

# CIP Update

March 10, 2015

Kevin B. Perry  
Director, Critical Infrastructure Protection  
[kperry.re@spp.org](mailto:kperry.re@spp.org)  
501.614.3251



# Agenda

- **CIP Version 5 Transition Update**
- **Training and Outreach**
- **CIP Version 5 Revisions**
- **CIP-014 (Physical Protection)**
- **CIP Breakout Sessions**
- **Q&A**

# CIP Version 5 Transition Update

- **2015 audits**
  - **Entity choice: audit against V3 or V5 language**
  - **V5 compliance is deemed to be V3 compliance**
  - **Will advise entity, possibly via Area of Concern, if audited process will not be V5 compliant**
  - **Auditor discretion to not find V3 violation if no equivalent V5 requirement**
  - **Open Enforcement Actions should be mitigated to V5 requirement**
  - **Setting aside time for V5 outreach**

# CIP Version 5 Transition Update

- **Two Lessons Learned approved by Standards Committee February 18, 2015, after industry comment:**
  - **Generation Segmentation**
  - **Far-End Relay**
- **Posted to the [NERC CIP V5 Transition web site](#) as Final Lessons Learned**

# CIP Version 5 Transition Update

- **Three Lessons Learned recently posted for industry comment:**
  - **EACMS (Electronic Access Control or Monitoring Systems) Mixed Trust Authentication**
  - **Interactive Remote Access**
  - **Programmable Electronic Device**
- **Comment period ended February 6, 2015**
- **CIP V5 Transition Advisory Group working on post-comment revisions**

# CIP Version 5 Transition Update

- **Top 15 Lessons Learned** planned to be at least posted for industry comment by **April 1, 2015**
  - [Lessons Learned plan](#) posted on the NERC web site
- **Next Lessons Learned** expected to be posted for industry comment:
  - **Generation Interconnection Point**
  - **Grouping BES Cyber Systems**
  - **Non-BA/non-TOP Control Centers**

# CIP Version 5 Transition Update

- **Virtualization summit held by NERC**
  - Brought together industry and key solution providers (Cisco and VMWare)
  - Looking to identify successful ways to deploy virtual environments (virtual machines, virtual LANs) within the CIP requirements
  - Virtualization Lesson Learned being developed by the V5 Transition Advisory Group with a late March target date to post for comment
  - The webinar was recorded and has been posted to the NERC web site

# NERC-Sponsored Training

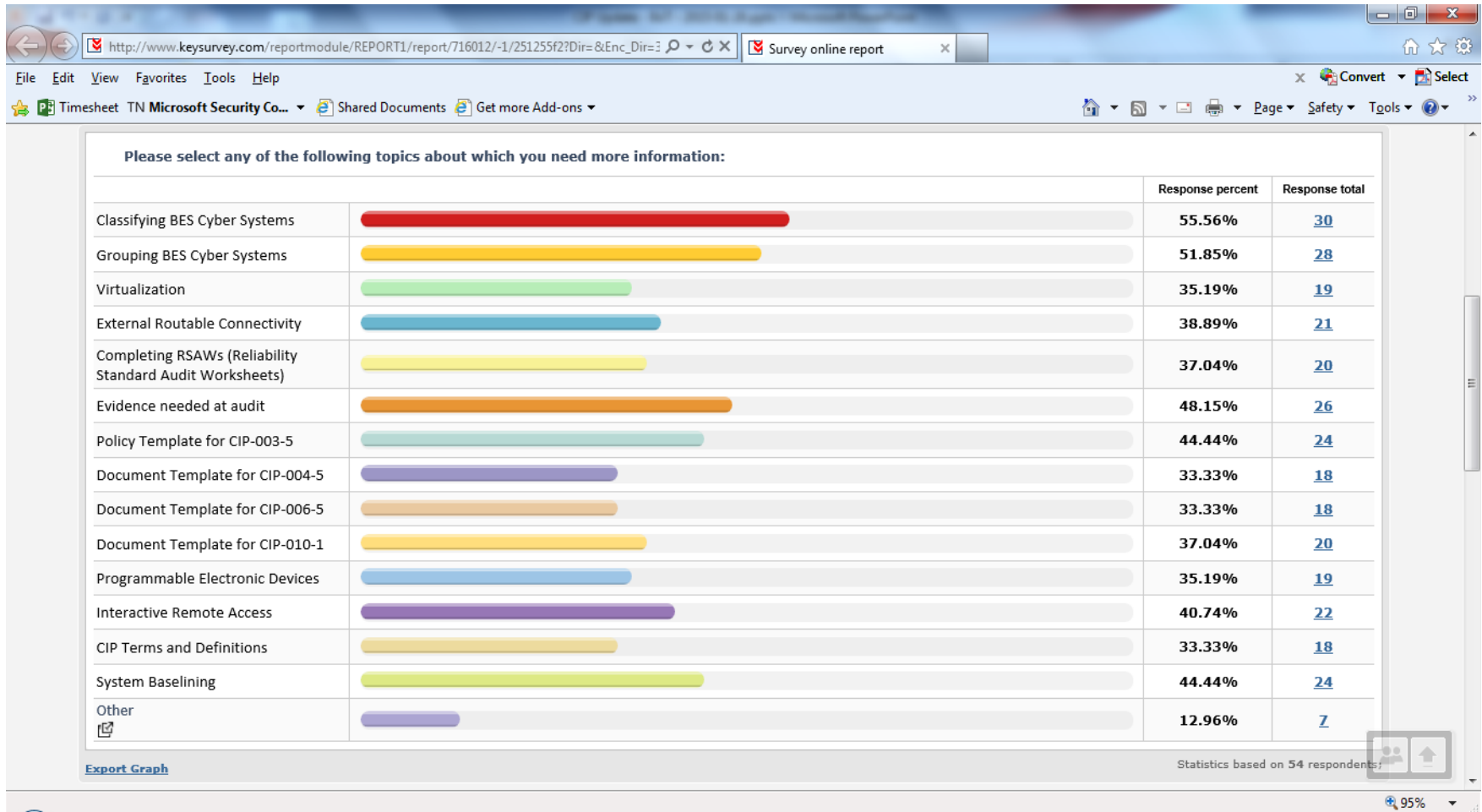
- [CIP Workshops and Curriculum](#) content being developed
  - Compilation of links and references to NERC and regional training, presentations, guidance, and other CIP V5 information
- **Small Group Advisory Training**
  - Three 3-day industry sessions scheduled in Atlanta:
    - February 24-26, 2015
    - March 24-26, 2015 (registration deadline 3/10/2015)
    - April 21-23, 2015 (registration deadline 4/10/2015)
  - Registration links posted on [CIP V5 Event Calendar](#)



# SPP Regional Outreach

- SPP RE and SPP RTO compliance staffs are collaborating on CIP V5 outreach
  - June “CIP Week” ([register here](#))
  - Webinars
  - Multi-entity outreach visits
  - One-on-one assistance visits
- Circulated an outreach survey to the SPP RE entities
  - Survey closed January 21, 2015; 57 respondents
  - Determined outreach needs by topic
  - Determined interest in site visits

# Outreach Survey Results



# CIP Standards Revisions

- **Initial revisions, balloted as the “-X” standards, adopted by the NERC Board of Trustees November 13, 2014**
  - **CIP-003-6 – Security Management Controls**
  - **CIP-004-6 – Personnel & Training**
  - **CIP-006-6 – Physical Security of BES Cyber Systems**
  - **CIP-007-6 – System Security Management**
  - **CIP-009-6 – Recovery Plans for BES Cyber Systems**
  - **CIP-010-2 – Configuration Change Management and Vulnerability Assessments**
  - **CIP-011-2 – Information Protection**

# CIP Standards Revisions

- **The initial revisions:**
  - **Removed Identify, Assess, and Correct Language from 17 requirements**
  - **Addressed the Communications Networks directives of FERC Order 791**
    - **CIP-006-6 / Requirement Part 1.10: Physical protection of cabling and other non-programmable components of BES Cyber Systems existing outside of the PSP.**
    - **CIP-007-6 / Requirement Part 1.2: Prevent unauthorized use of physical ports on non-programmable electronic components.**

# CIP Standards Revisions

- Remaining revisions, balloted as the “-7” standards, adopted by the NERC Board of Trustees February 12, 2015
  - CIP-003-7
  - CIP-004-7
  - CIP-007-7
  - CIP-010-3
  - CIP-011-3

# CIP Standards Revisions

- **The remaining revisions:**
  - **Clarified Cyber Security Plan requirements for Low Impact BES Cyber Systems**
  - **Clarified requirements for Transient Cyber Assets and Removable Media**
  - **Defined new terms**

# CIP Standards Revisions

- **“-X” and “-7” changes merged into new Version 6**
  - CIP-003-6 – Security Management Controls
  - CIP-004-6 – Personnel & Training
  - CIP-006-6 – Physical Security of BES Cyber Systems
  - CIP-007-6 – System Security Management
  - CIP-009-6 – Recovery Plans for BES Cyber Systems
  - CIP-010-2 – Configuration Change Management and Vulnerability Assessments
  - CIP-011-2 – Information Protection
- **Submitted to FERC February 13, 2015**

# CIP-014-1 (Physical Security)

- **Approved by FERC Order 802 on November 20, 2014**
- **Enforceable October 1, 2015**
- **Compliance milestones (latest date is Feb 16, 2017):**
  - **Initial Risk Assessment (IRA) complete on or before October 1, 2015**
  - **Assessment Verification (AV) = IRA + 90 calendar days**
  - **Assessment Modifications (AM) = AV + 60 calendar days**
  - **Control Center Notification (CCN) = AM + 7 calendar days**
  - **Security Plan (SP) = AM (or AV) + 120 calendar days**
  - **Security Plan Review (SPR) = SP + 90 calendar days**



# CIP-014 (Physical Security) Revisions

- Standard is being revised to address FERC Order 802 directives:
  - Remove the term “widespread” from CIP-014-1 or, alternatively, modify the standard to address Commission concerns
  - Responsive filing required six months after the effective date of Order 802 (due July 24, 2015)
- [Risk Assessment and Third-Party Verifications](#) guidance memorandum posted on the NERC web site

# CIP Breakout Sessions

- **Three CIP breakout sessions scheduled for this afternoon in the Auditorium**
  1. **1:00 – 2:00: Change Control and Configuration Management**
  2. **2:10 – 3:10: CIP V5 Lessons Learned and FAQ Discussion**
  3. **3:40 – 4:40: Open Q&A**
- **We plan to keep the WebEx and conference call open due to popular demand**

# Helpful Resources

- **NERC Website Links:**
  - **[CIP V5 Transition Home Page](#)**
    - **[CIP V5 Standards and Implementation Plan](#)**
    - **[CIP V5 Transition Guidance](#)**
    - **[CIP V5 Transition Study Lessons Learned](#)**
  - **[Project 2014-04 \(Physical Security\)](#)**
    - **[CIP-014-1](#)**
    - **[CIP-014-1 Implementation Plan](#)**
    - **[CIP-014 Revisions SAR](#)**

# Helpful Resources

- SPP RE Website: CIP V5 Outreach
  - [Identifying BES Cyber Systems SPP RE Webinar Updated 10-30-14](#)
  - [CIP V5 Transition Guidance SPP RE webinar- 2014-09-04](#)
  - [CIP\\_V5\\_SPP RE Hands-On Training Materials March 2014](#)

# SPP RE CIP Team

- [Kevin Perry](#), Director of Critical Infrastructure Protection  
(501) 614-3251
- [Shon Austin](#), Lead Compliance Specialist-CIP  
(501) 614-3273
- [Steven Keller](#), Lead Compliance Specialist-CIP  
(501) 688-1633
- [Jeremy Withers](#), Senior Compliance Specialist-CIP  
(501) 688-1676
- [Robert Vaughn](#), Compliance Specialist II-CIP  
(501) 482-2301