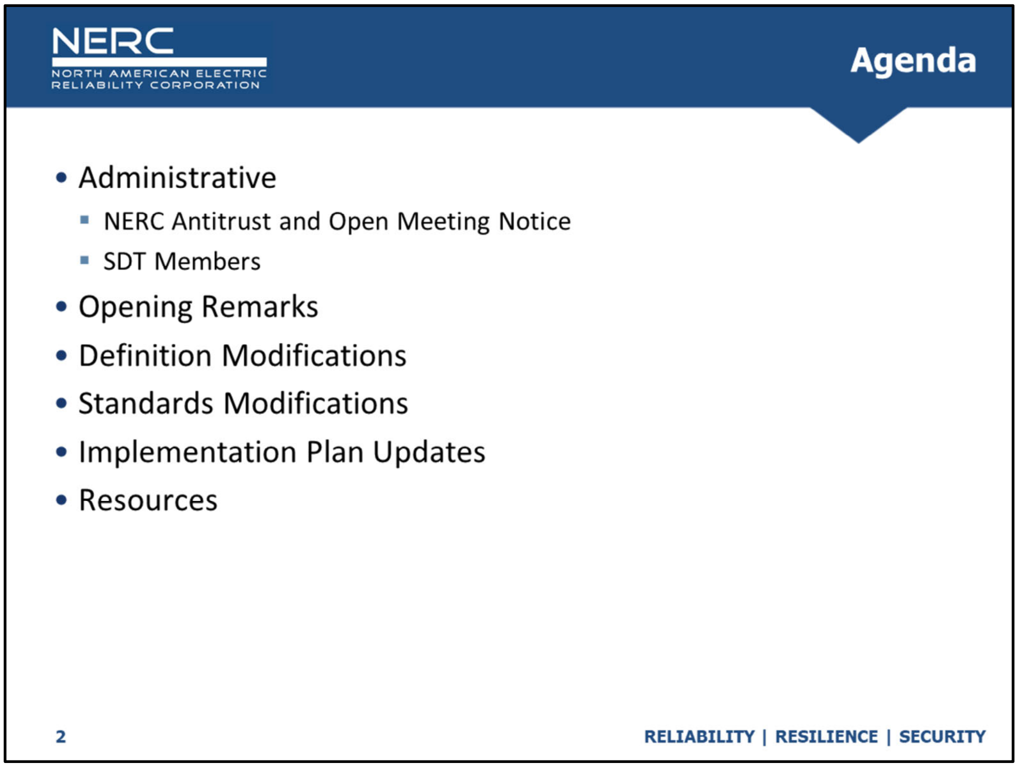
NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Virtualization Draft 4

Project 2016-02 Modification to CIP Standards

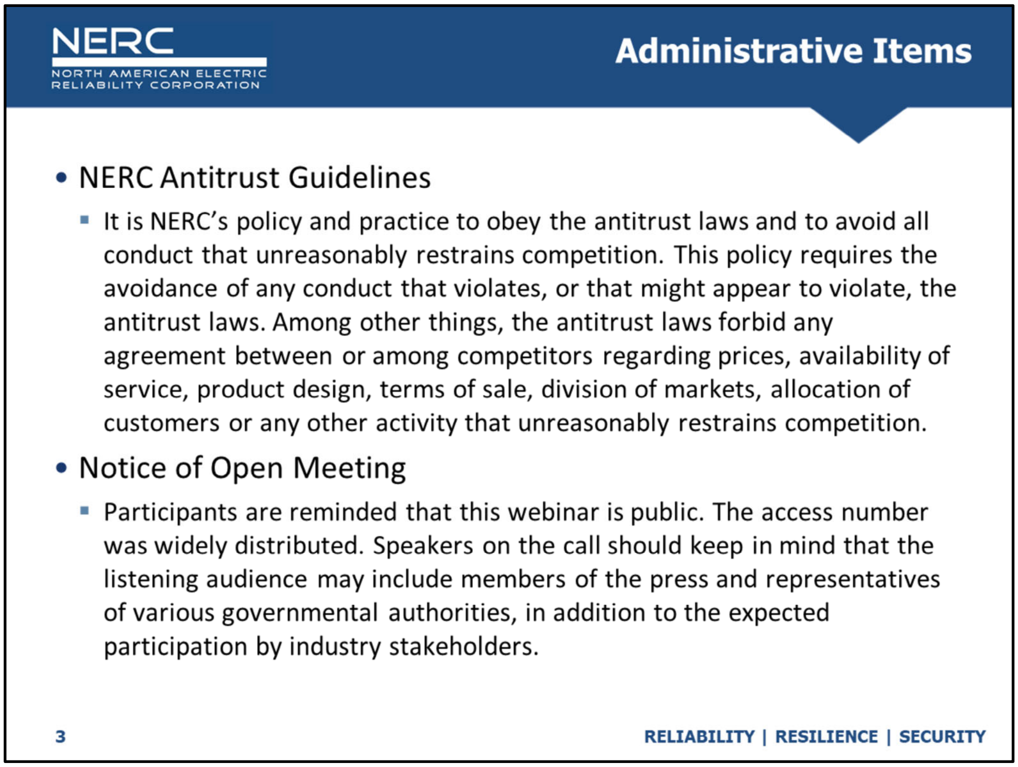
Project 2016-02 SDT
August 2022

RELIABILITY | RESILIENCE | SECURITY



Agenda

- Administrative
  - NERC Antitrust and Open Meeting Notice
  - SDT Members
- Opening Remarks
- Definition Modifications
- Standards Modifications
- Implementation Plan Updates
- Resources



NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Administrative Items

- NERC Antitrust Guidelines
  - It is NERC’s policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.
- Notice of Open Meeting
  - Participants are reminded that this webinar is public. The access number was widely distributed. Speakers on the call should keep in mind that the listening audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

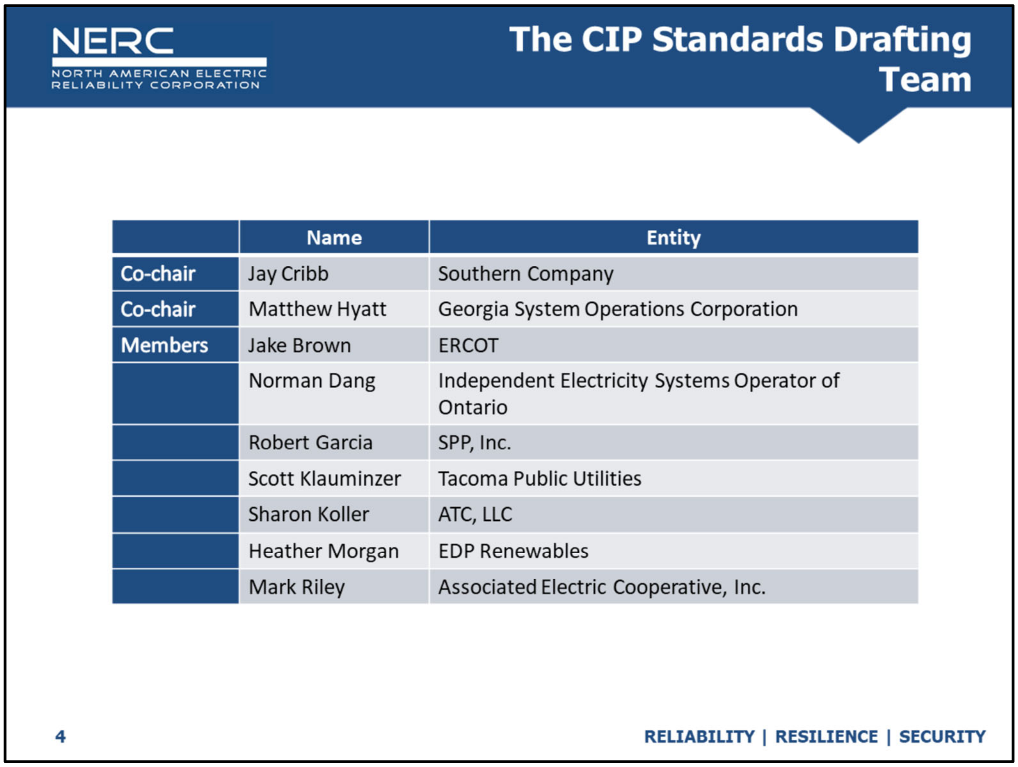
3 RELIABILITY | RESILIENCE | SECURITY

<Jordan>

Couple of reminders:

1) Please submit all questions via the slido Q&A. This will allow industry to up or down vote questions putting the popular questions at the for the SDT to review and address. There will be a slide explaining how slido works in a few min.

2) A reminder that the NERC Antitrust guidelines and public announcement apply to this meeting.



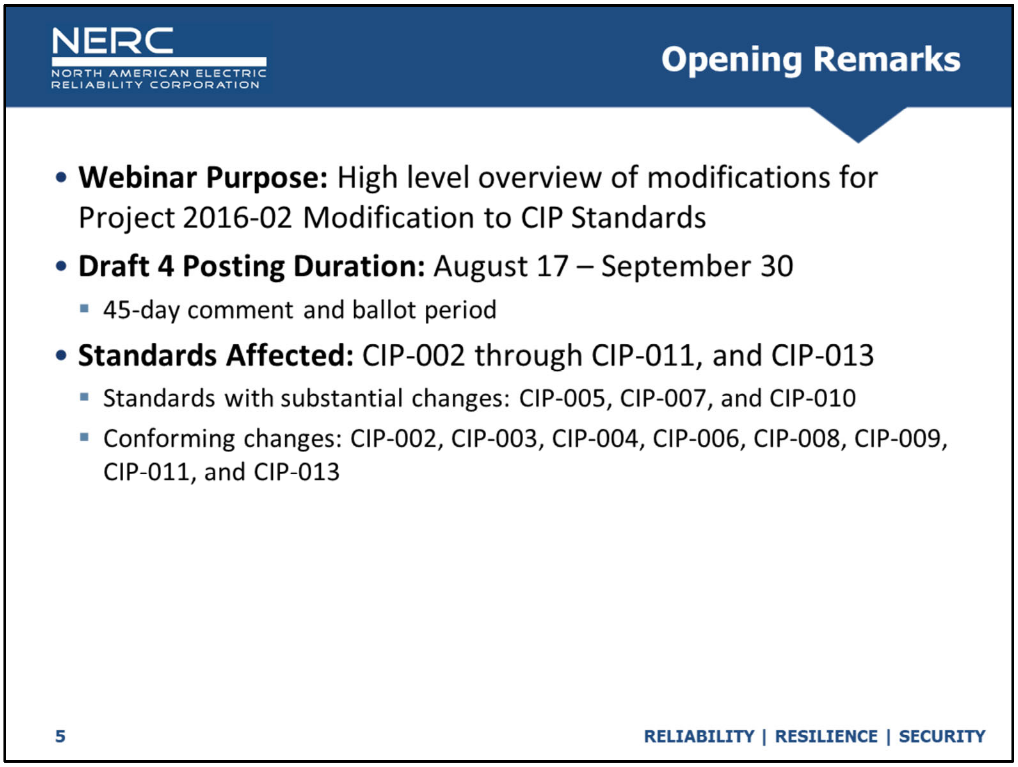
NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

The CIP Standards Drafting Team

	Name	Entity
Co-chair	Jay Cribb	Southern Company
Co-chair	Matthew Hyatt	Georgia System Operations Corporation
Members	Jake Brown	ERCOT
	Norman Dang	Independent Electricity Systems Operator of Ontario
	Robert Garcia	SPP, Inc.
	Scott Klauminzer	Tacoma Public Utilities
	Sharon Koller	ATC, LLC
	Heather Morgan	EDP Renewables
	Mark Riley	Associated Electric Cooperative, Inc.

<Jordan>

Here is a list of the 2016-02 SDT members. Should you have questions or concerns regarding information you hear today, do not hesitate to reach out to anyone on this list or even myself. We are all here to help and ensure industry is in a good place with the virtualization changes being made.

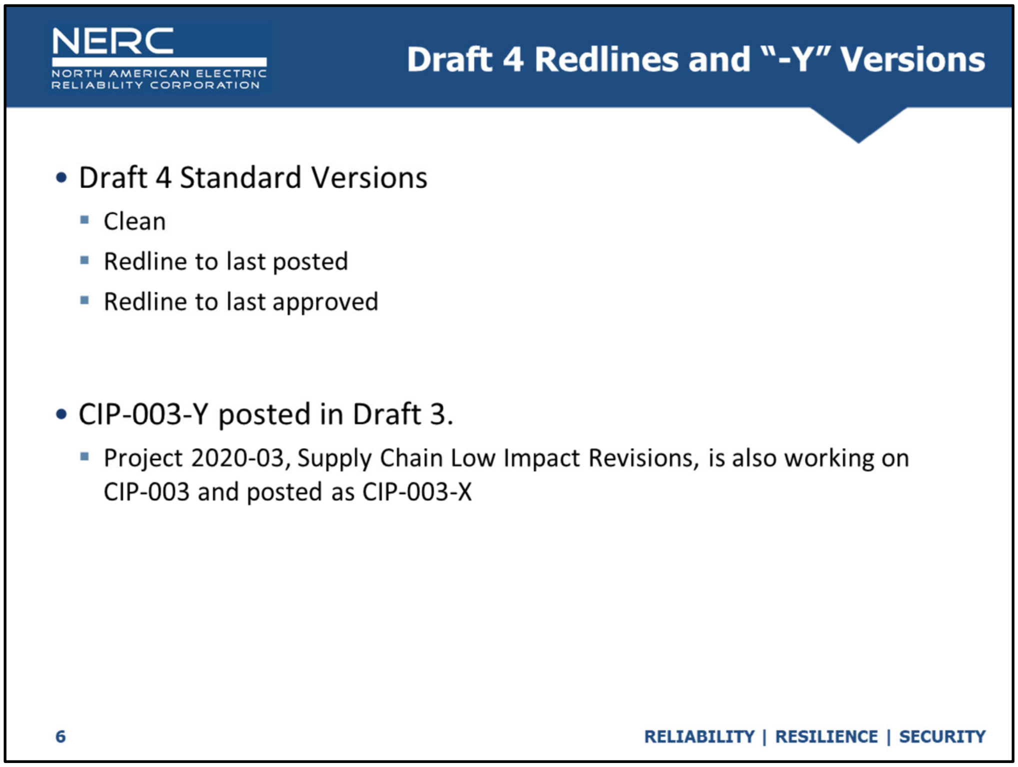


NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Opening Remarks

- **Webinar Purpose:** High level overview of modifications for Project 2016-02 Modification to CIP Standards
- **Draft 4 Posting Duration:** August 17 – September 30
  - 45-day comment and ballot period
- **Standards Affected:** CIP-002 through CIP-011, and CIP-013
  - Standards with substantial changes: CIP-005, CIP-007, and CIP-010
  - Conforming changes: CIP-002, CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013

<Jordan>



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Draft 4 Redlines and "-Y" Versions

- Draft 4 Standard Versions
  - Clean
  - Redline to last posted
  - Redline to last approved

- CIP-003-Y posted in Draft 3.
  - Project 2020-03, Supply Chain Low Impact Revisions, is also working on CIP-003 and posted as CIP-003-X

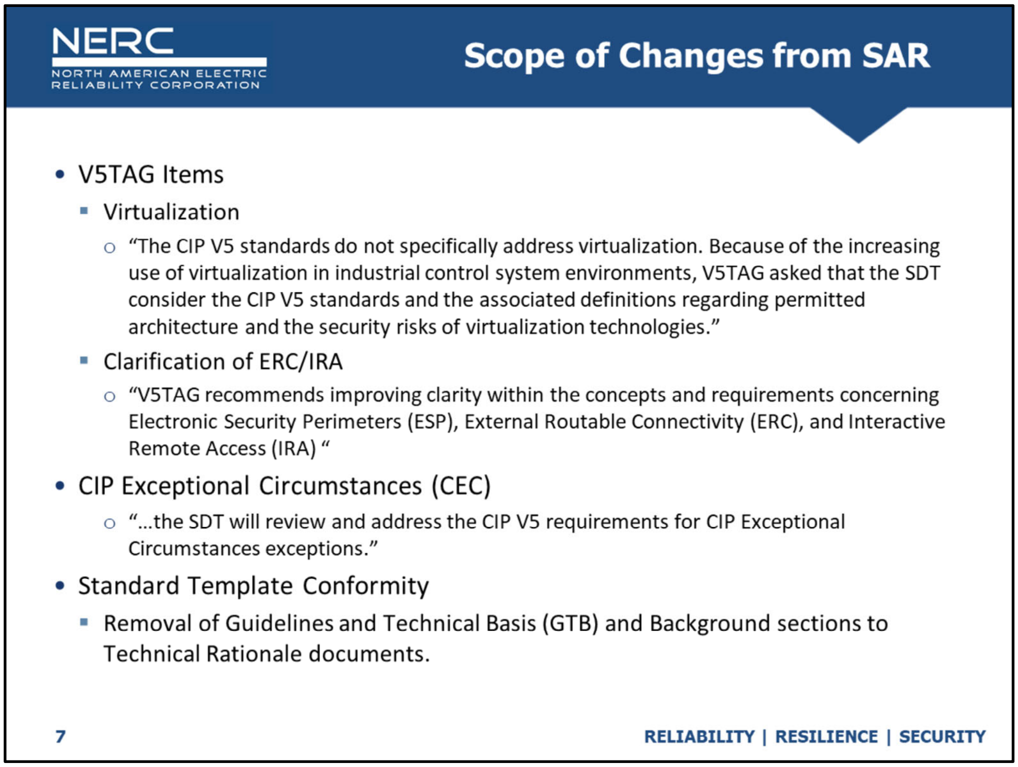
6

RELIABILITY | RESILIENCE | SECURITY

Jordan

- We have posted 11 standards and 3 versions of each, so 33 documents for just the standards alone.
- Shout out to Jordan for producing those. We heard that the RL to last approved is needed by the stakeholders.
- Two SDTs are modifying CIP-003 separately, so we are –Y and the Supply Chain Low impact revisions is –X.
- Depending on results from this comment/ballot period, we'll all coordinate on next steps with that standard.

- Add Extended ballot and comment period info.



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Scope of Changes from SAR

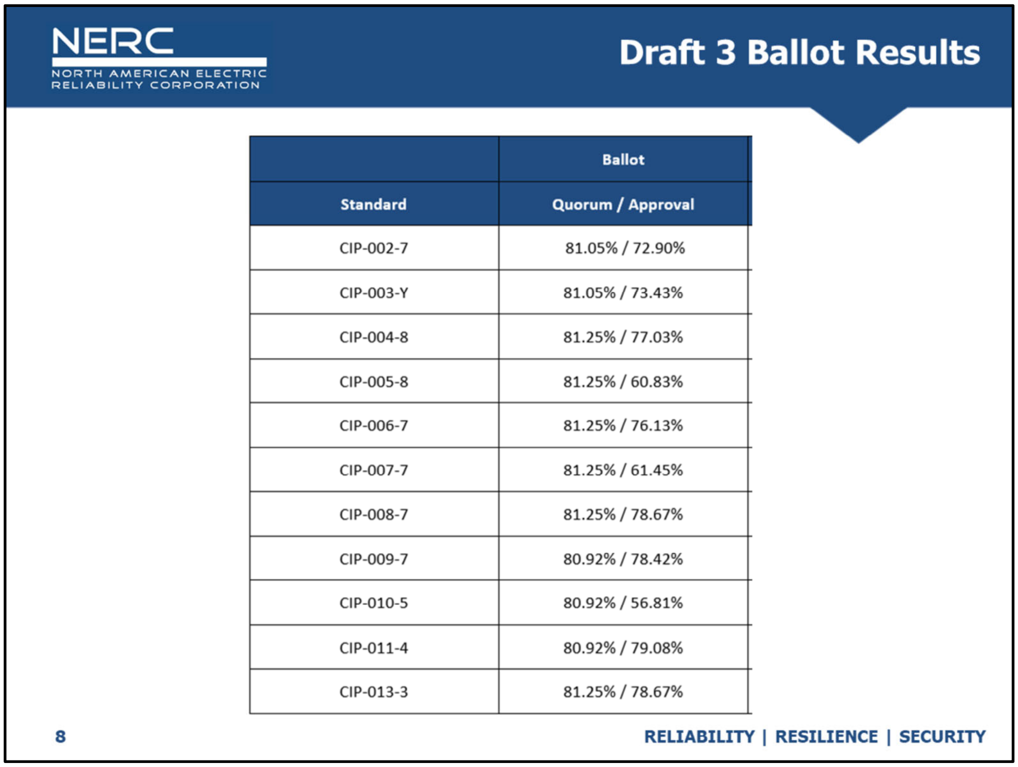
- V5TAG Items
  - Virtualization
    - "The CIP V5 standards do not specifically address virtualization. Because of the increasing use of virtualization in industrial control system environments, V5TAG asked that the SDT consider the CIP V5 standards and the associated definitions regarding permitted architecture and the security risks of virtualization technologies."
  - Clarification of ERC/IRA
    - "V5TAG recommends improving clarity within the concepts and requirements concerning Electronic Security Perimeters (ESP), External Routable Connectivity (ERC), and Interactive Remote Access (IRA) "
- CIP Exceptional Circumstances (CEC)
    - "…the SDT will review and address the CIP V5 requirements for CIP Exceptional Circumstances exceptions."
- Standard Template Conformity
  - Removal of Guidelines and Technical Basis (GTB) and Background sections to Technical Rationale documents.

7

RELIABILITY | RESILIENCE | SECURITY

<Matt>

- Before I get started on this section. On behalf of the standards drafting team, I'd like to welcome and thank everyone that is here today and would like to especially recognize all those who have contributed so heavily to the development of this revision. It has taken many experts, drafting team members, observers, active observers, workshops, feedback sessions, and leveraged many other platforms to get here!
- Your feedback is critical, and we are looking forward to getting more of it today!
- 2016-02 has completed several postings already and some of the V5TAG items are still remaining to be addressed
- Some of the V5TAG items are intended to address Highly technical topics related to providing clarifications for the use of virtualization and ERC/IRA
- While these topics werent out front for the entire time, these complex topics have been studied heavily throughout and are now being addressed
- As time went on, we also have a few additional items that are included in the posting including CEC's, and implementing the new standard template



NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Draft 3 Ballot Results

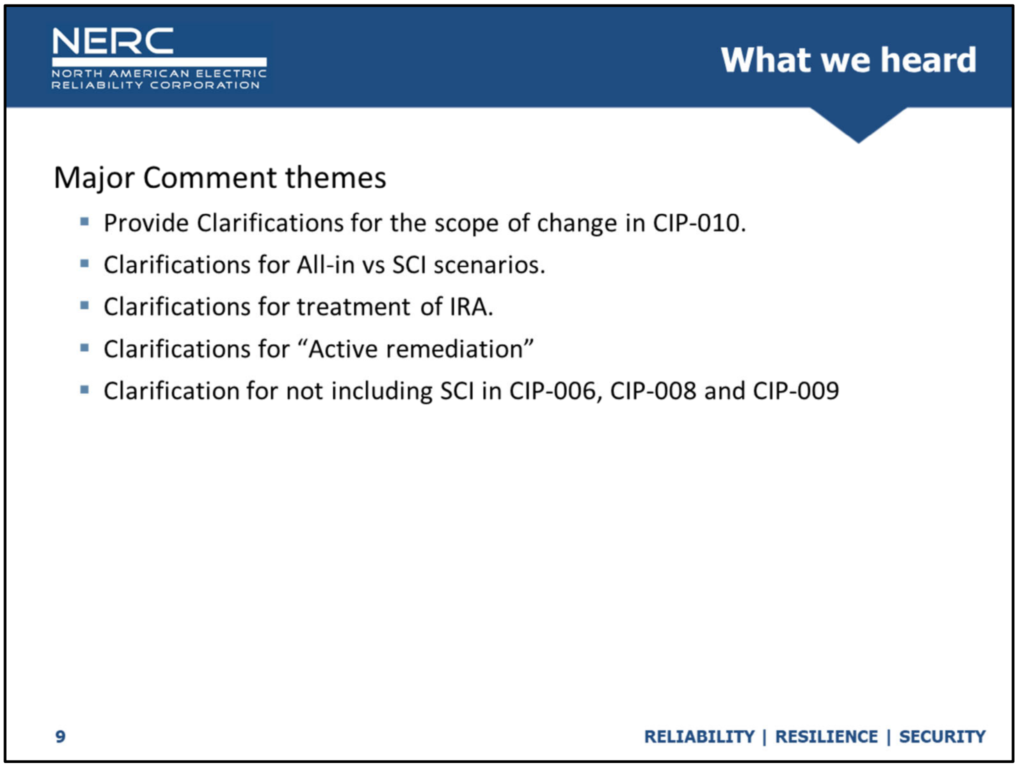
	Ballot
Standard	Quorum / Approval
CIP-002-7	81.05% / 72.90%
CIP-003-Y	81.05% / 73.43%
CIP-004-8	81.25% / 77.03%
CIP-005-8	81.25% / 60.83%
CIP-006-7	81.25% / 76.13%
CIP-007-7	81.25% / 61.45%
CIP-008-7	81.25% / 78.67%
CIP-009-7	80.92% / 78.42%
CIP-010-5	80.92% / 56.81%
CIP-011-4	80.92% / 79.08%
CIP-013-3	81.25% / 78.67%

8

RELIABILITY | RESILIENCE | SECURITY

<Matt>

- To get this kicked off, we wanted to take a few minutes to review the official ballot for Draft 3
- As you can see most of the industry appears to be relatively close on the acceptance of the approach we are on
- The majority of clarifications desired by industry are in CIP-005, CIP-007 and CIP-010
- When you review draft 4 this is very much refining what we have in draft 3 and making corrections for issues found by industry commenters
- The team attempted to really limit the changes to ensure that we stay on the path that was supported by the majority of industry.



NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

What we heard

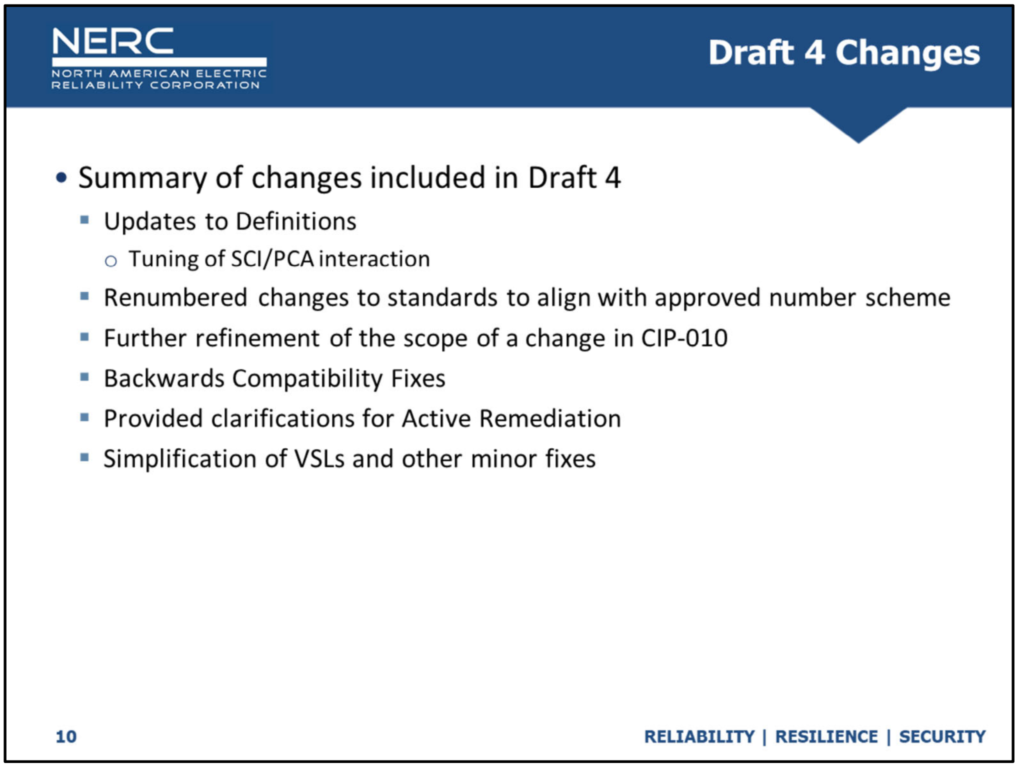
Major Comment themes

- Provide Clarifications for the scope of change in CIP-010.
- Clarifications for All-in vs SCI scenarios.
- Clarifications for treatment of IRA.
- Clarifications for “Active remediation”
- Clarification for not including SCI in CIP-006, CIP-008 and CIP-009

9 RELIABILITY | RESILIENCE | SECURITY

<Matt>

- Let me take a minute to talk through what the drafting team heard
- This is not an all-inclusive list, but these were the big items identified by industry
- We have those broken down into several comment themes
    - (read slide)
- Commenters did find some issues that are addressed in this posting but what was encouraging is that folks really appeared to understand the approach and offered some great feedback
- Let’s take a look at the summary of changes for this draft.



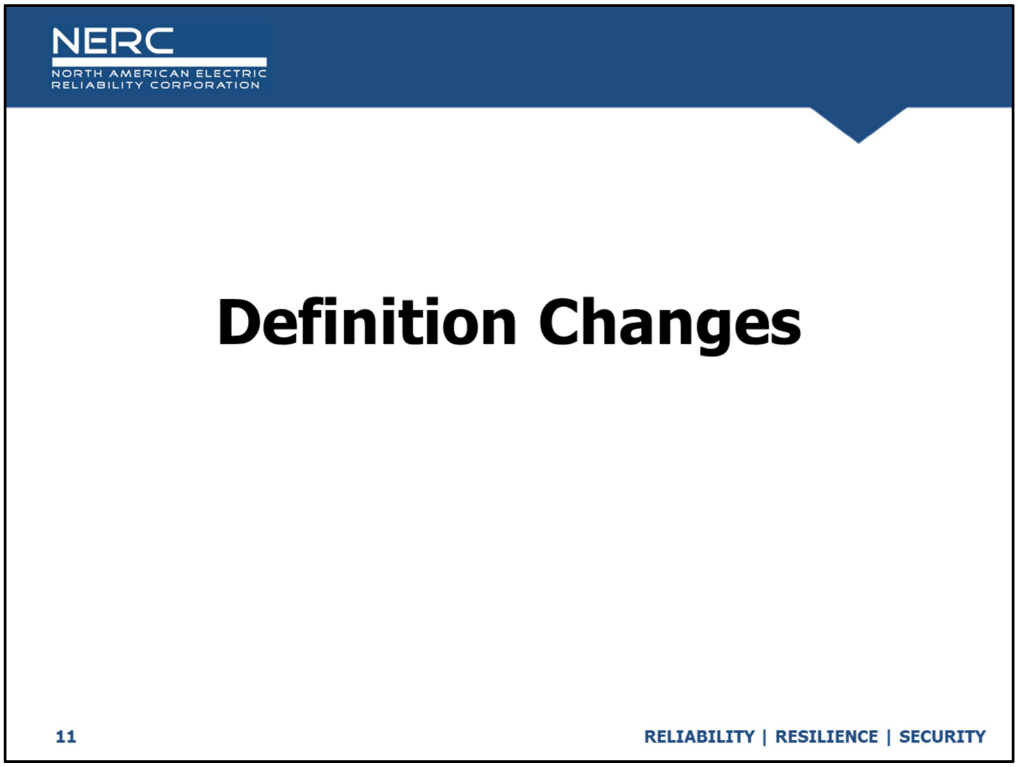
NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Draft 4 Changes

- Summary of changes included in Draft 4
  - Updates to Definitions
    - Tuning of SCI/PCA interaction
  - Renumbered changes to standards to align with approved number scheme
  - Further refinement of the scope of a change in CIP-010
  - Backwards Compatibility Fixes
  - Provided clarifications for Active Remediation
  - Simplification of VSLs and other minor fixes

<Matt>

- As we already discussed, we are attempting to make this draft 4 a refinement of the approach in Draft 3 as much as possible
- Summary of changes (read slide)
  - Not an all inclusive list
- After this quick summary, lets take a bit of a deeper dive into the changes. I will pass it to Jay (Speaker 3) to talk through some of the definitions changes in the draft.



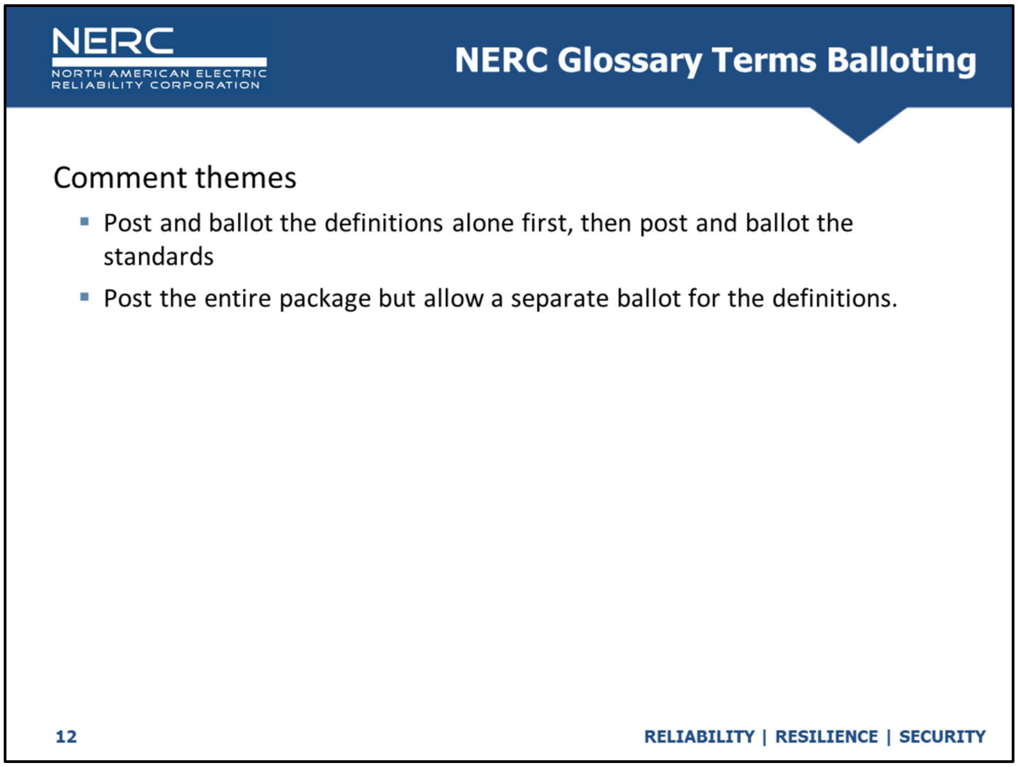
NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Definition Changes

11

RELIABILITY | RESILIENCE | SECURITY

Thanks, Matt. I'll be going through the changes we've made to the definitions from draft 3 to draft 4 in response to your comments, but first I'd like to address a couple of overall comment themes concerning the balloting of definitions.



NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

NERC Glossary Terms Balloting

Comment themes

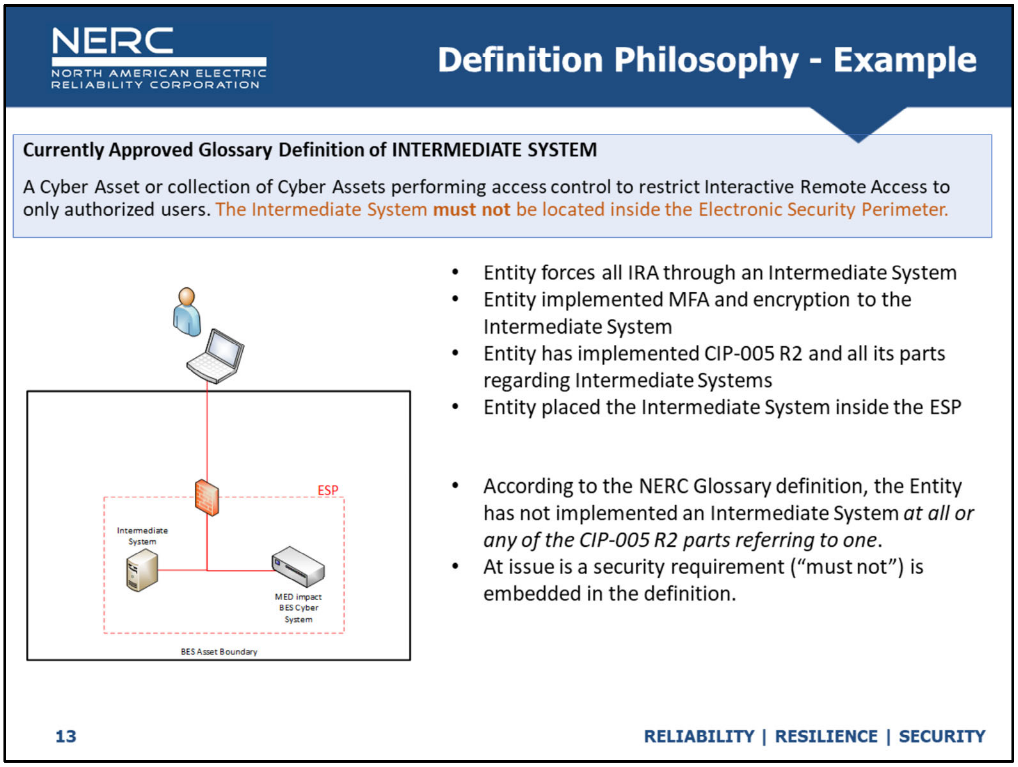
- Post and ballot the definitions alone first, then post and ballot the standards
- Post the entire package but allow a separate ballot for the definitions.

12

RELIABILITY | RESILIENCE | SECURITY

One theme was that we should ballot only the definitions first, get those correct, then bring the standards to ballot that use those definitions. If we did that, our thought is that we'd receive many more comments saying we can't vote on this definition without seeing the context of how its used in the standards. We've also seen where when working on requirements, we find the need to tweak a definition to match. It's a package deal. The second comment theme is we like having the entire package of definitions and all the standards together, but we'd like to be able to vote separately on the definitions, say to vote yes on standards but no on some definitions, but there is no ballot for the definitions. Let me say, yes, we agree with you, and that is a lesson learned for us and any future drafting teams. That leaves you having to vote no on the standards that use that definition, even if you approve of the standard, and leaves us having to discern from all the written comments that an issue with a standard not passing is actually a glossary term definition issue. So – lesson learned, but unfortunately, we can't change the ballot pool once established at the initial posting.

Another area that has driven several stakeholder comments gets to our 'philosophy of glossary terms' that we have used in our drafts; some examples are in the vein of "the scope of that definition is now much broader because you used Cyber System instead of BCS" and "since you took it out of the definition, can I now put my Intermediate System anywhere?" Legitimate questions if you are looking only at the definition, and I'd like to lay out the broader scenario of what we're up to. To do that, I'll walk through our 'poster child' example of Intermediate System.



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Definition Philosophy - Example

Currently Approved Glossary Definition of INTERMEDIATE SYSTEM

A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System **must not** be located inside the Electronic Security Perimeter.

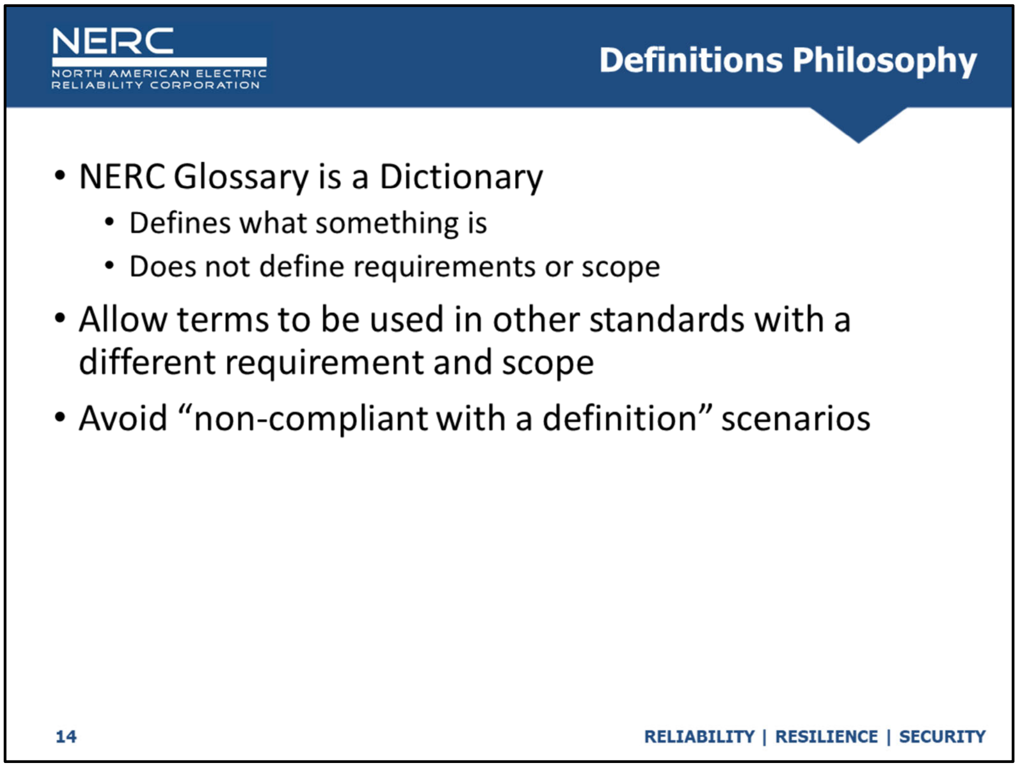
- Entity forces all IRA through an Intermediate System
- Entity implemented MFA and encryption to the Intermediate System
- Entity has implemented CIP-005 R2 and all its parts regarding Intermediate Systems
- Entity placed the Intermediate System inside the ESP

- According to the NERC Glossary definition, the Entity has not implemented an Intermediate System *at all or any of the CIP-005 R2 parts referring to one*.
- At issue is a security requirement ("must not") is embedded in the definition.

On the top of this slide you'll see the currently approved NERC glossary definition of Intermediate System. You'll notice the text in red and the bolded term "must not" and that is what makes this the 'poster child' example.

So let's imagine a hypothetical scenario - an entity is implementing an infrastructure for IRA, so they go to CIP-005 R2 and they start going down the page implementing what they read in the standard. They must force all IRA through an Intermediate System, so they put rules in their FW to direct all that traffic to the IS and block it to the BCS. They implement strong authentication on the IS, and they implement encryption from the remote client to the IS. They know how to find and disable vendor remote access. They have done everything in CIP-005 R2 to the letter. However, they put the IS inside the ESP.

What requirement is the entity in violation of? R2, but according to the glossary definition, they have not implemented an Intermediate System *at all*. Instead of missing one requirement part, it is as if they did nothing at all. The core issue is that "must not" in the definition – that is a requirement that should be in R2 (and its in 2.6.2), rather than the definition.



NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Definitions Philosophy

- NERC Glossary is a Dictionary
  - Defines what something is
  - Does not define requirements or scope
- Allow terms to be used in other standards with a different requirement and scope
- Avoid "non-compliant with a definition" scenarios

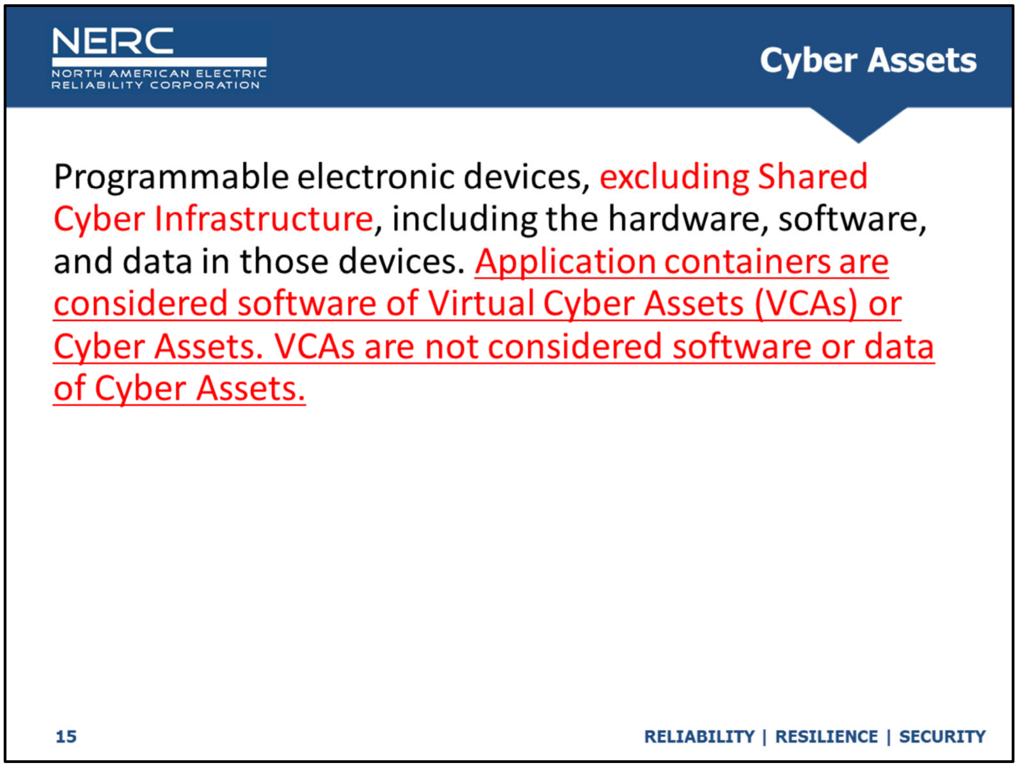
14

RELIABILITY | RESILIENCE | SECURITY

So that's one example. What we've attempted to do as we create or modify terms is keep the glossary as a dictionary – simply define what something is. The goal is to, as much as possible, keep what to do (requirements) and where to do it (scope) in a requirement in the standards. We've seen where scope changes, like CIP Sr Mgr that scopes itself to CIP-002 to CIP-011 in the definition – So when you add a CIP-013 that also mentions that role - you have a definition issue as well.

Addressing this in the definitions we're touching provides two benefits: 1) if the term is useful for another standard, or a requirement with a different scope – hopefully the term can be used as-is, and 2) it avoids this "non-compliant with a definition" strangeness.

In the past we've embedded this explanation in comment response documents which are not light reading, but I don't think we've addressed it in our webinars, so we wanted to take that opportunity today.



NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

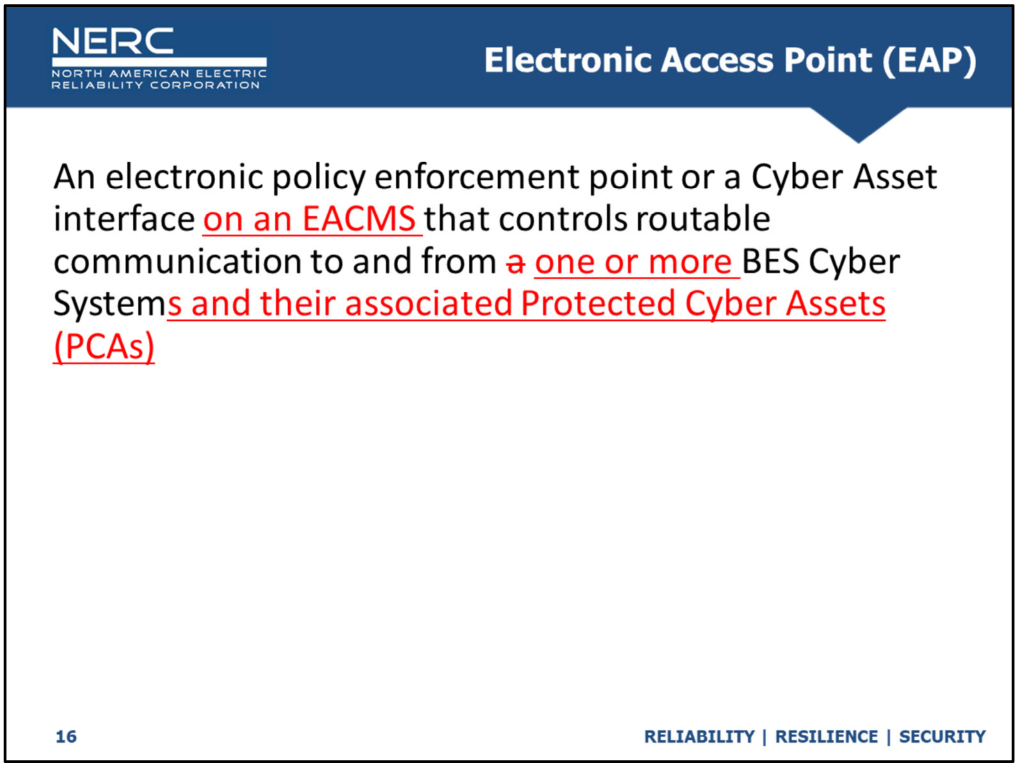
Cyber Assets

Programmable electronic devices, excluding Shared Cyber Infrastructure, including the hardware, software, and data in those devices. Application containers are considered software of Virtual Cyber Assets (VCAs) or Cyber Assets. VCAs are not considered software or data of Cyber Assets.

15

RELIABILITY | RESILIENCE | SECURITY

Now on to the changes we’ve made to individual definitions based on your comments. First up is Cyber Assets. The main definition has not changed at all. You’ll notice in several definitions we’ve gone to making statements about what something is AND what it is not. We’ve found we can get more clarity in a more concise manner that way. You’ll notice here that we moved the ‘excluding SCI’ up since this definition and SCI are both “programmable electronic device” based terms that are mutually exclusive. Then we’ve clarified just what the “software and data in those devices” means in a virtualization world. For example, containers can have some aspects that make them look more VCA like, but we’ve found that if you start down the path of treating a software application like a VCA, the suite of standards gets extremely convoluted and induces migraines. So we've clarified that an application container is to be treated like a native application in both this and the VCA definition. Then we added “VCAs are not considered software or data of Cyber Assets” to make it clear that if you have a HW server, put a hypervisor on it and run VCAs on it, you can’t go the route of saying that is one CA and all the virtual servers are just ‘software or data on the device’ and not manage those servers under CIP-007 for example. Our intent in all this is to help with identification clarity.



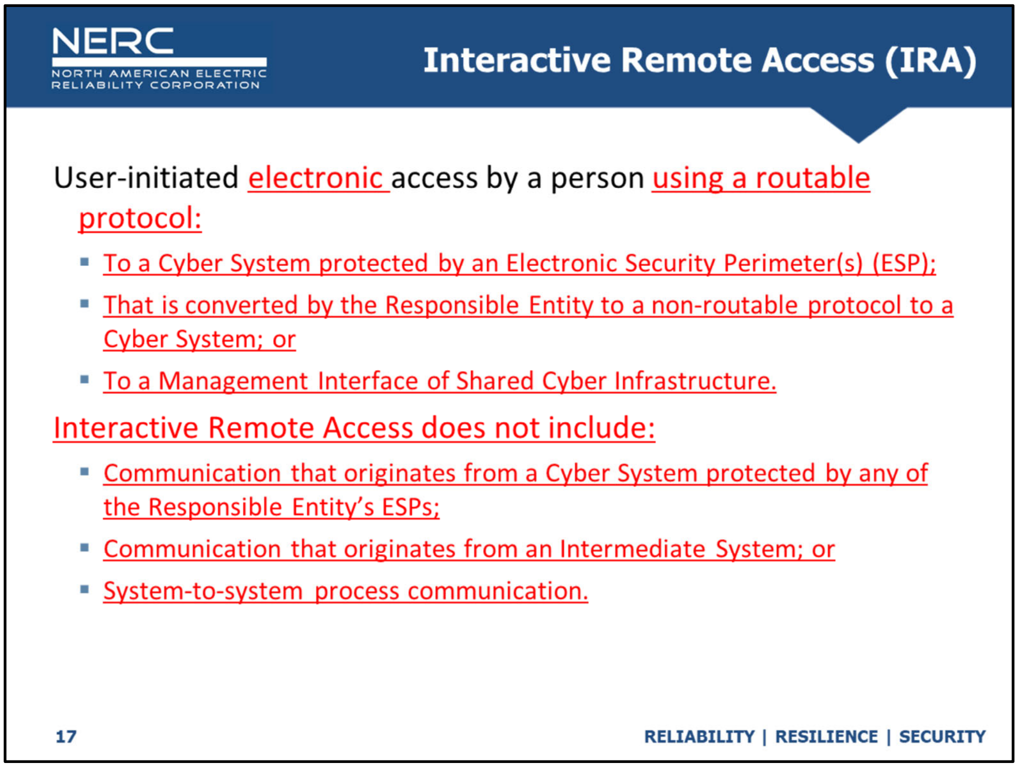
NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Electronic Access Point (EAP)

An electronic policy enforcement point or a Cyber Asset interface on an EACMS that controls routable communication to and from ~~a~~ one or more BES Cyber Systems and their associated Protected Cyber Assets (PCAs)

16 RELIABILITY | RESILIENCE | SECURITY

Next is EAP and we've made two edits here. We've added "on an EACMS" to help clarify in particular CIP-005 R1.3 concerning the mgt interface of an EACMS that enforces an ESP, which Scott will talk about in a bit. We've also clarified the grouping aspect of today's ESPs by changing it from "a BCS" to "one or more BCS and their associated PCAs" to make it clear the EAP and ESP as you've know it is still there, controlling access to a group of cyber assets on a network.



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Interactive Remote Access (IRA)

User-initiated electronic access by a person using a routable protocol:

- To a Cyber System protected by an Electronic Security Perimeter(s) (ESP);
- That is converted by the Responsible Entity to a non-routable protocol to a Cyber System; or
- To a Management Interface of Shared Cyber Infrastructure.

Interactive Remote Access does not include:

- Communication that originates from a Cyber System protected by any of the Responsible Entity's ESPs;
- Communication that originates from an Intermediate System; or
- System-to-system process communication.

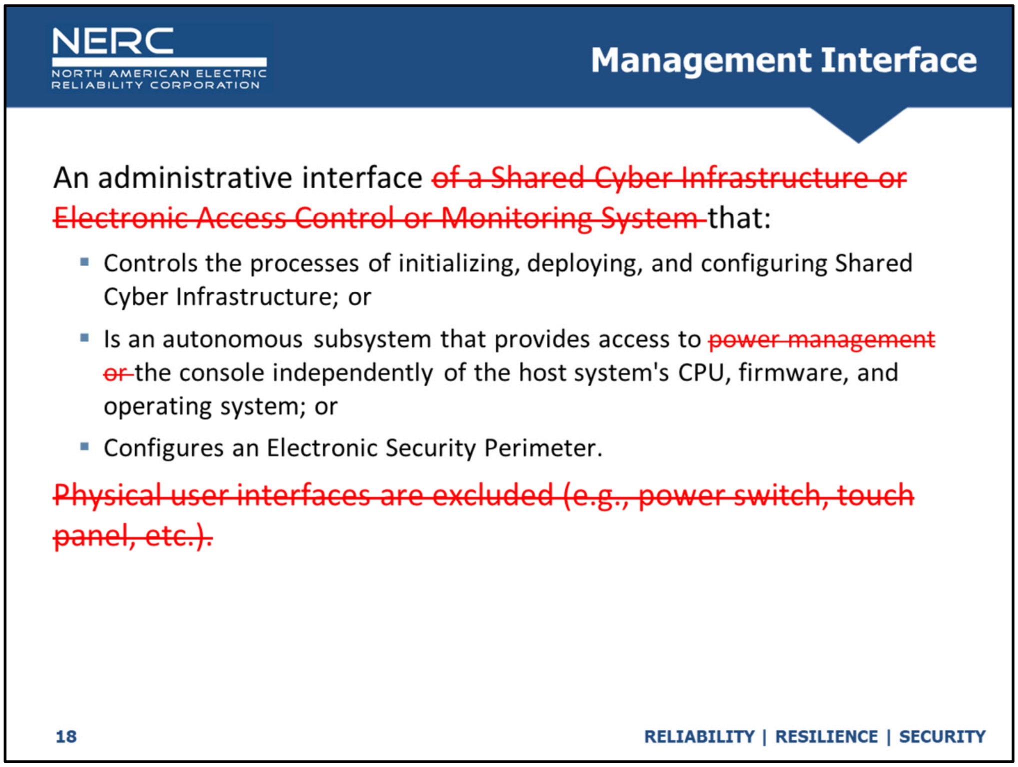
17 RELIABILITY | RESILIENCE | SECURITY

Next is IRA. We received a good number of comments on this, and we took a different approach to incorporate your comments; dividing it into statements of what it is, and what it is not. As you can see, it's a redo but we think this has much more clarity and incorporates what you told us you wanted to see.

We added the adjective 'electronic' just to make it clear up front that this is not physical access to a console, and we moved the "using a routable protocol" up to indicate the scope is remote sessions that originate with a routable protocol. We then put in three bullets of potential targets of IRA. First is a Cyber System protected by an ESP – this is the traditional, historical view of IRA. I'm talking to something inside an ESP. We use the "protected by" phrasing rather than 'inside' or "outside" to better incorporate ZT principles that are not network-perimeter based as they are implemented in the future. Also note that in keeping with our definition philosophy, it uses the generic Cyber System. The scoping of the targets of IRA security controls is in CIP-005 R2, and not within the definition.

The second bullet is the scenario this SDT was to clarify from the V5TAG in our SAR. We've added "converted by the Responsible Entity to a non-routable protocol" in response to comments, such as scenarios where Entity B puts a circuit in to Entity A's facility and gives Entity A a DB9 serial cable to plug into their system to exchange data. Entity A does not know if Entity B converts to routable protocol somewhere upstream. If they do, and they can do IRA over that circuit, then its on Entity B to identify that IRA and implement CIP-005 R2 on their routable protocol side, not Entity A who is serial only. On the flip side, if Entity A has routable protocol connectivity to their site, and THEY convert to serial and allow IRA to their system, then this bullet clarifies that is IRA even if the last few feet are serial. We think this language clarifies these "500 mile serial cable" scenarios. Finally, we have a target of the Management Interface of SCI, since in SCI situations that is elevated risk access and warrants a specific scope.

We then provide 3 bullets of what IRA is not. The first bullet carries over the longstanding exemption of origin points that are in another of the entity's ESPs. For those comments concerned with IRA incorporating operators in a control center operating devices in the field, we hope this new format of the definition clarifies that is not IRA, just like today. The second bullet was added due to your comments where, as written, it could require an IS behind your IS recursively, setting up a hall of mirrors situation. Thanks for finding that and we think this exclusion fixes it. The 3rd bullet was also due to your comments of wanting that clarity and specificity in the current definition reinstated into this one; so the system to system process communication exclusion is back. So...major rework of this definition for this draft, and it's our hope its much clearer and addresses the comment themes we heard from you.



NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Management Interface

An administrative interface ~~of a Shared Cyber Infrastructure or Electronic Access Control or Monitoring System~~ that:

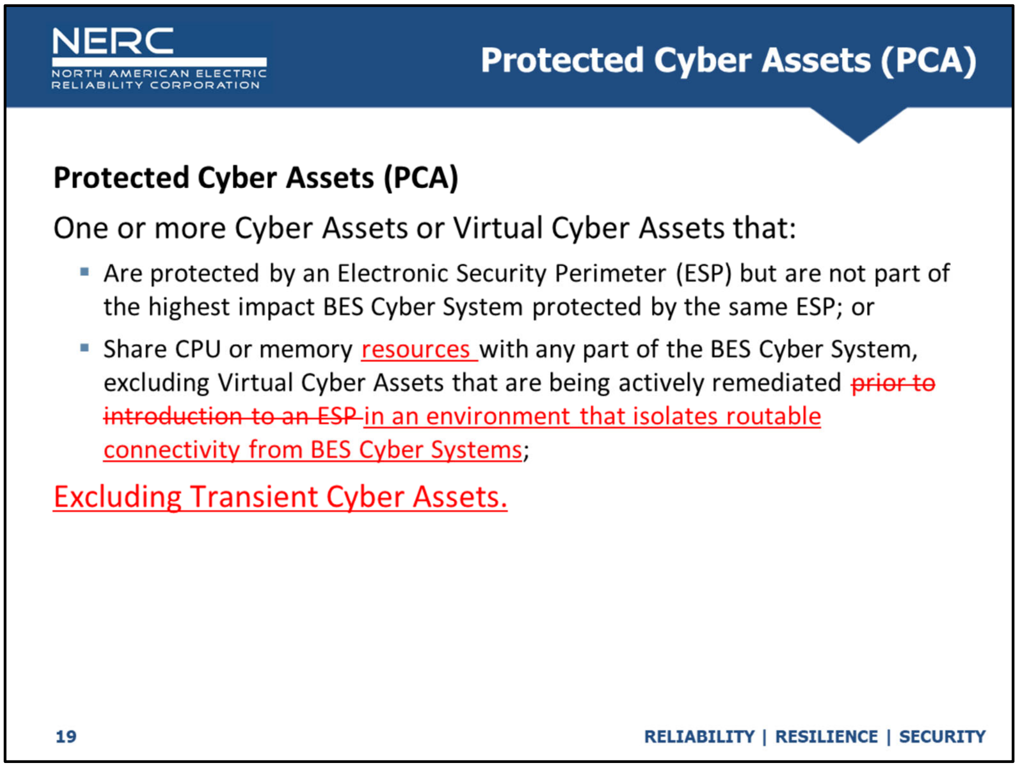
- Controls the processes of initializing, deploying, and configuring Shared Cyber Infrastructure; or
- Is an autonomous subsystem that provides access to ~~power management or~~ the console independently of the host system's CPU, firmware, and operating system; or
- Configures an Electronic Security Perimeter.

~~Physical user interfaces are excluded (e.g., power switch, touch panel, etc.).~~

18

RELIABILITY | RESILIENCE | SECURITY

For Management Interface, we pulled the specific scope out along the lines of our philosophy and its use is scoped in requirements. Beyond that, we received comments that the power mgt functions and power switches added more confusion than they provided clarity, so we removed those. We're really talking about a *management* interface, typically a 'console', where a user can configure the functionality.


NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Protected Cyber Assets (PCA)

Protected Cyber Assets (PCA)

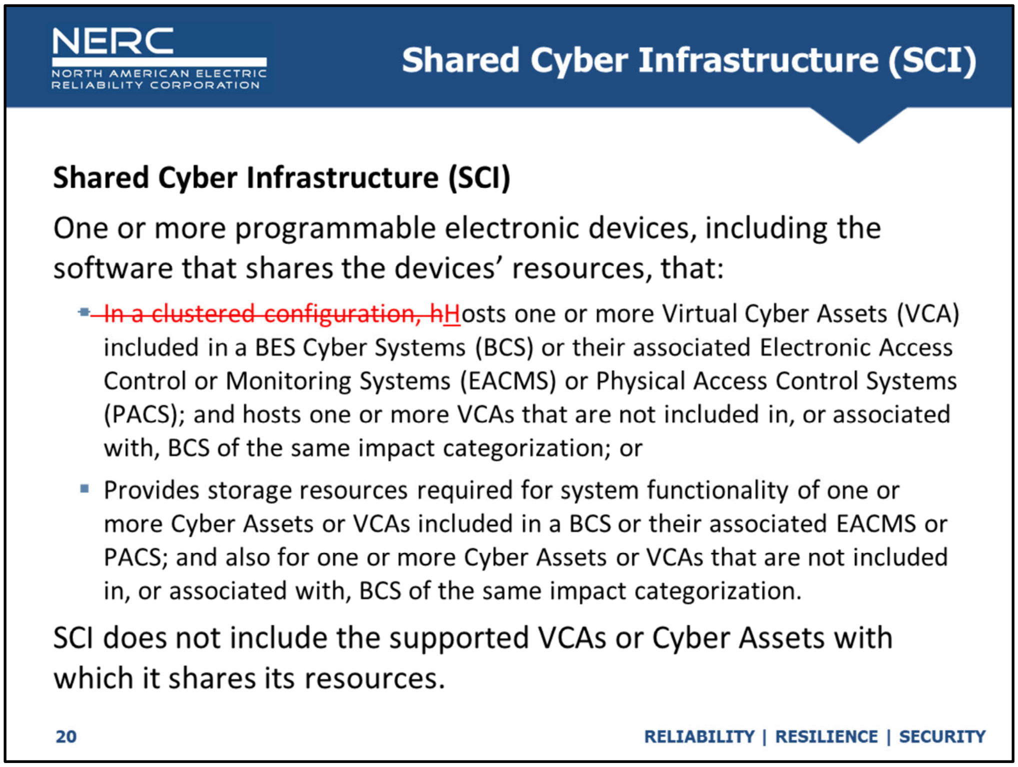
One or more Cyber Assets or Virtual Cyber Assets that:

- Are protected by an Electronic Security Perimeter (ESP) but are not part of the highest impact BES Cyber System protected by the same ESP; or
- Share CPU or memory resources with any part of the BES Cyber System, excluding Virtual Cyber Assets that are being actively remediated ~~prior to introduction to an ESP~~ in an environment that isolates routable connectivity from BES Cyber Systems;

Excluding Transient Cyber Assets.

19 RELIABILITY | RESILIENCE | SECURITY

Protected Cyber Assets, in general, are those things that due to their proximity and potential for access to a BCS (a pivot point) are therefore treated like a BCS. There are now TWO forms of that proximity. The first bullet is the traditional network peer and is unchanged. Virtualization allows for a "hardware peer"; another cyber system sharing and executing on the same hardware as the BCS. Thus the addition of the 2nd bullet. We received some comments on the specificity of the terms CPU and memory, and we discussed at length how we could point to this risk in another way and we think this is still the best, most concise way we can define this. We did add the word 'resources' to point to CPU and memory resources rather than simply CPU and memory as a result of discussions around continued innovation in hardware and the various ways you can "carve up" and partition underlying HW these days even down to cores. Next, you'll see this is one of the places where we addressed the comments about needing more description and clarity around remediation VLANs. We used "Prior to introduction to the ESP" in the last draft and that wasn't at the level of clarity needed, so you'll now see this "in an environment that isolates routable connectivity from the BCS" as a much more descriptive phrase concerning remediation VLANs and similar technology. Finally, we explicitly stated that a TCA, while temporarily connected, does not become a PCA for that duration.



NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Shared Cyber Infrastructure (SCI)

Shared Cyber Infrastructure (SCI)

One or more programmable electronic devices, including the software that shares the devices' resources, that:

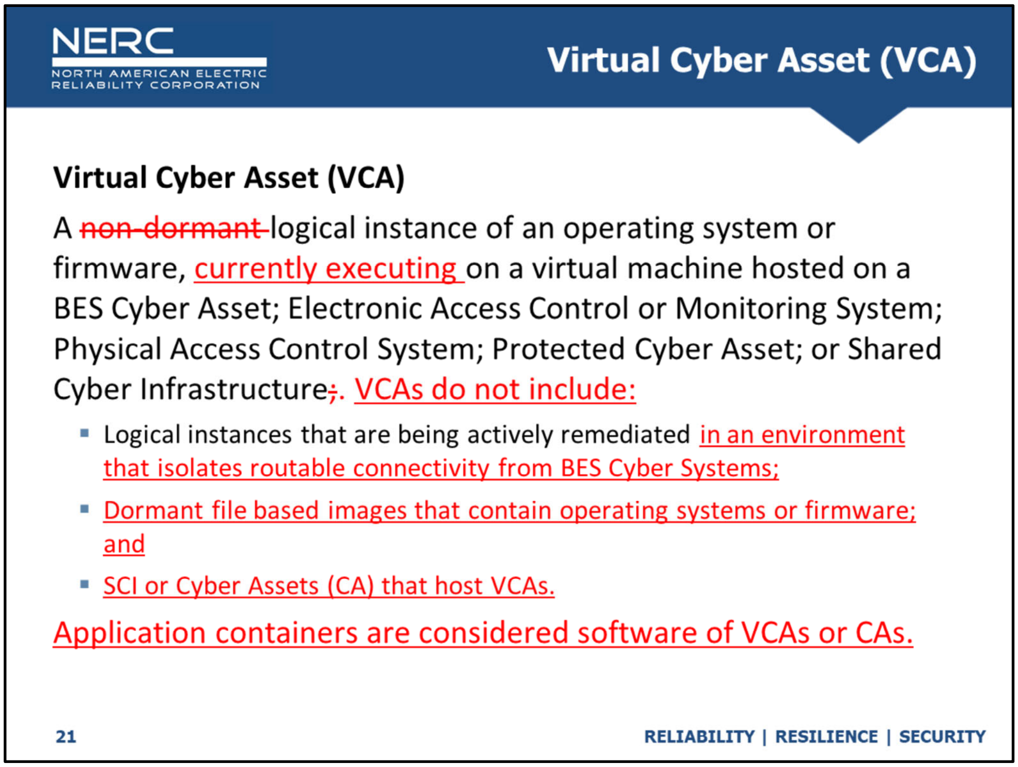
- ~~In a clustered configuration, h~~Hosts one or more Virtual Cyber Assets (VCA) included in a BES Cyber Systems (BCS) or their associated Electronic Access Control or Monitoring Systems (EACMS) or Physical Access Control Systems (PACS); and hosts one or more VCAs that are not included in, or associated with, BCS of the same impact categorization; or
- Provides storage resources required for system functionality of one or more Cyber Assets or VCAs included in a BCS or their associated EACMS or PACS; and also for one or more Cyber Assets or VCAs that are not included in, or associated with, BCS of the same impact categorization.

SCI does not include the supported VCAs or Cyber Assets with which it shares its resources.

20

RELIABILITY | RESILIENCE | SECURITY

SCI, from your comments, seems to be in a good place, the comments were more around wanting guidance for implementation rather than issues with the definition itself. The only change we made here was to remove the 'in a clustered configuration'. We had put that in draft 3 to help clarify, but its really an example – and we found it opened a gap. If I have a single hypervisor and host two VCAs of different impact levels on it, and I employ some CPU/memory compartmentalization to avoid them being PCAs, then it completely fell out of the definition of SCI because one hypervisor does not a cluster make. A very niche scenario, but we struck that phrase to not have that gap.



NERC NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Virtual Cyber Asset (VCA)

Virtual Cyber Asset (VCA)

A ~~non-dormant~~ logical instance of an operating system or firmware, currently executing on a virtual machine hosted on a BES Cyber Asset; Electronic Access Control or Monitoring System; Physical Access Control System; Protected Cyber Asset; or Shared Cyber Infrastructure~~;~~. VCAs do not include:

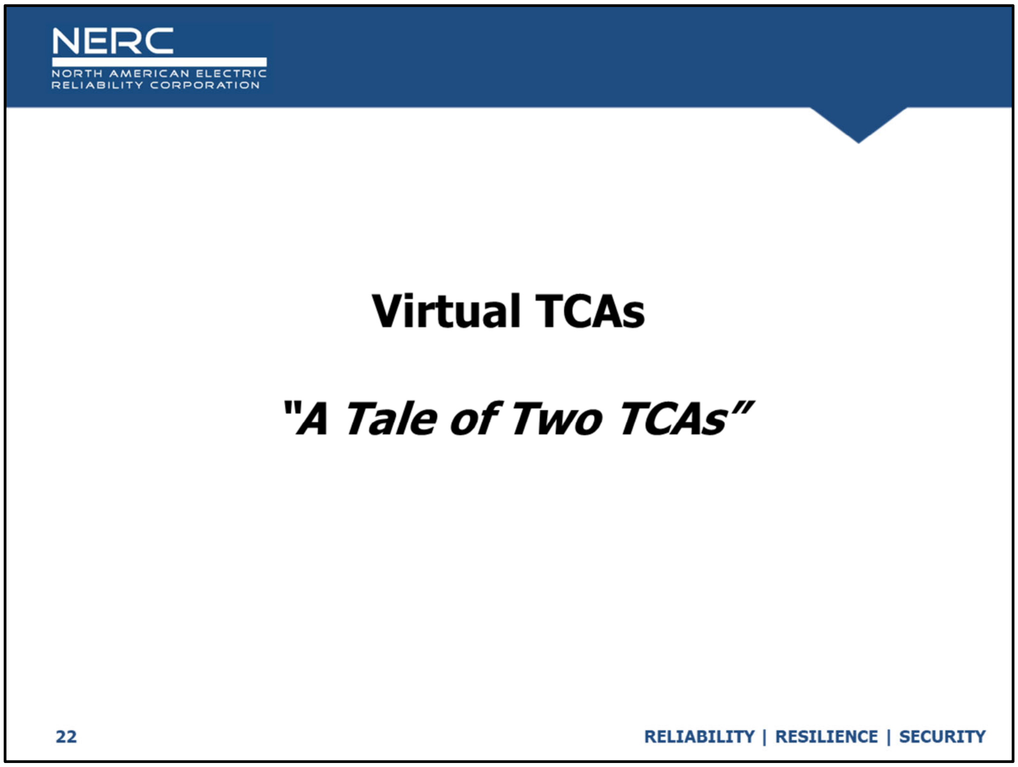
- Logical instances that are being actively remediated in an environment that isolates routable connectivity from BES Cyber Systems;
- Dormant file based images that contain operating systems or firmware; and
- SCI or Cyber Assets (CA) that host VCAs.

Application containers are considered software of VCAs or CAs.

21 RELIABILITY | RESILIENCE | SECURITY

And finally in our draft 3 to 4 changes to definitions, we have VCA. One comment theme was we understand a dormant VCA, but the phrase 'non-dormant' simply meaning "not that" wasn't clear. So we replaced 'non dormant' with 'currently executing' which is more precise. Then we added or modified three bullets of what a VCA is not. The first bullet uses our more descriptive language for remediation VLAN environments. So a VCA is not a instance being remediated moments before it does become a VCA, or a dormant file image, or the hardware underneath it. It is the logical instance, while it is executing and performing its function. Then, just as in the CA definition, we clarified that application containers are software, not a VCA in and of themselves.

Now, you may be thinking "look at all that SCOPE in this definition!" BCA, EACMS, PACS, PCA, SCI – why is all that in there and why did you not just say Cyber Systems. In this case, those are the things that can host VCAs and its not all cyber systems - there is one type missing – a TCA and that is on purpose and was another comment theme; that a VCA on a TCA should be considered another TCA.

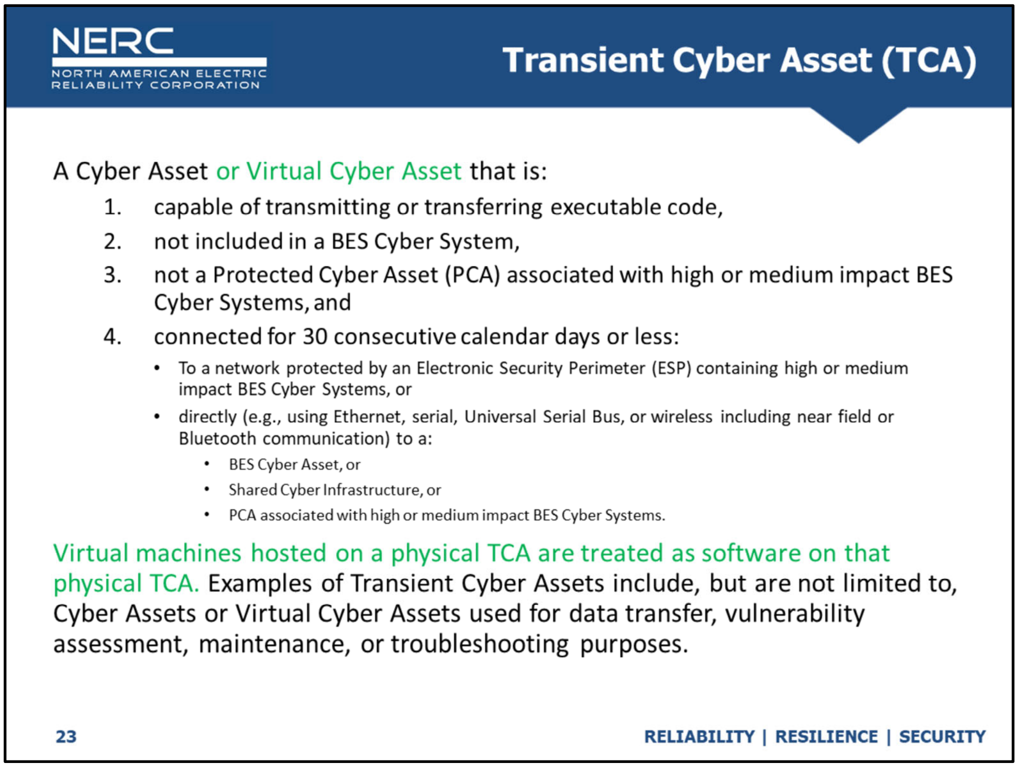


NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Virtual TCAs

"A Tale of Two TCAs"

Which is our segue into the next topic of Virtual TCAs that I've titled "a tale of two TCAs". There are two types and we are distinguishing between them.



NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

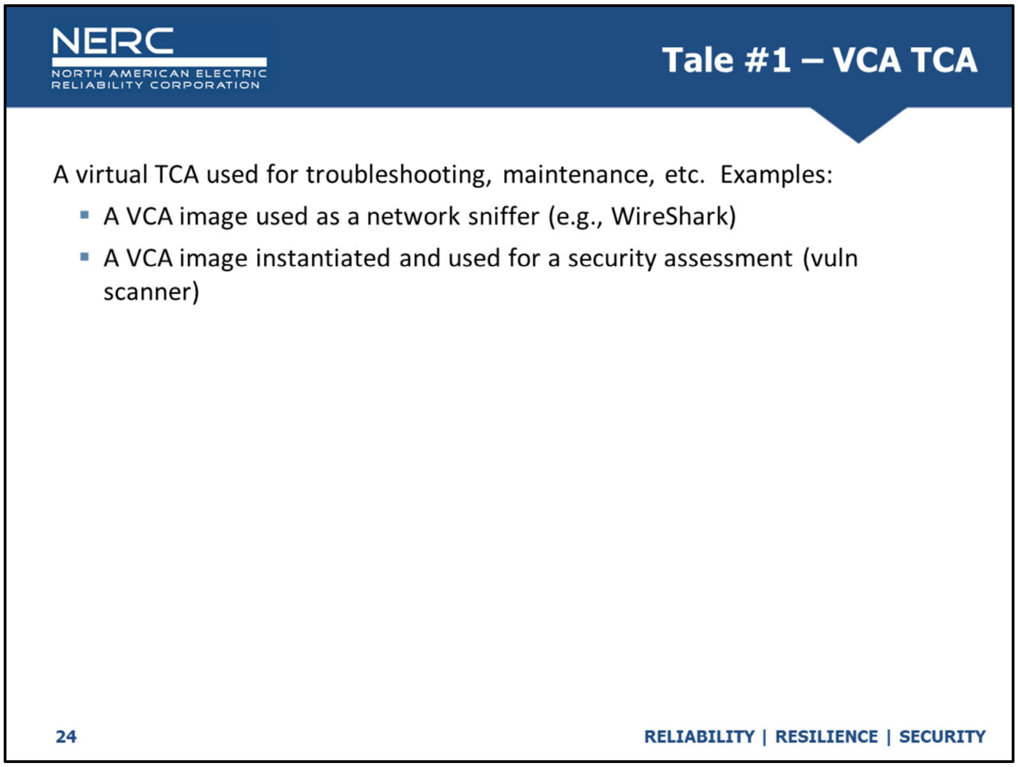
Transient Cyber Asset (TCA)

A Cyber Asset or Virtual Cyber Asset that is:

1. capable of transmitting or transferring executable code,
2. not included in a BES Cyber System,
3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and
4. connected for 30 consecutive calendar days or less:
   - To a network protected by an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or
   - directly (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) to a:
     - BES Cyber Asset, or
     - Shared Cyber Infrastructure, or
     - PCA associated with high or medium impact BES Cyber Systems.

Virtual machines hosted on a physical TCA are treated as software on that physical TCA. Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets or Virtual Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Jay
No changes from Draft 3 so no redline. This slide is to talk about the comments received on VCA TCAs and the green text it involves.



NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

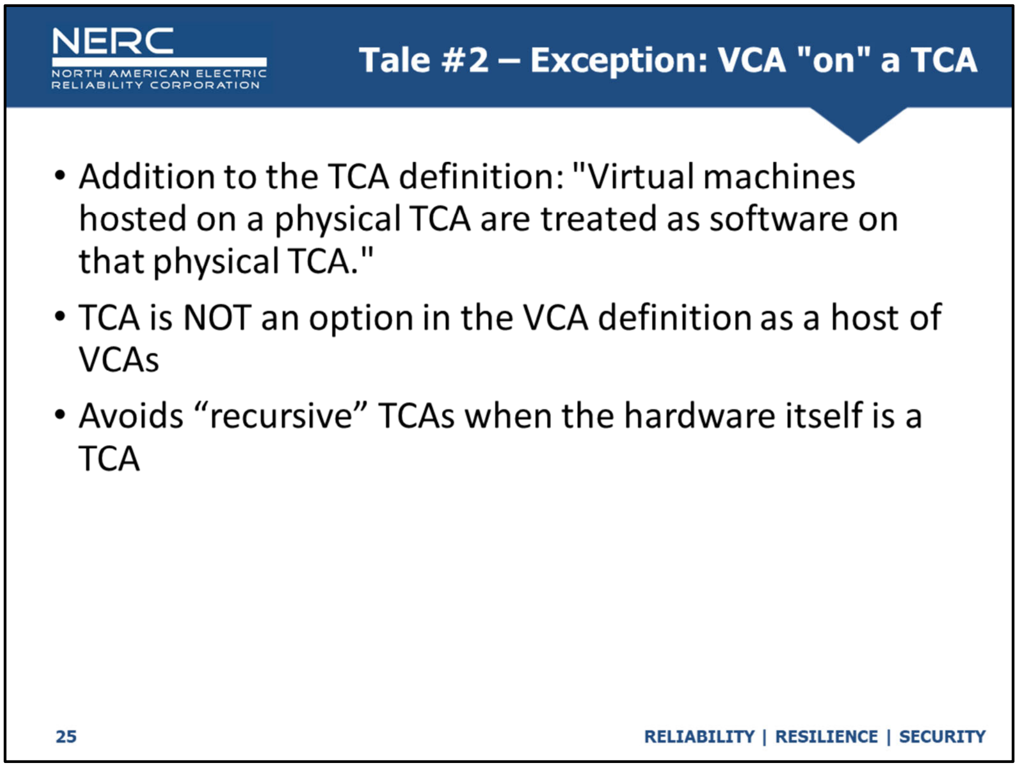
Tale #1 – VCA TCA

A virtual TCA used for troubleshooting, maintenance, etc. Examples:

- A VCA image used as a network sniffer (e.g., WireShark)
- A VCA image instantiated and used for a security assessment (vuln scanner)

Let’s begin with our current proposed definition of TCA. We’ve not made any changes since the last draft, so the green text is just for emphasis. In the first line, we state that a TCA can be a VCA, it can be virtual in form. Then the green sentence below the bullets has one exception – VMs hosted on a physical TCA are treated as software on that physical TCA. Why? Let’s tell the tale of two, “boots on the ground” examples.

Tale #1 begins in a control center’s big data center with racks and racks of hardware as a resource pool, an underlay on top of which the systems, networks, and storage of a BCS are configured virtually. The entity, in order to troubleshoot network problems in this all-virtual environment, creates another VM image say with linux and wireshark, a network sniffer, and this image lives in the environment but is only instantiated on rare occasions. When they need to troubleshoot a network, they instantiate that image on the virtual network, it becomes a VCA *in form* and a TCA *in function*, analogous to the old days with the huge luggable HW sniffers that you physically plugged in and captured packets. This is a VCA TCA. Another example we’ve heard of is a vendor providing security assessment services sends you a VM image to instantiate in your environment, let it run a few hours, then send them the data it collected for analysis. Another VCA TCA.



NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

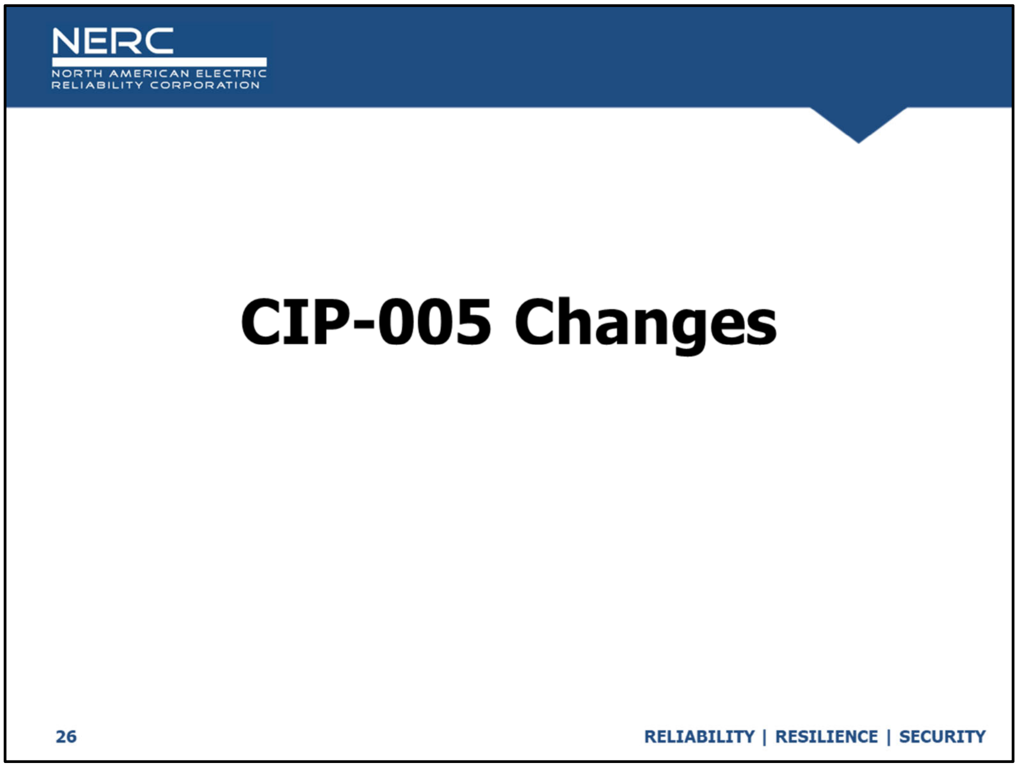
Tale #2 – Exception: VCA "on" a TCA

- Addition to the TCA definition: "Virtual machines hosted on a physical TCA are treated as software on that physical TCA."
- TCA is NOT an option in the VCA definition as a host of VCAs
- Avoids "recursive" TCAs when the hardware itself is a TCA

25 RELIABILITY | RESILIENCE | SECURITY

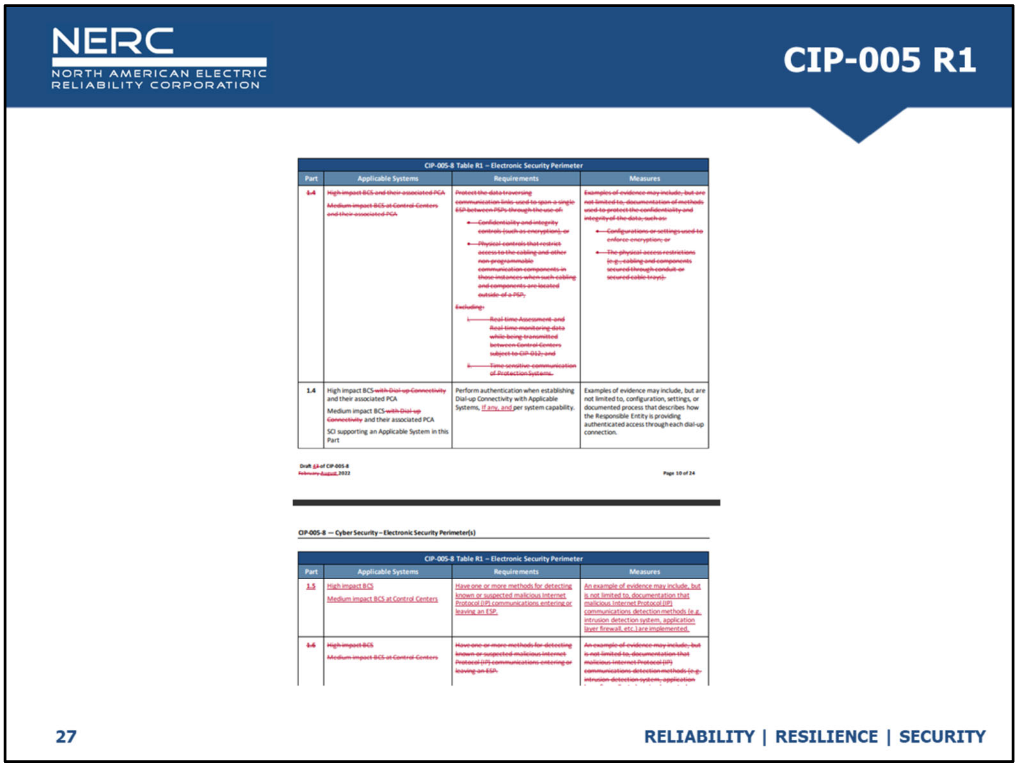
Tale #2 is about that green sentence concerning VCAs on physical TCAs. Go with me to a plant site that's been around for a few decades and you are an I&C tech. The HRSG duct burner flame detector isn't working quite right and you need to go check it. Now that detector came with a small piece of software for talking to it. This little piece of software is anti the definition of 'common off the shelf'. It is for that model duct burner flame detector from that vendor. And…its old enough that its 32 bit software and won't run on today's 64 bit OS. So you have it in a VM image file with a 32 bit OS so that you can actually execute it and fix the flame detector, and you run it with some form of 'vm player' on the TCA laptop. So you the technician, go over to the I&C shop and check out one of the plant's physical TCA laptops that has this on it. That's the magic moment we have to think about when writing this standard. You the technician are going to check out a tool, in this case a TCA laptop, in order to go do your job – fix the flame detector. Nobody is thinking, nor we say should they be thinking, that no, you are actually checking out multiple different TCAs. Our position is it should not be a cyber security regulatory violation if your documentation doesn't show that you checked out several TCAs when you grabbed that one laptop to go get the duct burner working. If you are authorized to use the TCA laptop, you shouldn't need a separate authorization to use the software tool on the laptop simply because it needs to run in a VM player. Treat it as software on the physical TCA because that's what it is, its just having to run on an emulation layer in order to work. We're not out to create a recursive TCA tangle, and that is the "why" behind this statement in this definition.

So that is a recap of the changes we've made to the definitions in response to draft 3 comments. With that, I'll turn it over to Scott Klauminzer for our next section.



CIP-005 Changes

Thank you, Jay!
Next slide please


NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-005 R1

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	Applicable Systems	Requirements	Measures
~~1.4~~	~~High impact BCS and their associated PCA~~ ~~Medium impact BCS at Control Centers and their associated PCA~~	~~Protect the data traversing communication links used to span a single ESP between PSPs through the use of:~~ ~~• Confidentiality and integrity controls (such as encryption), or~~ ~~• Physical controls that restrict access to the cabling and other non-programmable communication components in those instances when such cabling and components are located outside of a PSP,~~ ~~Excluding:~~ ~~i. Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012; and~~ ~~ii. Time sensitive communication of Protection Systems.~~	~~Examples of evidence may include, but are not limited to, documentation of methods used to protect the confidentiality and integrity of the data, such as:~~ ~~• Configurations or settings used to enforce encryption; or~~ ~~• The physical access restrictions (e.g., cabling and components secured through conduit or secured cable trays).~~
1.4	High impact BCS ~~with Dial-up Connectivity~~ and their associated PCA Medium impact BCS ~~with Dial-up Connectivity~~ and their associated PCA SCI supporting an Applicable System in this Part	Perform authentication when establishing Dial-up Connectivity with Applicable Systems, if any, and per system capability.	Examples of evidence may include, but are not limited to, configuration, settings, or documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.

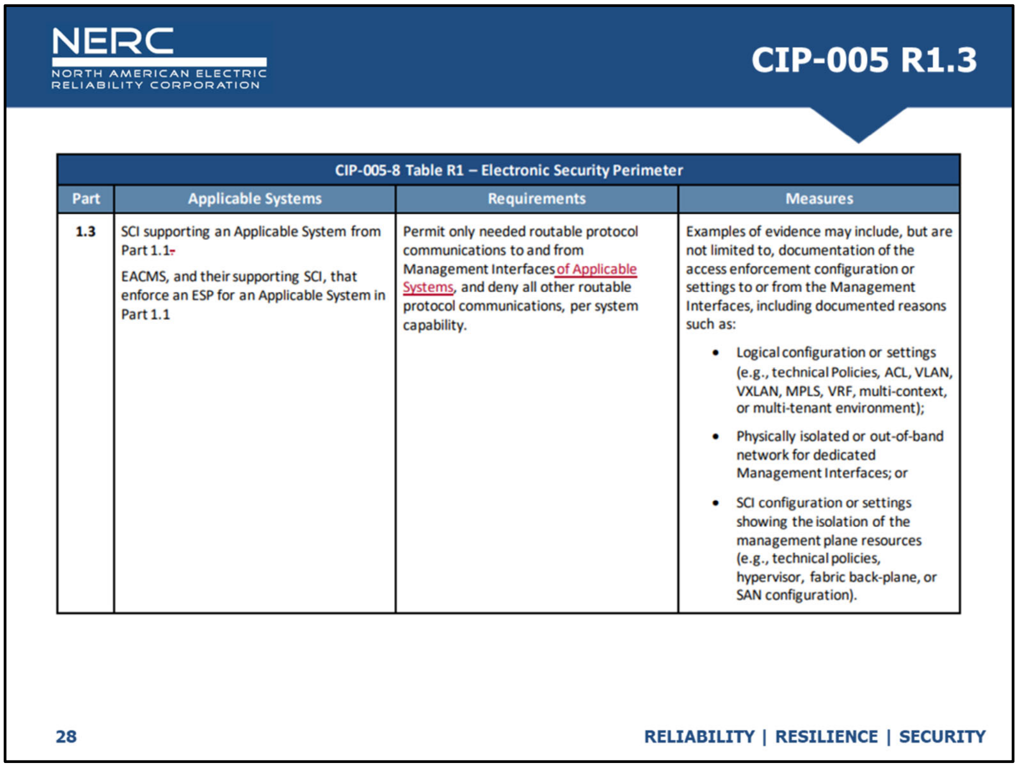
Draft 2~~1~~ of CIP-005-8
~~February~~ August 2022

Page 10 of 24

CIP-005-8 — Cyber Security – Electronic Security Perimeter(s)

CIP-005-8 Table R1 – Electronic Security Perimeter			
Part	Applicable Systems	Requirements	Measures
1.5	High impact BCS Medium impact BCS at Control Centers	Have one or more methods for detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving an ESP.	An example of evidence may include, but is not limited to, documentation that malicious Internet Protocol (IP) communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.
~~1.6~~	~~High impact BCS~~ ~~Medium impact BCS at Control Centers~~	~~Have one or more methods for detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving an ESP.~~	~~An example of evidence may include, but is not limited to, documentation that malicious Internet Protocol (IP) communications detection methods (e.g. intrusion detection system, application~~

In CIP-005 R1, most of the redline here comes from a change in response to comments to move the new requirement part in R1 to the end of the Requirement Parts, to avoid renumbering 1.4 – 1.6. So, the red on screen here actually reverts much of the language to the approved.



NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

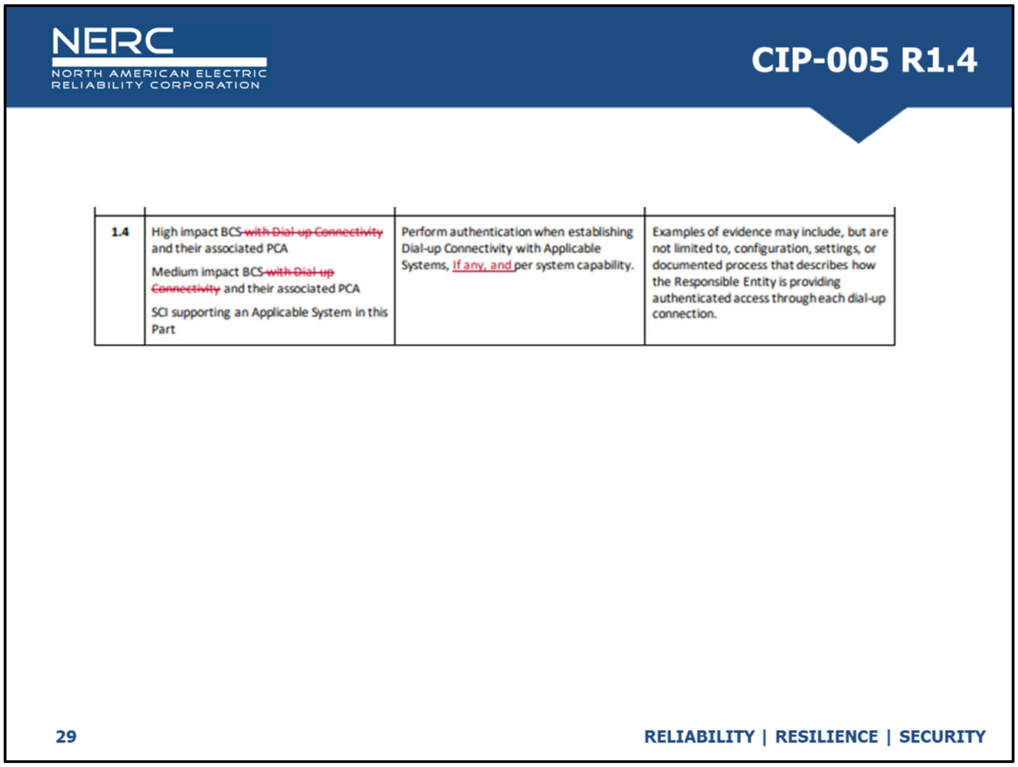
CIP-005 R1.3

CIP-005-8 Table R1 – Electronic Security Perimeter

Part	Applicable Systems	Requirements	Measures
1.3	SCI supporting an Applicable System from Part 1.1~~.~~ EACMS, and their supporting SCI, that enforce an ESP for an Applicable System in Part 1.1	Permit only needed routable protocol communications to and from Management Interfaces of Applicable Systems, and deny all other routable protocol communications, per system capability.	Examples of evidence may include, but are not limited to, documentation of the access enforcement configuration or settings to or from the Management Interfaces, including documented reasons such as: • Logical configuration or settings (e.g., technical Policies, ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); • Physically isolated or out-of-band network for dedicated Management Interfaces; or • SCI configuration or settings showing the isolation of the management plane resources (e.g., technical policies, hypervisor, fabric back-plane, or SAN configuration).

28 RELIABILITY | RESILIENCE | SECURITY

In CIP-005 R1 Part 1.3, the insertion of “Applicable Systems” in the requirement language is to reinforce how the scope of the requirement is defined by the Applicable Systems column. While Management Interfaces will exist in many places, it is only on those Applicable Systems that we must permit only needed routable protocol communications. This requirement part does not apply to anything not specifically called out in the Applicable Systems Column, which in this case is limited to the SCI Supporting an Applicable System from Part 1.1 (and not to the Applicable Systems of Part 1.1 themselves) and EACMS that enforce an ESP.



NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

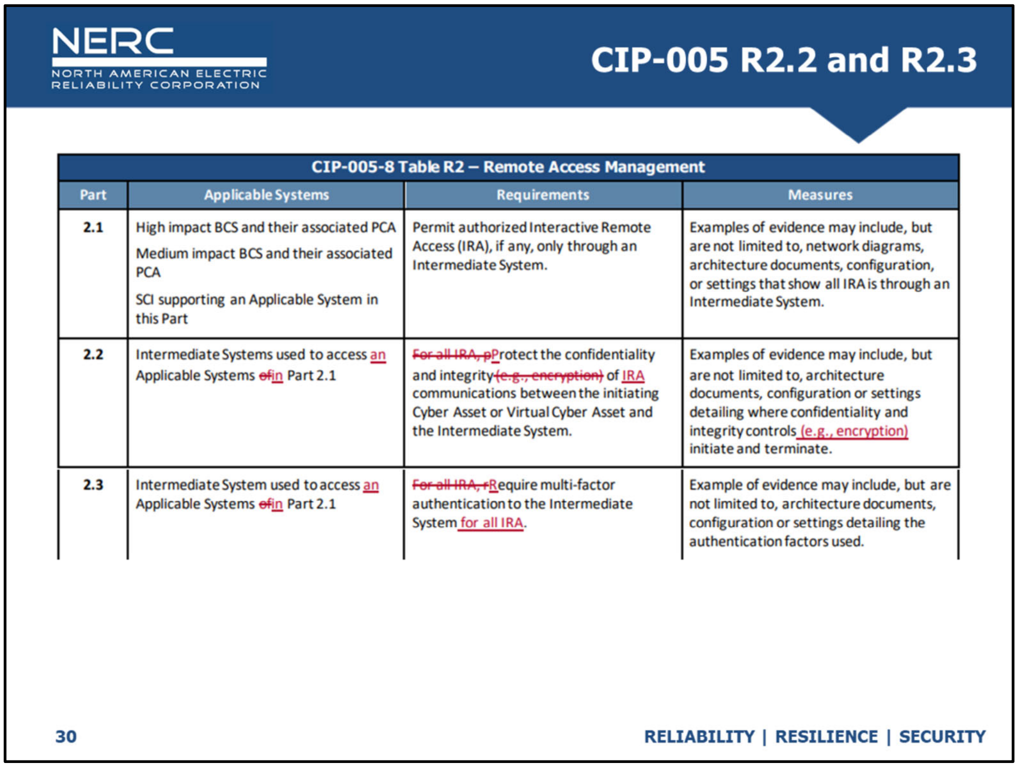
CIP-005 R1.4

1.4	High impact BCS ~~with Dial-up Connectivity~~ and their associated PCA Medium impact BCS ~~with Dial-up Connectivity~~ and their associated PCA SCI supporting an Applicable System in this Part	Perform authentication when establishing Dial-up Connectivity with Applicable Systems, If any, and per system capability.	Examples of evidence may include, but are not limited to, configuration, settings, or documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.

29

RELIABILITY | RESILIENCE | SECURITY

The SDT chose to move the Applicable Systems scoping language "with Dial-up Connectivity" to the requirement language through the inclusion of "if any". This change was required to eliminate any ambiguity of whether the SCI or the BCS (or both?) must have Dial-up communications to be applicable through the inclusion of the "SCI supporting an Applicable System in this Part" language.



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

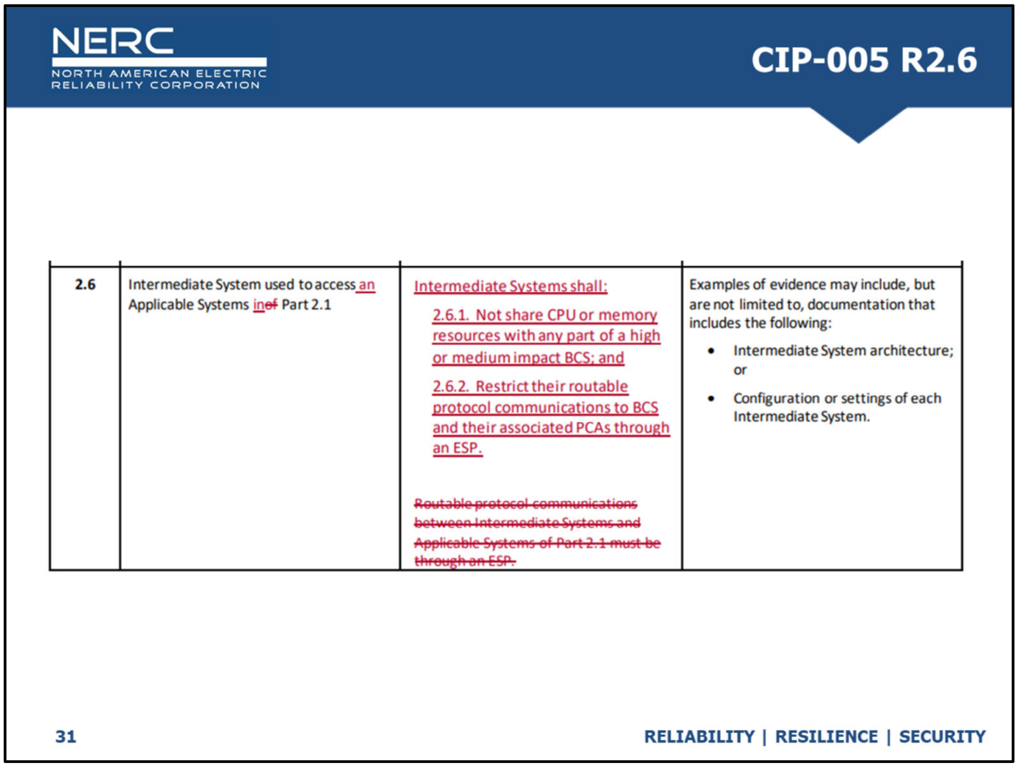
CIP-005 R2.2 and R2.3

CIP-005-8 Table R2 – Remote Access Management

Part	Applicable Systems	Requirements	Measures
2.1	High impact BCS and their associated PCA Medium impact BCS and their associated PCA SCI supporting an Applicable System in this Part	Permit authorized Interactive Remote Access (IRA), if any, only through an Intermediate System.	Examples of evidence may include, but are not limited to, network diagrams, architecture documents, configuration, or settings that show all IRA is through an Intermediate System.
2.2	Intermediate Systems used to access an Applicable Systems ~~of~~in Part 2.1	~~For all IRA, p~~Protect the confidentiality and integrity ~~(e.g., encryption)~~ of IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.	Examples of evidence may include, but are not limited to, architecture documents, configuration or settings detailing where confidentiality and integrity controls (e.g., encryption) initiate and terminate.
2.3	Intermediate System used to access an Applicable Systems ~~of~~in Part 2.1	~~For all IRA, r~~Require multi-factor authentication to the Intermediate System for all IRA.	Example of evidence may include, but are not limited to, architecture documents, configuration or settings detailing the authentication factors used.

30 RELIABILITY | RESILIENCE | SECURITY

Most of the minor changes in CIP-005 R2 are to align the language of the requirements to begin with a verb, as in Permit, or Protect, or Require… and then to move the example (of encryption) to a measure.



NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

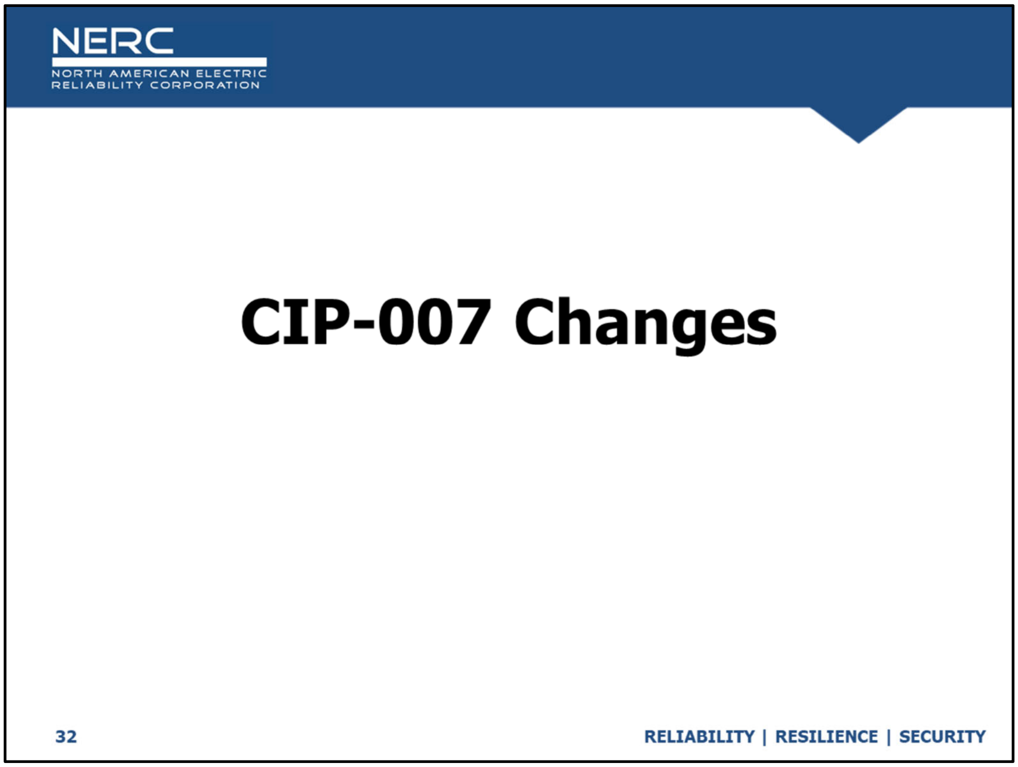
CIP-005 R2.6

2.6	Intermediate System used to access an Applicable Systems in~~of~~ Part 2.1	Intermediate Systems shall: 2.6.1. Not share CPU or memory resources with any part of a high or medium impact BCS; and 2.6.2. Restrict their routable protocol communications to BCS and their associated PCAs through an ESP. ~~Routable protocol communications between Intermediate Systems and Applicable Systems of Part 2.1 must be through an ESP.~~	Examples of evidence may include, but are not limited to, documentation that includes the following: • Intermediate System architecture; or • Configuration or settings of each Intermediate System.

31

RELIABILITY | RESILIENCE | SECURITY

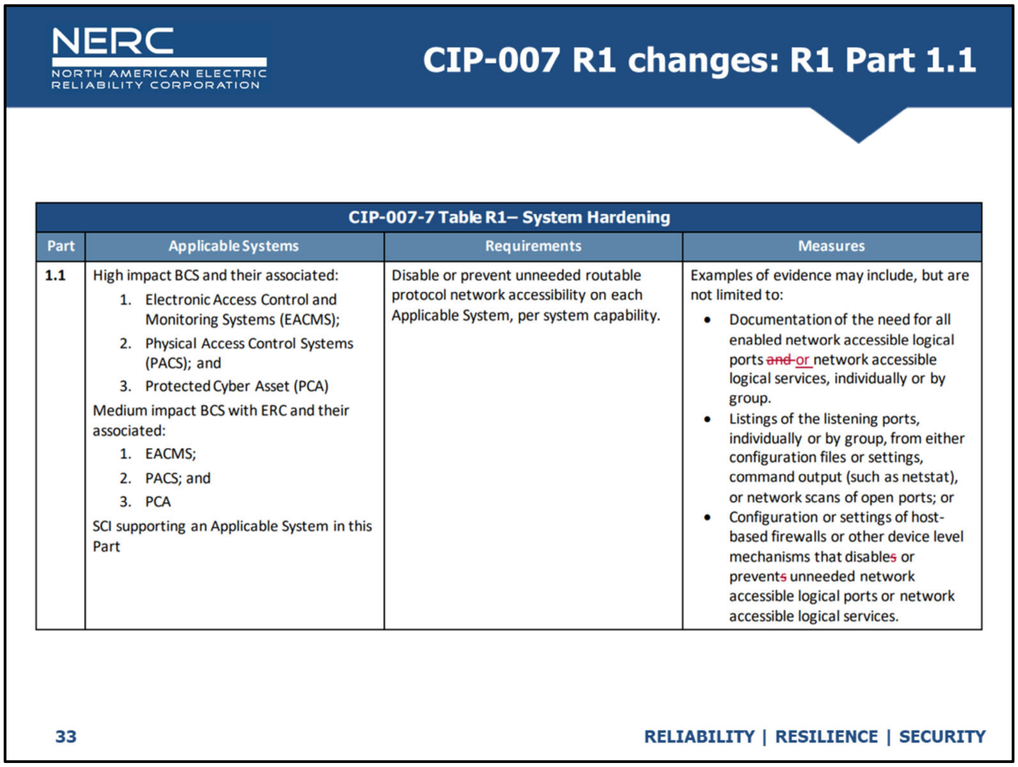
With this requirement language in 2.6.1 the PCA definition cannot apply to an IS, regarding CPU and memory sharing. This Requirement Part addresses the high-risk scenario of an Internet facing system also hosting a high or medium impact BES Cyber System. Additionally, with the modifications to Intermediate System definition, the requirement like language for where the IS must be placed in relation to the BCS was added to Requirement Part 2.6.2 to remove this definition based implied requirement, and aid in clarity.



NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP-007 Changes

Now CIP-007 there are a couple of minor changes from draft 3.



NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

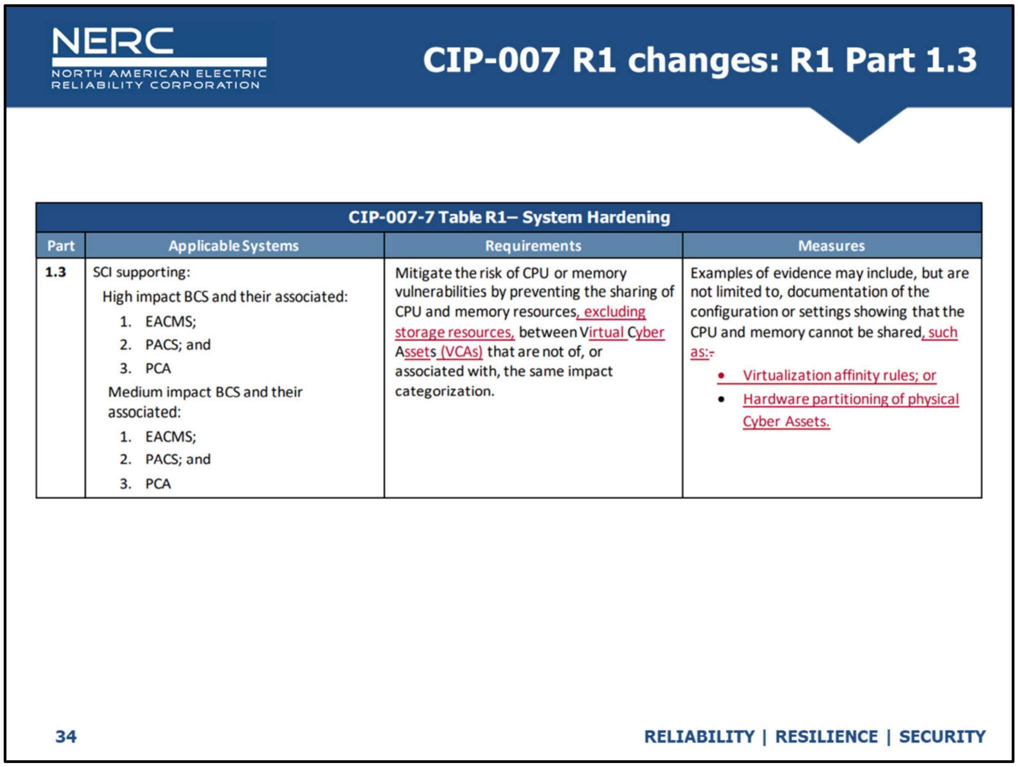
CIP-007 R1 changes: R1 Part 1.1

CIP-007-7 Table R1– System Hardening

Part	Applicable Systems	Requirements	Measures
1.1	High impact BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); 2. Physical Access Control Systems (PACS); and 3. Protected Cyber Asset (PCA) Medium impact BCS with ERC and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled network accessible logical ports ~~and~~ or network accessible logical services, individually or by group. • Listings of the listening ports, individually or by group, from either configuration files or settings, command output (such as netstat), or network scans of open ports; or • Configuration or settings of host-based firewalls or other device level mechanisms that disable~~s~~ or prevent~~s~~ unneeded network accessible logical ports or network accessible logical services.

The first change is found within Requirement 1 Part 1.1 where the first measure has been modified to clearly show the intended implementation options. You can see in the first Measure that we changed “and” to “or” between the list of network accessible ports and network accessible services. This removed the implication of possibly needing to provide BOTH a list of ports, AND a list of services.

Additionally, we received comments that indicated there was some confusion about the level at which routable protocol network accessibility is to be controlled. The SDT would like to clarify how the language of the requirement makes it clear that the requirement must be performed ON each Applicable System, as opposed to somewhere not “on” each Applicable System, such as the network. CIP-005 R1 Controls typically will not serve CIP-007 R1 Part 1.1, except in scenarios like zero-trust, where controls are applied “on” the Applicable Systems as well as other locations in the security architecture.



NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP-007 R1 changes: R1 Part 1.3

CIP-007-7 Table R1– System Hardening

Part	Applicable Systems	Requirements	Measures
1.3	SCI supporting: High impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA	Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU and memory resources, excluding storage resources, between Virtual Cyber Assets (VCAs) that are not of, or associated with, the same impact categorization.	Examples of evidence may include, but are not limited to, documentation of the configuration or settings showing that the CPU and memory cannot be shared, such as:~~.~~ • Virtualization affinity rules; or • Hardware partitioning of physical Cyber Assets.

34

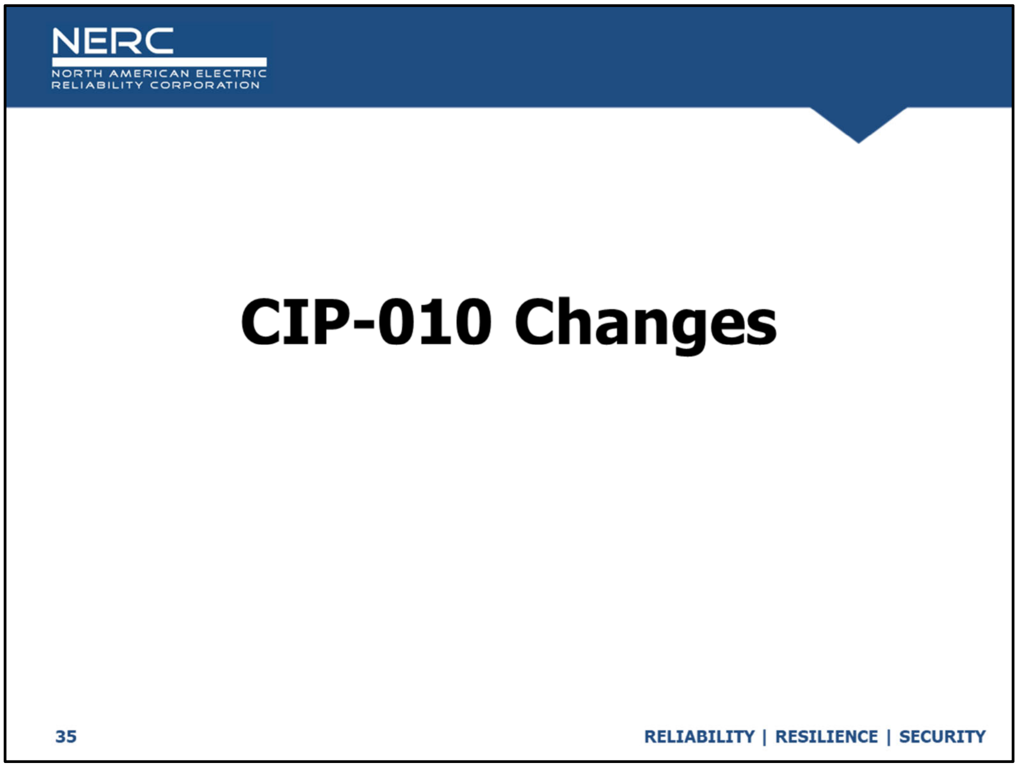
RELIABILITY | RESILIENCE | SECURITY

The Second location that was changed in CIP-007 R1 is found within Part 1.3, where the SDT added an exclusion for storage resources, to clarify that SCI Storage resources are NOT considered memory resources for this requirement part. Excluding storage resources in this way ensures that non-volatile storage resources are not considered part of the memory resources that must not be shared with differing impact levels.

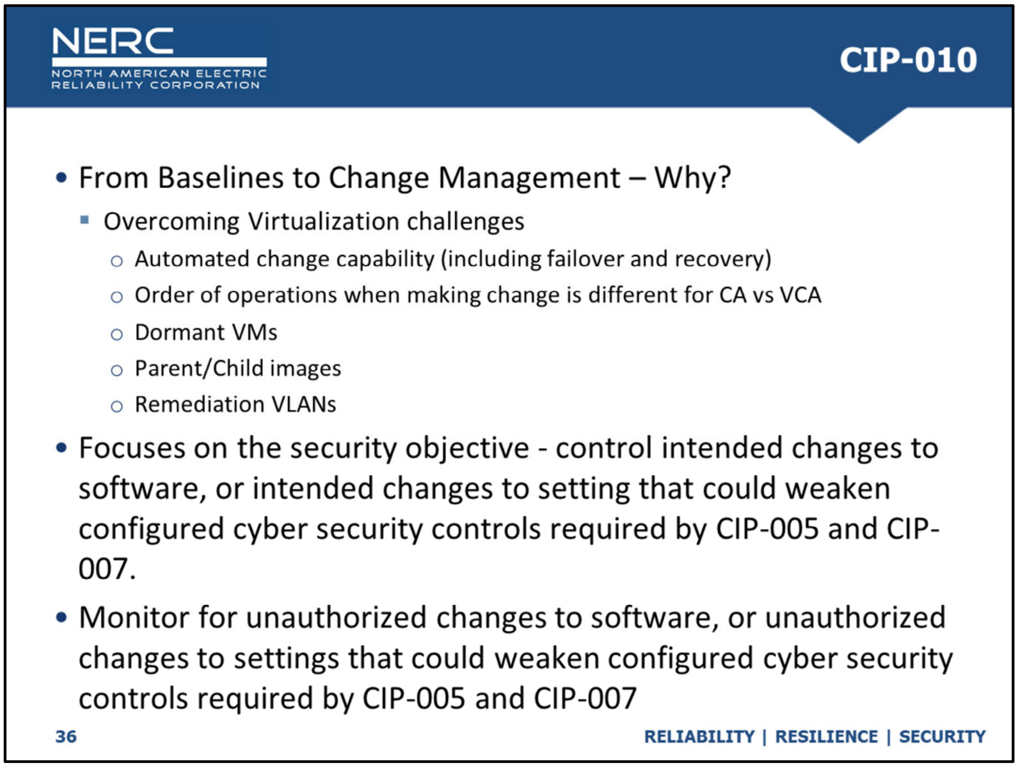
Since this requirement is meant to address the risk of side channel attack, and the vulnerability is typically not present in storage systems, the exclusion does not negatively affect the security of the Standard.

The SDT also provided additional clarity in the measures column for virtualization affinity rules or other hardware partitioning schemes in order to ensure that alternate methods which achieve the objective of the Requirement are considered.

And now I'll pass it off to Norm

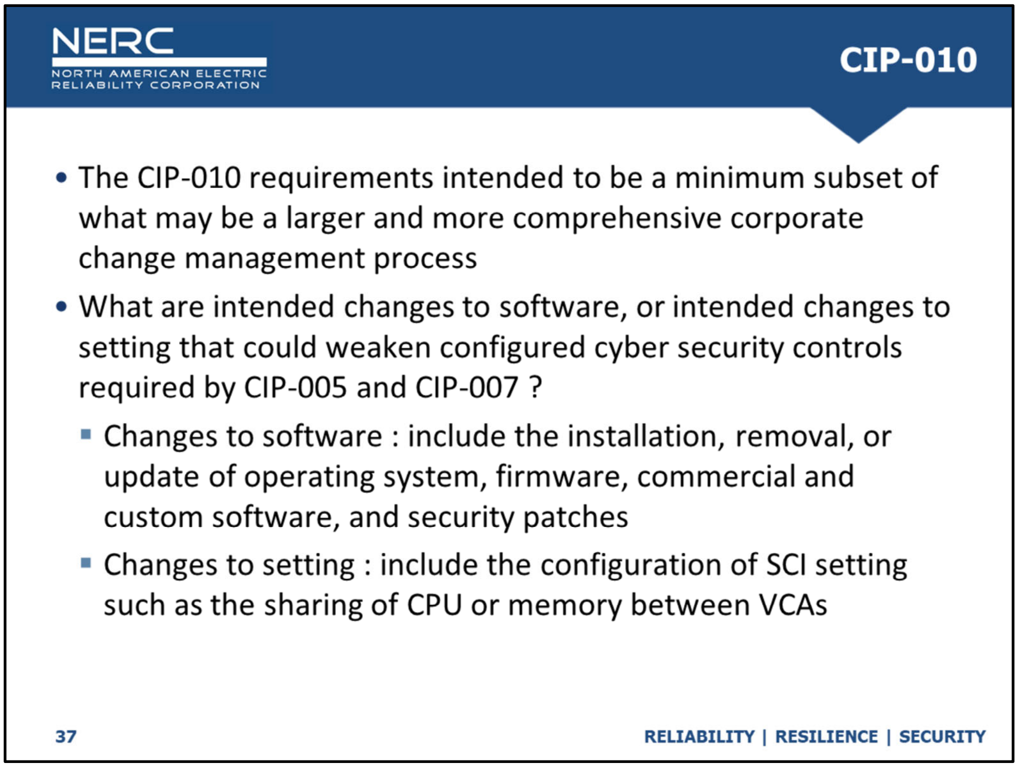


CIP-010 Changes



CIP-010

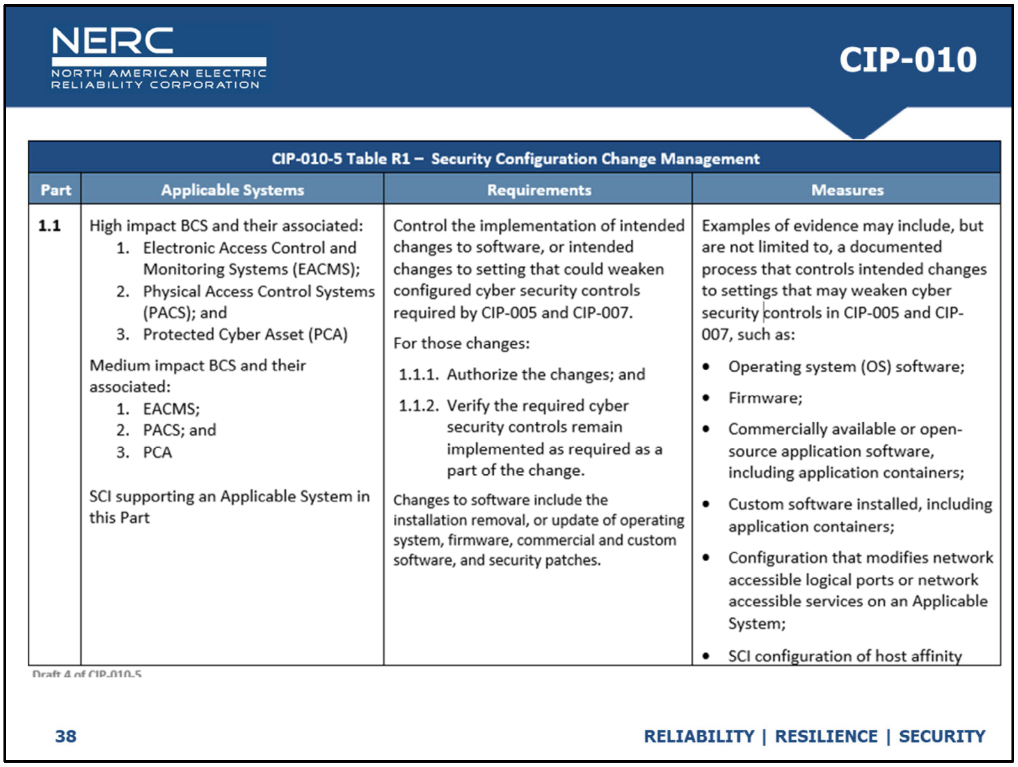
- From Baselines to Change Management – Why?
  - Overcoming Virtualization challenges
    - Automated change capability (including failover and recovery)
    - Order of operations when making change is different for CA vs VCA
    - Dormant VMs
    - Parent/Child images
    - Remediation VLANs
- Focuses on the security objective - control intended changes to software, or intended changes to setting that could weaken configured cyber security controls required by CIP-005 and CIP-007.
- Monitor for unauthorized changes to software, or unauthorized changes to settings that could weaken configured cyber security controls required by CIP-005 and CIP-007



NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP-010

- The CIP-010 requirements intended to be a minimum subset of what may be a larger and more comprehensive corporate change management process
- What are intended changes to software, or intended changes to setting that could weaken configured cyber security controls required by CIP-005 and CIP-007 ?
  - Changes to software : include the installation, removal, or update of operating system, firmware, commercial and custom software, and security patches
  - Changes to setting : include the configuration of SCI setting such as the sharing of CPU or memory between VCAs

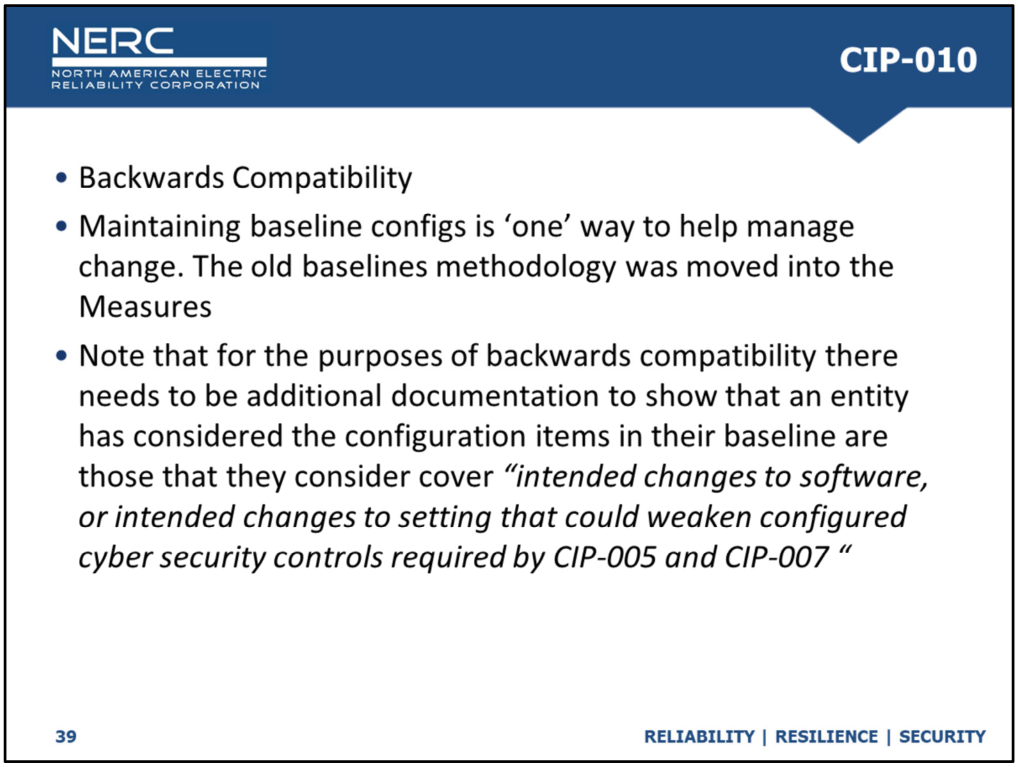


NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-010

CIP-010-5 Table R1 – Security Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High impact BCS and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); 2. Physical Access Control Systems (PACS); and 3. Protected Cyber Asset (PCA) Medium impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI supporting an Applicable System in this Part	Control the implementation of intended changes to software, or intended changes to setting that could weaken configured cyber security controls required by CIP-005 and CIP-007. For those changes: 1.1.1. Authorize the changes; and 1.1.2. Verify the required cyber security controls remain implemented as required as a part of the change. Changes to software include the installation removal, or update of operating system, firmware, commercial and custom software, and security patches.	Examples of evidence may include, but are not limited to, a documented process that controls intended changes to settings that may weaken cyber security controls in CIP-005 and CIP-007, such as: • Operating system (OS) software; • Firmware; • Commercially available or open-source application software, including application containers; • Custom software installed, including application containers; • Configuration that modifies network accessible logical ports or network accessible services on an Applicable System; • SCI configuration of host affinity

Draft 4 of CIP-010-5

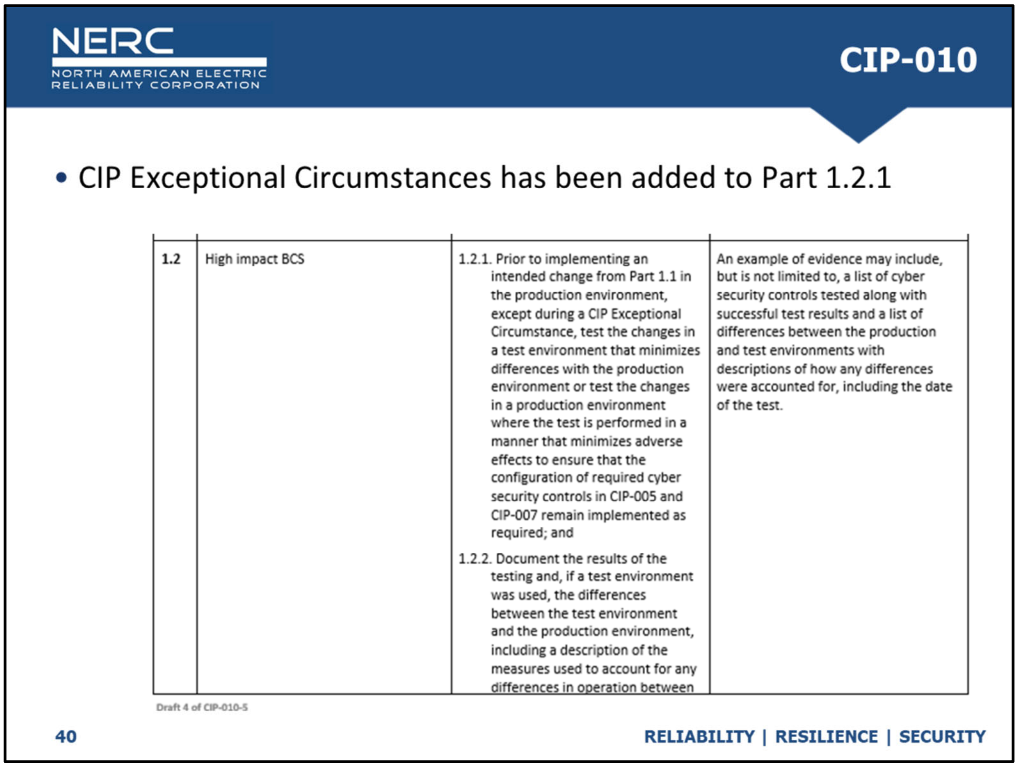


NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP-010

- Backwards Compatibility
- Maintaining baseline configs is ‘one’ way to help manage change. The old baselines methodology was moved into the Measures
- Note that for the purposes of backwards compatibility there needs to be additional documentation to show that an entity has considered the configuration items in their baseline are those that they consider cover *“intended changes to software, or intended changes to setting that could weaken configured cyber security controls required by CIP-005 and CIP-007 “*

Norm



NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP-010

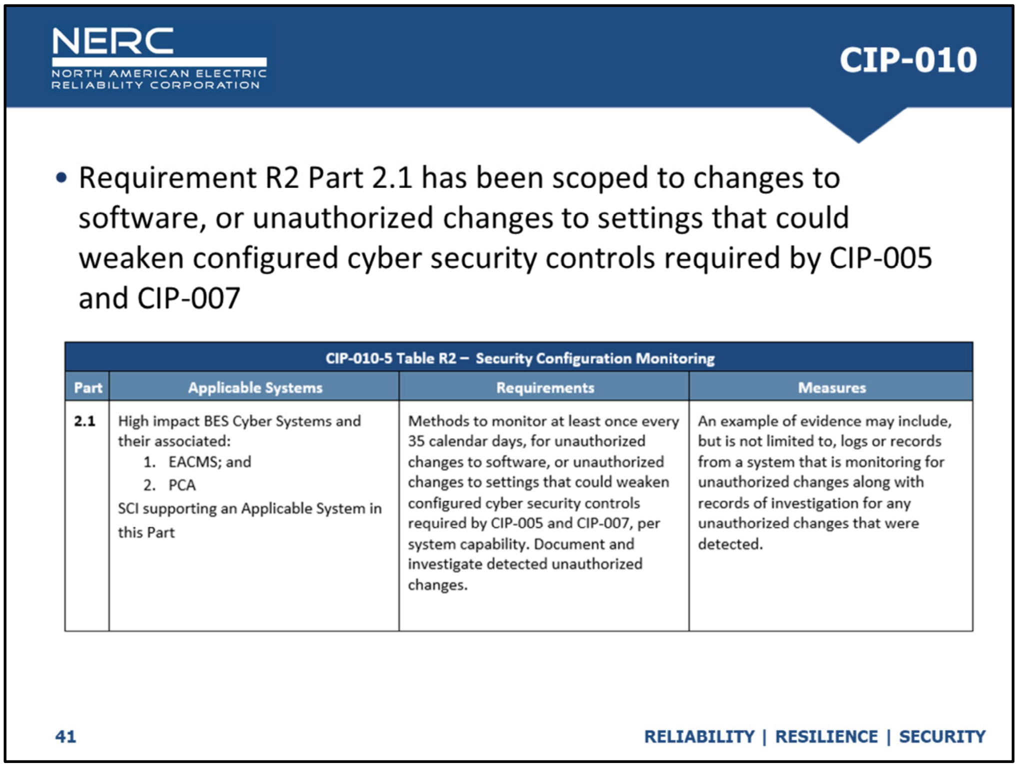
- CIP Exceptional Circumstances has been added to Part 1.2.1

1.2	High impact BCS	1.2.1. Prior to implementing an intended change from Part 1.1 in the production environment, except during a CIP Exceptional Circumstance, test the changes in a test environment that minimizes differences with the production environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects to ensure that the configuration of required cyber security controls in CIP-005 and CIP-007 remain implemented as required; and 1.2.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including the date of the test.

Draft 4 of CIP-010-5

RELIABILITY | RESILIENCE | SECURITY

Norm



NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP-010

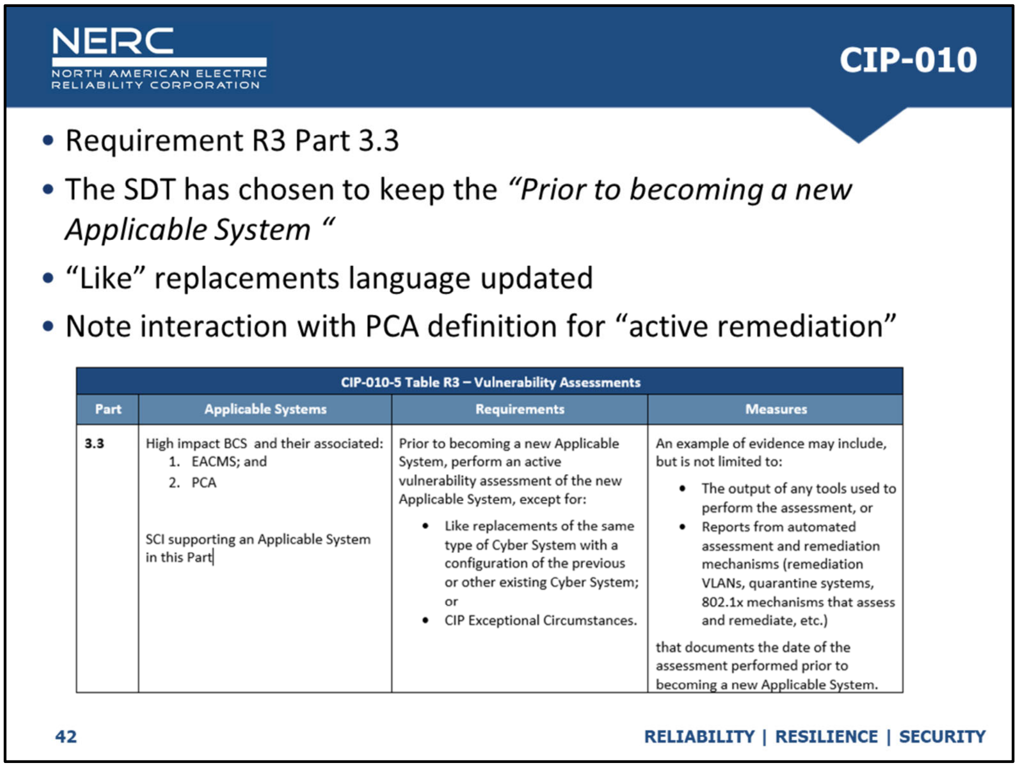
- Requirement R2 Part 2.1 has been scoped to changes to software, or unauthorized changes to settings that could weaken configured cyber security controls required by CIP-005 and CIP-007

CIP-010-5 Table R2 – Security Configuration Monitoring

Part	Applicable Systems	Requirements	Measures
2.1	High impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Methods to monitor at least once every 35 calendar days, for unauthorized changes to software, or unauthorized changes to settings that could weaken configured cyber security controls required by CIP-005 and CIP-007, per system capability. Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs or records from a system that is monitoring for unauthorized changes along with records of investigation for any unauthorized changes that were detected.

41 RELIABILITY | RESILIENCE | SECURITY

Norm



NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

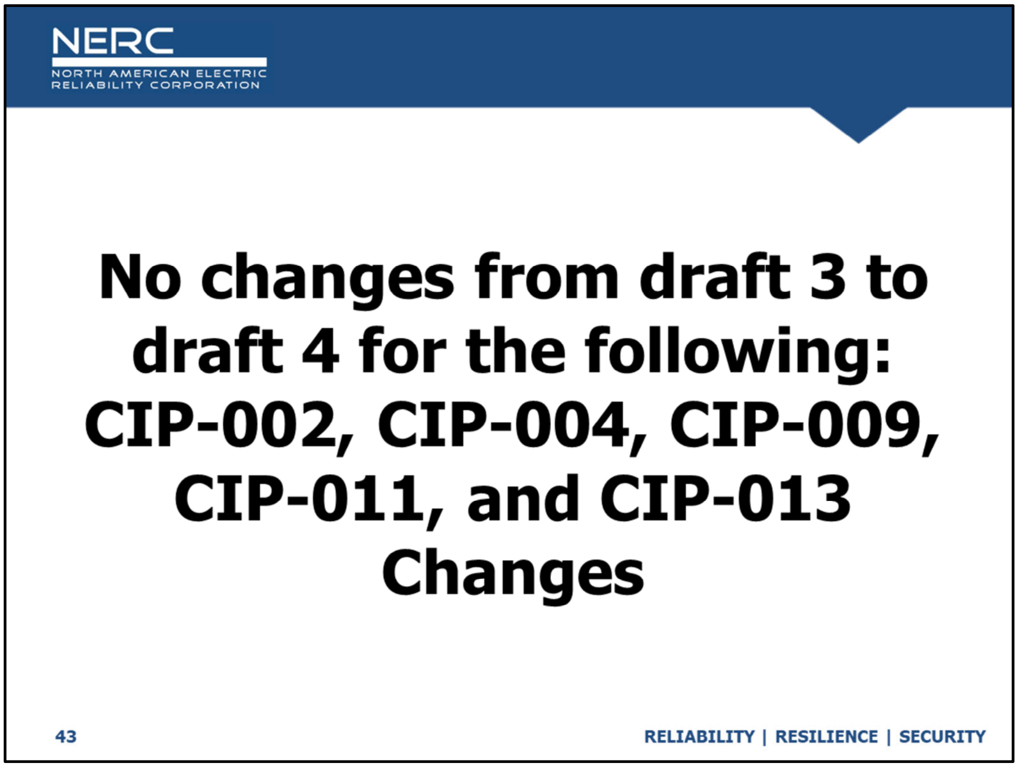
CIP-010

- Requirement R3 Part 3.3
- The SDT has chosen to keep the *"Prior to becoming a new Applicable System "*
- "Like" replacements language updated
- Note interaction with PCA definition for "active remediation"

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High impact BCS and their associated: 1. EACMS; and 2. PCA SCI supporting an Applicable System in this Part	Prior to becoming a new Applicable System, perform an active vulnerability assessment of the new Applicable System, except for: • Like replacements of the same type of Cyber System with a configuration of the previous or other existing Cyber System; or • CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to: • The output of any tools used to perform the assessment, or • Reports from automated assessment and remediation mechanisms (remediation VLANs, quarantine systems, 802.1x mechanisms that assess and remediate, etc.) that documents the date of the assessment performed prior to becoming a new Applicable System.

42 RELIABILITY | RESILIENCE | SECURITY

Norm
Pass to Robert.



NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

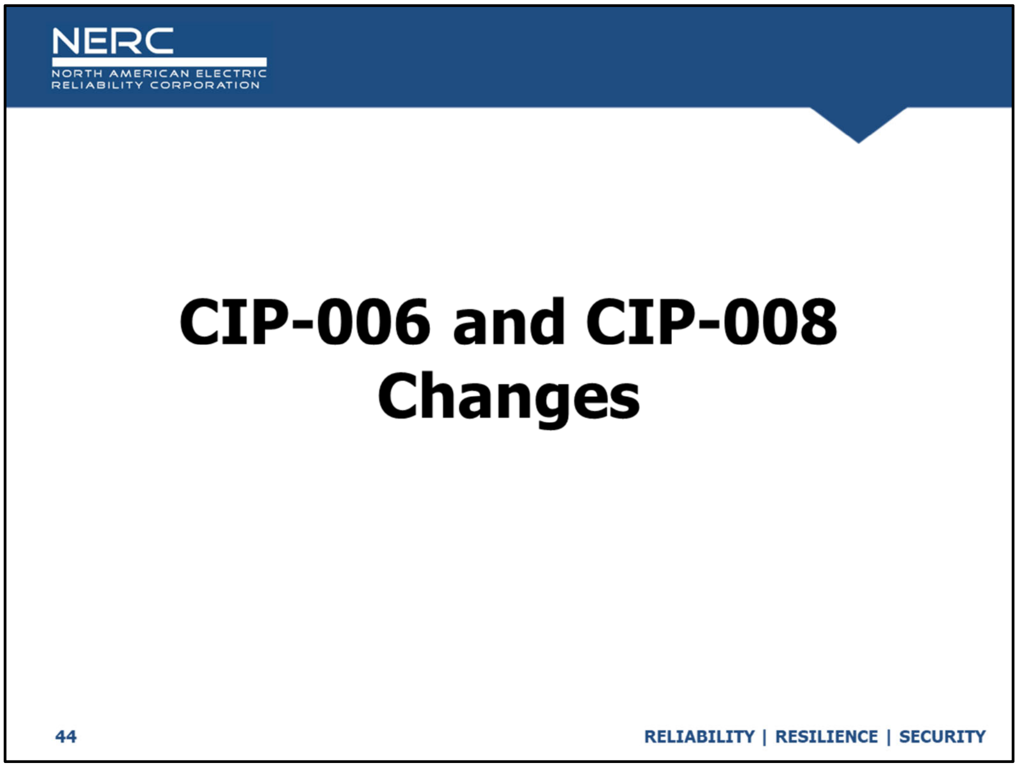
No changes from draft 3 to draft 4 for the following: CIP-002, CIP-004, CIP-009, CIP-011, and CIP-013 Changes

43

RELIABILITY | RESILIENCE | SECURITY

Robert

No changes made to these slides from draft 3 to draft 4. As mentioned in before slides, all standards were added for additional ballot based on definitional changes.



NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

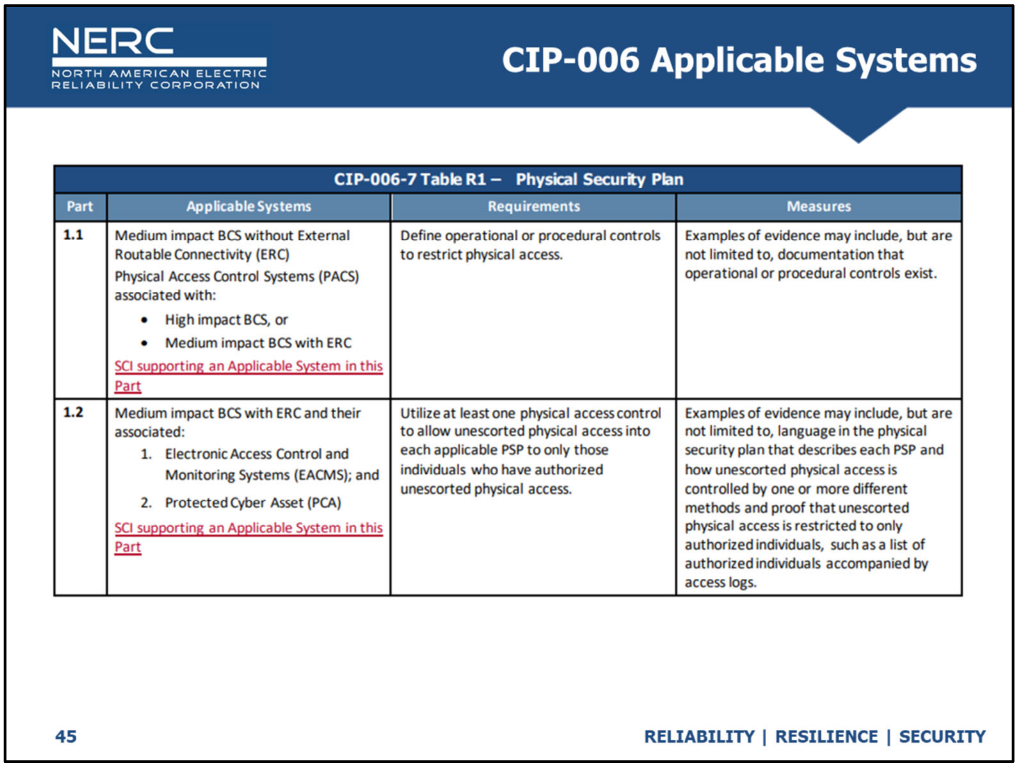
CIP-006 and CIP-008 Changes

RELIABILITY | RESILIENCE | SECURITY

ROBERT

Good morning/afternoon everyone.

The changes in this draft as they pertain to CIP-006 and CIP-008 are slight and deal with the identification of Applicable Systems.



NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP-006 Applicable Systems

CIP-006-7 Table R1 – Physical Security Plan

Part	Applicable Systems	Requirements	Measures
1.1	Medium impact BCS without External Routable Connectivity (ERC) Physical Access Control Systems (PACS) associated with: • High impact BCS, or • Medium impact BCS with ERC SCI supporting an Applicable System in this Part	Define operational or procedural controls to restrict physical access.	Examples of evidence may include, but are not limited to, documentation that operational or procedural controls exist.
1.2	Medium impact BCS with ERC and their associated: 1. Electronic Access Control and Monitoring Systems (EACMS); and 2. Protected Cyber Asset (PCA) SCI supporting an Applicable System in this Part	Utilize at least one physical access control to allow unescorted physical access into each applicable PSP to only those individuals who have authorized unescorted physical access.	Examples of evidence may include, but are not limited to, language in the physical security plan that describes each PSP and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

45

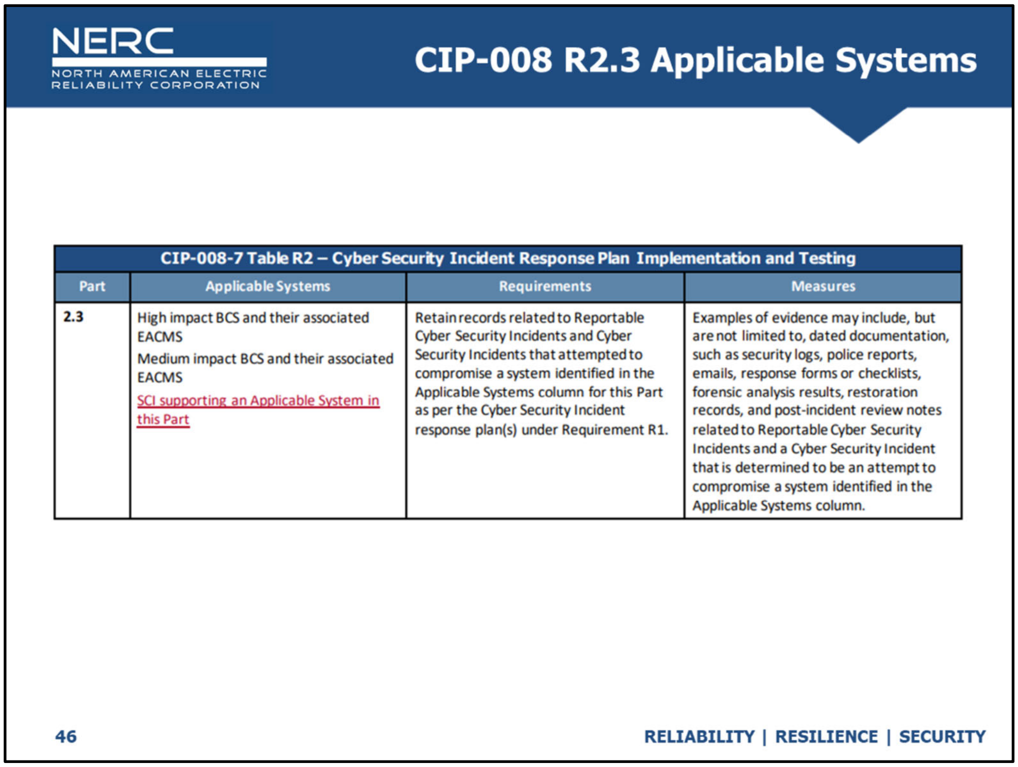
RELIABILITY | RESILIENCE | SECURITY

ROBERT

In CIP-006, we have added SCI to the Applicable Systems column of nearly every requirement based on the comments received after our last draft posting.

The commenters understood that SCI was implicitly included, but asked for the addition to improve clarity and understanding.

The team agrees that this improves clarity and understanding.



NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP-008 R2.3 Applicable Systems

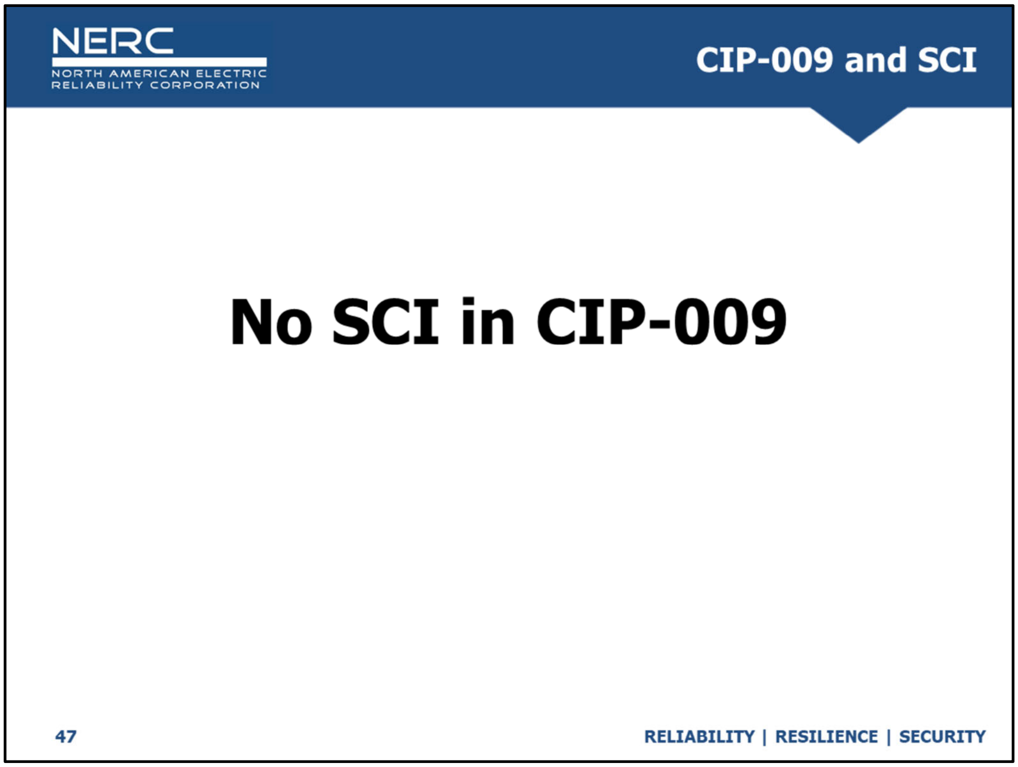
CIP-008-7 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	Applicable Systems	Requirements	Measures
2.3	High impact BCS and their associated EACMS Medium impact BCS and their associated EACMS SCI supporting an Applicable System in this Part	Retain records related to Reportable Cyber Security Incidents and Cyber Security Incidents that attempted to compromise a system identified in the Applicable Systems column for this Part as per the Cyber Security Incident response plan(s) under Requirement R1.	Examples of evidence may include, but are not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents and a Cyber Security Incident that is determined to be an attempt to compromise a system identified in the Applicable Systems column.

46 RELIABILITY | RESILIENCE | SECURITY

ROBERT

In CIP-008, we have added SCI to the Applicable Systems column of Requirement 2.3.

SCI was added to this requirement to ensure that the information required for proper Incident Reporting is being collected and retained.



NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP-009 and SCI

No SCI in CIP-009

47

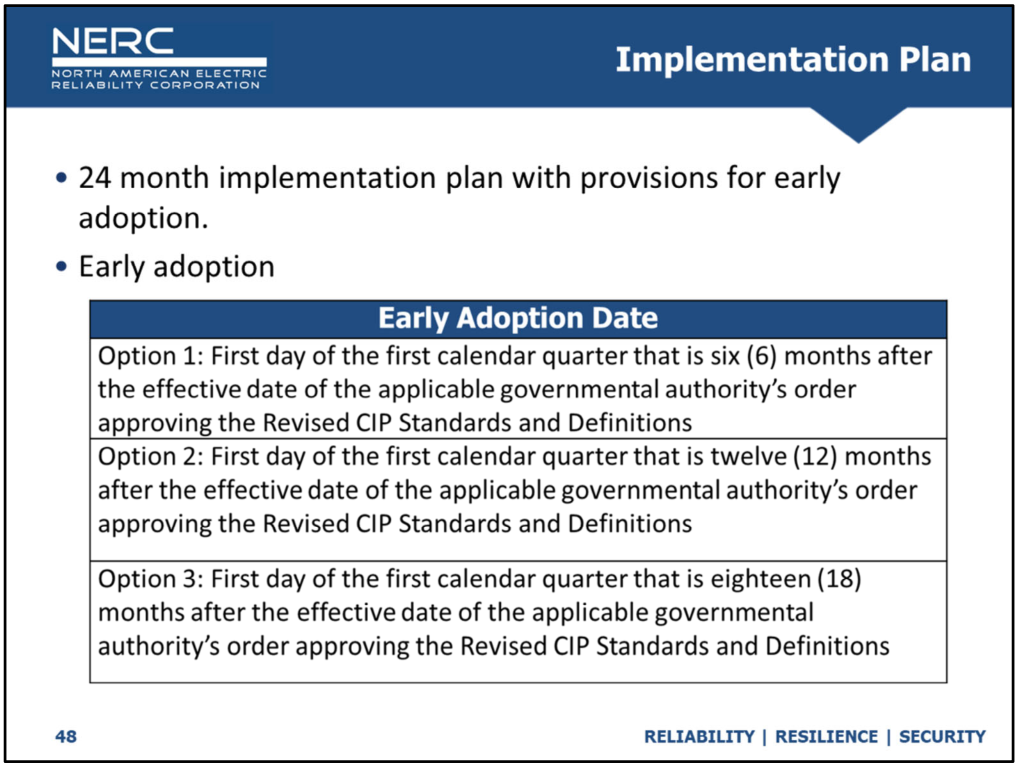
RELIABILITY | RESILIENCE | SECURITY

ROBERT

While SCI has been added to many parts of CIP-006 and CIP-008, we have purposely not added it to CIP-009. This is a potential source of confusion, so we wanted to proactively address it.

In essence, an entity may choose to replace SCI and VCAs with physical hardware as part of their BCS Recovery Plan, instead of replacing their SCI, therefor we wanted to ensure the Requirements within CIP-009 would no preclude an entity from doing so.

Now I will pass things to Jordan to review the Implementation Plan.



NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

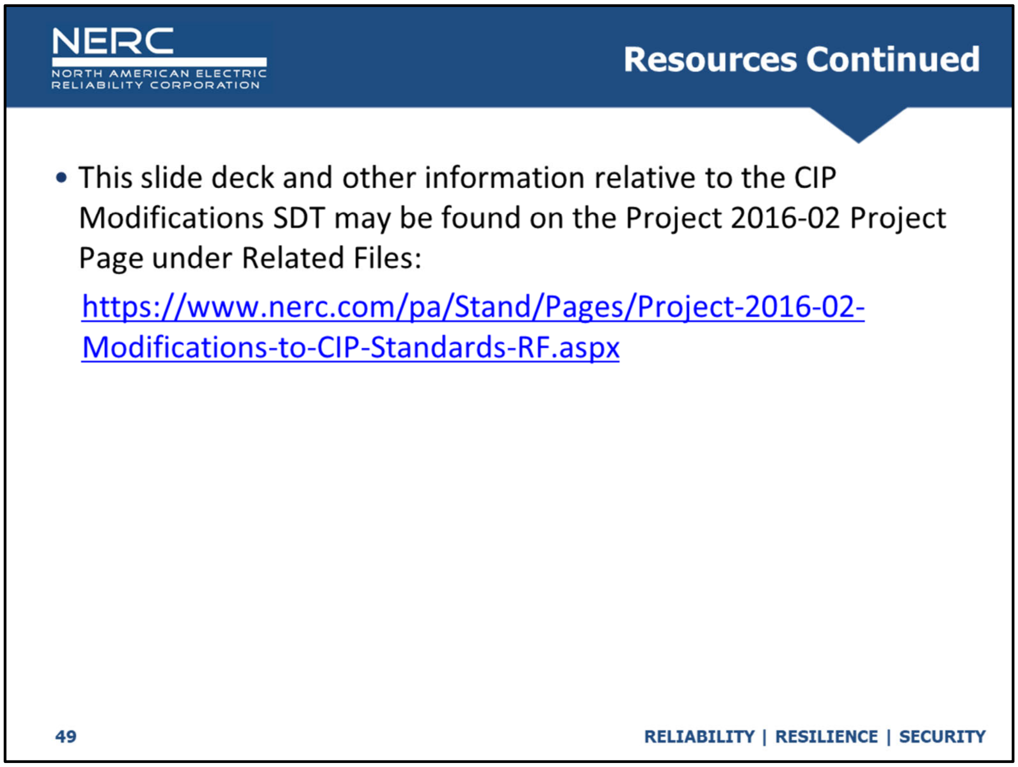
Implementation Plan

- 24 month implementation plan with provisions for early adoption.
- Early adoption

Early Adoption Date
Option 1: First day of the first calendar quarter that is six (6) months after the effective date of the applicable governmental authority's order approving the Revised CIP Standards and Definitions
Option 2: First day of the first calendar quarter that is twelve (12) months after the effective date of the applicable governmental authority's order approving the Revised CIP Standards and Definitions
Option 3: First day of the first calendar quarter that is eighteen (18) months after the effective date of the applicable governmental authority's order approving the Revised CIP Standards and Definitions

Speaker: Jordan

24 month implementation plan with early adoption available. Change made for this draft is the Early adoption date. This allows entities to work with their respective region and determine an early adoption date from the three listed options to adopt the virtualization standards early.



Resources Continued

- This slide deck and other information relative to the CIP Modifications SDT may be found on the Project 2016-02 Project Page under Related Files:

  https://www.nerc.com/pa/Stand/Pages/Project-2016-02-Modifications-to-CIP-Standards-RF.aspx

Resource page for previous webinars.

Questions and Answers