Tyson Jarrett
CIP Enforcement Analyst

Utilizing Related Requirements to Identify Gaps in Security

January 30, 2012

Phoenix, Arizona

One oversight…Multiple issues

Agenda

- What are related requirements
- How to identify related requirements
- What to do when an issue is found
- How to prevent issues with related requirements

Why should you be aware of related requirements

- Identify Risks to Reliability
- Identify and correct security gaps
- Protect your resources

What are related requirements?

- Standards and requirements with steps that are similar, related, or otherwise linked to steps outlined in other standards and requirements.

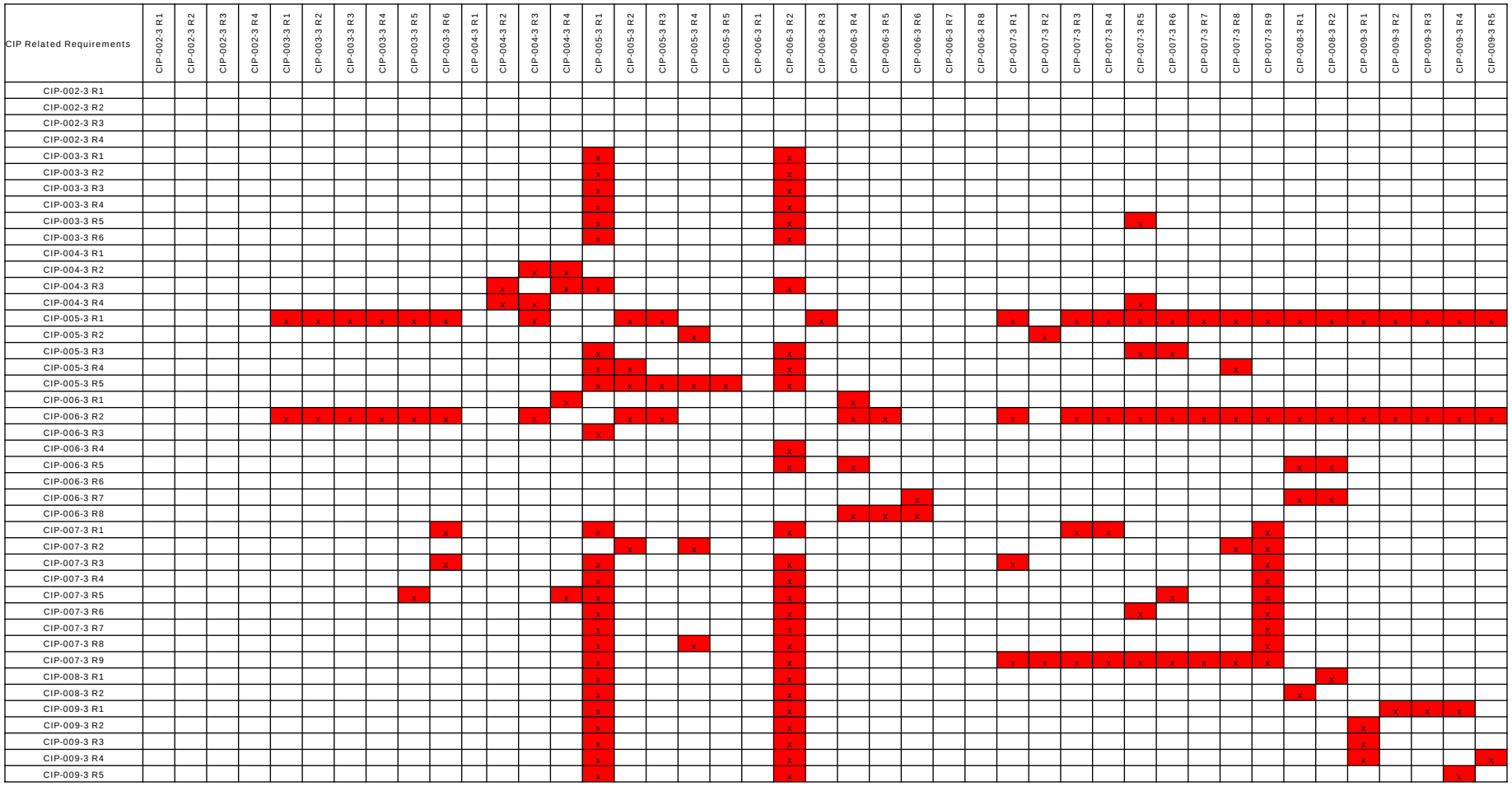
Commonly related requirements

- CIP 005 R4 = CIP 007 R8
- Require similar protections, but to different assets…
- An issue with a CVA for assets within a ESP (CIP 007 R8) vs. an issue with a CVA for access points (CIP 005 R4)

Commonly related requirements

- CIP 004 R2 = CIP 004 R3 = CIP 004 R4 (training, PRA and access)
- Why are they related?
- Typically done in conjunction with one another
  - i.e., access not granted until PRA, training, and authorization done.

CIP Related Requirements – Matrix



How to identify related requirements

1. Requirements referencing other standards/requirements

2. Requirements with similar actions

3. Requirements typically done at the same time

References other requirements

- Standard or requirement that directly relates to and references other standards or Requirements.

References other requirements- List

- CIP 002 R2 = CIP 002 R3 = CIP 002 R4 (Review and approval)
- CIP 003 R1.1 = CIP 002 – CIP 009
- CIP 003 R1.3 = CIP 003 R2 (CIP Senior Manager)
- CIP 005 R1.5 = CIP 003, CIP 004 R3, CIP 005 R2 and R3, CIP 006 R3, CIP 007 R1 and R3-R9, CIP 008, CIP 009 (25 referenced requirements)
- CIP 005 R2.5.3 = CIP 004 R4 (Review of authorization rights)

References other requirements– List cont..

- CIP 005 R5.1 = CIP 005 (Current and approved documentation)
- CIP 005 R5.3 = CIP 008 (Logs of reportable cyber security incidents
- CIP 006 R2.2 = CIP 003, CIP 004 R3, CIP 005 R2 and R3, CIP 006 R4 and R5, CIP 007, CIP 008, CIP 009 (27 referenced requirements)
- CIP 006 R5 = CIP 008 (Logs handled in accordance with CIP 008)

References other requirements– List cont..

- CIP 006 R7 = CIP 008 (Logs kept according to CIP 008)
- CIP 006 R8 = CIP 006 R4, R5, R6 (Ensure security systems function)
- CIP 007 R3 = CIP 003 R6 (Security patch management)
- CIP 007 R5.1.1 = CIP 003 R5 (Accounts implementation)
- CIP 007 R5.1.3 = CIP 003 R5, CIP 004 R4 (Review of access privileges)

References other requirements– List cont..

- CIP 007 R6.3 = CIP 008 (Logs related to system events)
- CIP 007 R9 = CIP 007 (Review and approval of documentation)
- CIP 008 R2 = CIP 008 R1.1 (Keep documentation per CIP 008 R1.1)

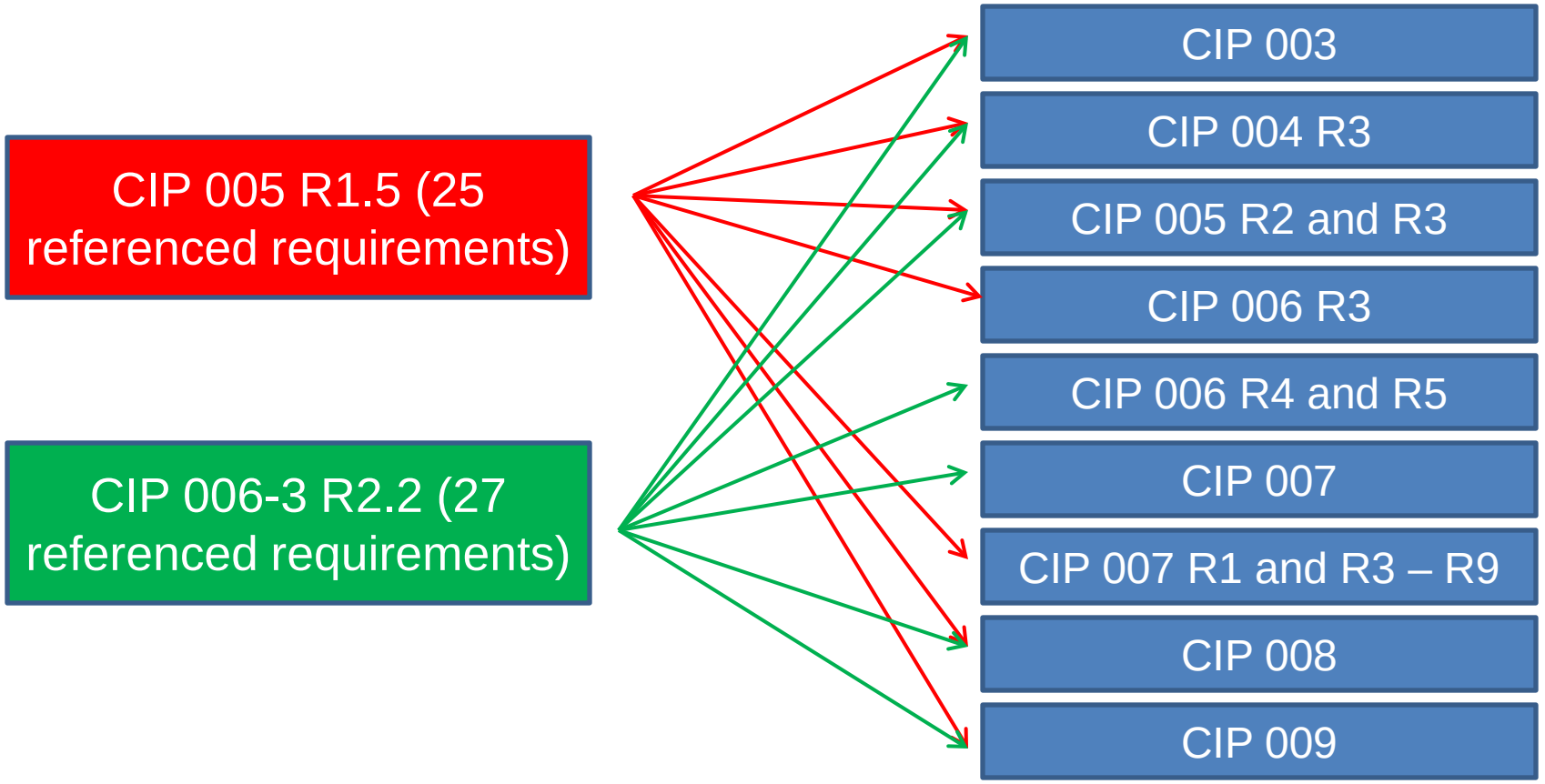
References other requirements – Example 1

- CIP 006 R7: “The Responsible Entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the Requirements of Standard CIP-008-3.”

References other requirements– Example 2

- Devices within ESPs enabled ports/services that are not required (CIP 007 R2)
- Devices used in Access Control and Monitoring of Electronic Security Perimeters may also have enabled ports/services that are not required (CIP 005 R1.5)

References other requirements– Example 2 cont..



Requirements with similar actions

- Standards or requirements that require similar actions to other standards or requirements, although not explicitly referenced in the standard.

List of Requirements with similar actions

- CIP 004 R4 = CIP 006 R1.4 = CIP 007 R5 (Access authorization and revocation)
- CIP 005 R2 = CIP 005 R4 (Ports and services)
- CIP 005 R3 = CIP 007 R6 = CIP 006 R5 (Monitoring logical and physical access)
- CIP 005 R4 = CIP 007 R8 (Cyber vulnerability Assessment)

List of Requirements with similar actions cont..

- CIP 007 R1 = CIP 007 R3 (Testing of security patches)
- CIP 007 R2 = CIP 007 R8 (Ports and services)
- CIP 007 R5 = CIP 007 R8 (Default user accounts)

Requirements with similar actions - examples

- Due to configuration error system events related to cyber security not sending automated alerts (CIP 007 R6)

- May also be an issue with configuration of alerting for attempts at or actual unauthorized accesses (CIP 005 R3) to Electronic Security Perimeter(s)

Requirements with similar actions - examples

- Operator discovered a device with default administrator account not renamed or password changed (CIP 007 R5.2.1)

- Why was this not caught during annual CVA(s)? May also be an issue with CVA process

Typically done at the same time

- Requirements not necessarily linked or related, but typically done in conjunction with one another.

Typically done at the same time - List

- CIP 004 R4 = CIP 004 R3 = CIP 004 R2 (Access authorization depends on PRA and training completion)
- CIP 003 R6 = CIP 007 R1 (Change control requires testing prior to implementation)
- CIP 007 R1 = CIP 007 (Testing helps ensure CIP 007 security controls in place)
- CIP 009 R4 = CIP 009 R5 (backup media tested when conducting backups)

Typically done at the same time - example

- CIP 007 R1 – Lack of testing may lead to un-known issues with existing CIP 007 security controls.
  - Excessive ports open (CIP 007 R2)
  - Anti-Virus (CIP 007 R4)
  - Un-documented accounts (CIP 007 R5)
  - Monitoring (CIP 007 R6)

Typically done at the same time - example

- Device placed into production without testing to ensure security controls not adversely affected (CIP 007 R1)

- Change control procedures typically require testing prior to implementation. Why was Change Control not followed?

What should a registered entity do when an issue is found?

- Look for related requirements that may have same/similar issue
  - Don’t stop at the root cause, find all the symptoms
- Plan how to mitigate the root cause **AND** all associated symptoms

Scope and Mitigation: Scope

Root Cause

•Cold!!

Symptom

•Cold!!
•Fever
•Runny Nose
•Tired
•Don’t feel good

Scope and Mitigation: Root Cause

Root Cause	Mitigating Root Cause
	
•Cold!!	•Keep Warm

Scope and Mitigation: Symptom

Symptom

- Cold!!
- Fever
- Runny Nose
- Tired
- Don’t feel good

Mitigating symptoms

- Keep Warm
- See a doctor
- Take medicine
- Get rest
- Drink plenty of water

WECC

Preventing issues of related requirements

- Know the commonly related standards and how to identify them
  - Be aware of how requirements can be related on an on-going basis (i.e. Periodic reviews)
- Maintain/Establish Communication between departments
  - IT, physical security, compliance, etc.
  - Break down Silos

Preventing issues of related requirements

- Every entity is different, some requirements may be related for one entity but not for another, depending on procedures in place

- Don’t just memorize what is typically related, know what is related for your organization

Preventing issues of related requirements - Communication

- Enhance interdepartmental communication
  1. “We thought IT was doing that…”
  2. “I’m just a gates, guns, and guards guy; I leave the technical stuff for IT”
  3. “Well that device belongs to Generation so we didn’t do anything to it”

Why communication is key

- CIP and O&P standards could also be related
  - CIP 001 = CIP 008 (sabotage and incident reporting)
  - EOP 005-1 = CIP 002 (Identification of Blackstart resources)
  - EOP 008-1 R1.2.5 = CIP 005 and CIP 006 (Physical and Cyber security)
  - And possibly more…

Best User Reporting Practices Checklist

Self Report/Self Cert Checklist

- ☐ Is the version of the standard (in effect at the time of the violation) identified?
- ☐ Are all multiple subrequirements in scope identified?
- ☐ Have you confirmed the scope?
  - Are all multiple subrequirements in scope identified?
  - Have you reviewed all instances of non-compliance?
  - Have you reviewed all applicable related requirements?

- ☐ Has this violation been previously reported (e.g. self report, audit finding or self cert)?
  - If yes, please use the WECC Data Request Form to provide more details on the previously reported violation (including a change in scope)
- ☐ Does the violation description include:
  - All devices/facilities/personnel in scope?
  - Names/IDs of devices/facilities/personnel?
  - Where are these devices located (e.g. ESP, PSP, facility)?
  - What are these devices used for?
  - What type of access do the personnel have (e.g. cyber, physical or both)?
  - Any additional information required to assess the VSL (e.g. percentages, instances of non compliance)? VSL
- ☐ Is the start and end date of the violation identified?
- ☐ Are the compensating measures (that lower the risk) identified?

Resources

- Best User Reporting Practices checklist
- Matrix of commonly related standards

Summary

- Know the commonly related Standards and Requirements
- Know how to identify potentially related requirements
- Understand Prevention Steps
  - Break down Silos
- Approach WECC with questions

Questions?

Tyson Jarrett
CIP Enforcement Analyst
801.819.7676
Tjarrett@wecc.biz