20Available%20for%20RAI%20Industry%20Outreach%20Workshop.pdf

Lessons Learned

- Six Study participants – identified
- Impact of CIP V 5 to those participants
- Areas of Concern identified
  - Challenges in understanding the CIP Standards
  - Challenges in implementing the Requirements
  - Challenges in building resource capability

http://www.nerc.com/pa/CI/tpv5impmntnstdy/CIPv5_Implem_Study_Final_Report_Oct2014.pdf

Topics of Interest Identified

CIP Version 5 Reference
CIP-002-5
CIP-002-5
CIP-005-5
CIP-006-5
CIP-010-1

Table 4: Topics of Moderate Interest to Study Participants

CIP Version 5 Reference	Topic
CIP-002-5	Determining BES Cyber Systems that could adversely impact the BES within 15 minutes
CIP-004-5	Personnel risk assessments
CIP-005-5	External routable connectivity as it applies to serially connected devices
CIP-005-5	Routable communication used in substations
CIP-005-5	Intermediate systems
CIP-006-5	Response to unauthorized physical access within 15 minutes
CIP-006-5	Two-factor access control
CIP-007-5	Patch management process
CIP-007-5	Logging of shared access accounts
CIP-007-5	Read-only access
CIP-007-5	Password management for line protection relays

RFI Process

- NERC Standards Development Process contains a formal Request for Interpretation component
- Historically slow
- With implementation of standing IDT – Fast
- With FERC issuance of Remand – Halted
- Questions remain on future of RFI process vs lessons learned guidance

Transition Plan

- When to transition?
- When is your scheduled audit?
- Compatibility Tables and Audit Declaration

Version 5	Applicability													Compatibility	Version 3
	High Impact BES	High Impact BES w/ Dial-up	High Impact BES w/ ERC	Medium Impact BES	Medium Impact BES – CC	Medium Impact BES w/ Dial-up	Medium Impact BES w/ ERC	Medium Impact BES - NO ERC	Low Impact BES	EACMS	PACS	PCA	EAP	Local hardware - PSP	
003-5 R1. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: 1.1 Personnel & Training (CIP-004); 1.2 Electronic Security Perimeters (CIP-005) Including interactive Remote Access; 1.3 Physical security of BES Cyber Systems (CIP-006); 1.4 System security management (CIP-007); 1.5 Incident Reporting and response planning (CIP-008); 1.6 Recovery plans for BES Cyber Systems (CIP-009); 1.7 Configuration change management and vulnerability assessments (CIP-010); 1.8 Information protection (CIP-011); and 1.9 Declaring and responding to CIP Exceptional Circumstances.		X		X										MC	**003-3 R1.** Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following: R1.1 The cyber security policy addresses the requirements in Standards CIP-002-3 through CIP-009-3, including provision for emergency situations. R1.3 Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

http://www.nerc.com/pa/CI/Documents/V3-V5%20Compatibility%20Tables.pdf

Asset Identification Approach

Options provided to the Industry in Support of the Transition to Version 5	
Continue to comply by maintaining a valid RBAM for Critical Asset identification pursuant to CIP-002-3.	Option 1
For Responsible Entities that have already adopted the CIP V4 Critical Asset Criteria (CIP-002-4, Attachment 1), use the CIP V4 Critical Asset Criteria in its entirety, with the exception of criterion 1.4 (Blackstart Resources) and criterion 1.5 (Cranking Paths), to identify assets subject to the controls in CIP-003-3 through CIP-009-3.	Option 2
Use the CIP V5 "High" and "Medium" Impact Rating Criteria (CIP-002-5.1, Attachment 1) to identify assets subject to the controls in the CIP V5 Standards.	Option 3

http://www.nerc.com/pa/CI/Documents/V3-V5%20Transition%20Guidance%20FINAL.pdf

Next Steps

- Survey participants to gauge need for additional sessions on specific CIP V 5 Challenges
- Schedule additional sessions if needed depending on survey feedback
- Hold as needed deep dive conversations with customers who have specific questions or areas of concern

Join the ABB DCS Users Group

- **Website: www.adcsug.com**
- Users of ABB control system products and services in the power and water industries.
  - Forum to: share experiences, learn and collaborate with industry peers, measurably influence and improve ABB control products and services
- Top 5 reasons to join the group:
  - Networking: true peer-to-peer forums
  - Improvement suggestions: day-to-day challenges discussed and ideas exchanged
  - News: related articles and information from the industry
  - Events calendar: stay connected with users and ABB Power Generation
  - Polls / surveys: express your opinion and make your voice heard
- "The value of a users group, and that in particular of ABB DCS Users Group, is that as a group we have more access and leverage to change and improve the product than as individuals acting alone. It also allows us to participate in discussions that bring the best ideas forward and facilitates sharing information that helps everyone." - Bill Ossman, ABB DCS Users Group STECO member


QUESTIONS