

Welcome

NPCC Fall 2018 Workshop

Scott Nied
Providence, RI
November 7, 2018

Welcome – Before We Begin

Go to www.slido.com and enter “NPCC2018”

OR

Get the slido app on your
Phone and enter “NPCC2018”

We will explain in a minute!

Get ready for a test.



November 7 Classroom Tracks

2:00 pm, 3:00 pm, 4:00 pm

	2:00 pm	3:00 pm	4:00 pm
Track 1	A	B	C
Track 2	B	C	A
Track 3	C	A	B

A: Entity Risk Assessment Team (Mozart Room, Mezzanine Level)

B: Compliance Monitoring Team (Beethoven Room, Mezzanine Level)

C: Mitigation/Enforcement Team (Leydn Room – Temple Level)

Thursday

- We are offering a box lunch (slido poll)
- NO we are not having a raffle for those who attend the end
- We will have treats though

Compliance Solutions

- Proven Compliance Solutions
- SOS Intl
- Assurx
- Cooper Compliance
- SigmaFlow, LLC
- FoxGuard Solutions, Inc.
- AESI Inc.
- WizNucleus

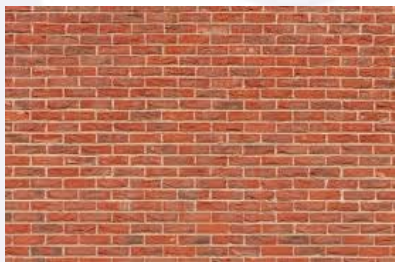


NPCC Workshop Disclaimer

This information, developed by Northeast Power Coordinating Council, Inc. (“NPCC”) staff, provides nonbinding guidance to industry stakeholders regarding existing and/or emerging Reliability Standards. If anything herein conflicts with the applicable Reliability Standard, approved Implementation Guidance, or any other applicable rule, order, regulation, etc., the latter will govern. This information is specific to NPCC and should not be relied upon in any other Regional Entity or at NERC. Compliance with Reliability Standards ultimately depends on the facts and circumstances, quality of evidence, and the language of the Reliability Standard.

Two Results

- Stakeholders viewpoint
- Stronger ERO



ERO Challenges

- Industry Expectations
- Demand Side/DER growing
- Inverter proliferation
- Human Perf – levels of awareness
- Cyber Threat Matrix



- Questions?
- Send comments/questions through slido
- Javier is monitoring them
- He will vet them for the speaker

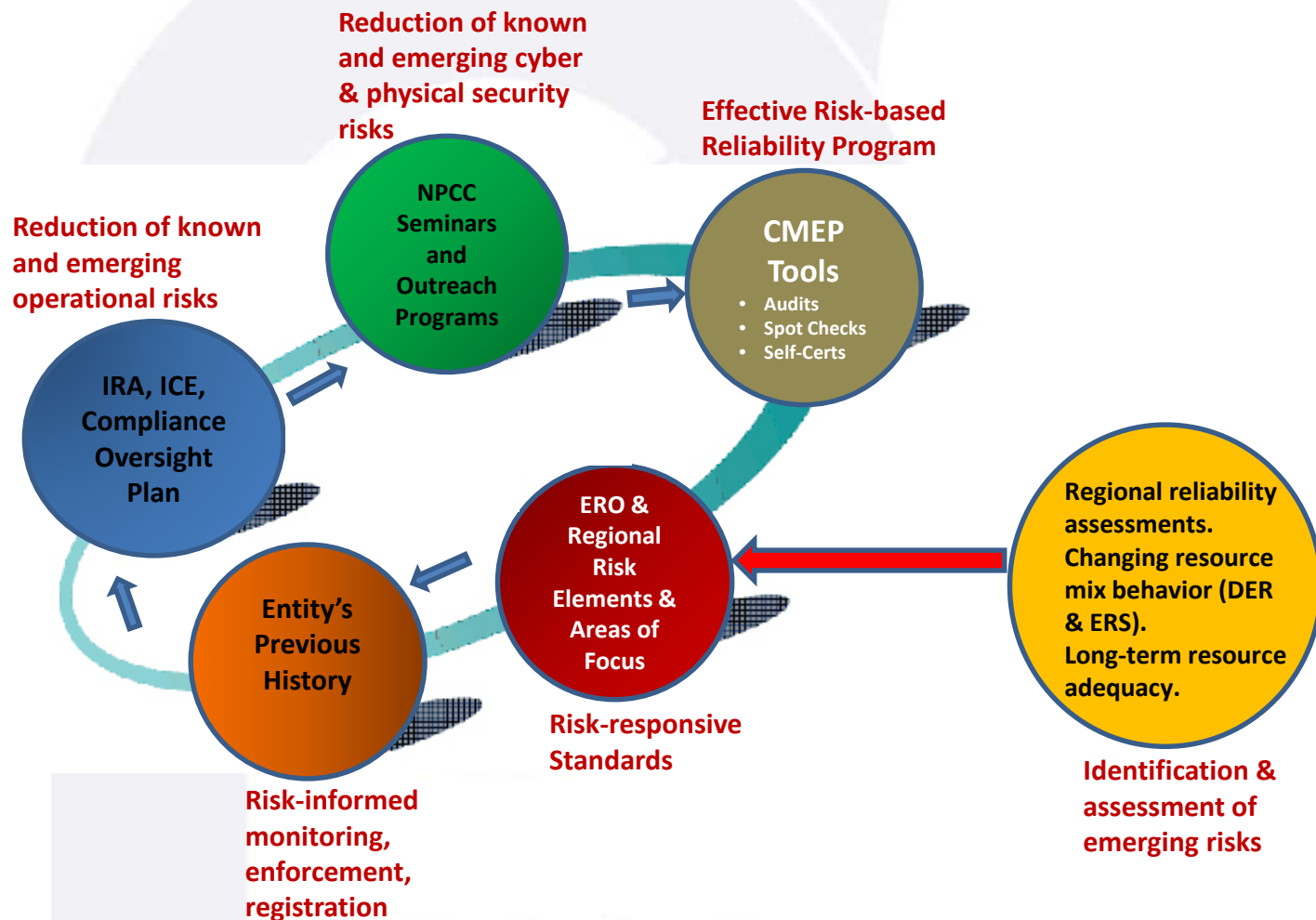


snied@npcc.org

RESILIENCY, ALIGNMENT, CONTROLS

Sal Buffamante
**NPCC 2018 Fall Compliance &
Standards Workshop**

Resiliency and Risk-Based Compliance



Resiliency

In a broad interpretation, FERC defined resiliency as: “The ability to withstand and reduce the magnitude and/or duration of disruptive events, which includes the capability to anticipate, absorb, adapt to, and/or rapidly recover from such an event.”

Therefore, NPCC plans to consider broader challenges that can affect the reliable flow of energy and how to recover from events due to known and emerging risks such as severe weather, physical and cyber attacks, accidents and fuel supply disruptions.



Resiliency



Emerging
Reliability
Risks

Reduction of
Known Risks

Cyber and
Physical
Security Risks

Effective ERO
Recovery
Operations

Risk Responsive Standards

Compliance and Control

Risk Based Reliability and CMEP Tools

ERO Alignment

The ERO Enterprise is focused on continuous improvement and alignment of Compliance Monitoring and Enforcement Program (CMEP) and Organization Registration and Certification Program (ORCP) activities. Greater alignment across the ERO Enterprise ensures effective and efficient use of resources, is important to achieving regulatory fairness, and allows stakeholders and the ERO Enterprise to focus on the most significant risks to reliability.

The ERO Enterprise Program Alignment Process relies on input from NERC's oversight and monitoring, regional observations, and registered entity reporting. The program aims to strengthen the ERO Enterprise's collaborative and transparent approach to resolving consistency issues.

ERO Alignment

Examples: TOP-001-4

R13. Each Transmission Operator shall ensure that a Real-time Assessment is performed at least once every 30 minutes.

R20. Each Transmission Operator shall have, and provide upon request, evidence that could include, but is not limited to, system specifications, system diagrams, or other documentation that lists its data exchange capabilities, **including redundant and diversely routed data exchange infrastructure** within the Transmission Operator's primary Control Center, for the exchange of Real-time data with its Reliability Coordinator, Balancing Authority, and the entities it has identified it needs data from in order to perform its Real-time monitoring and Real-time Assessments as specified in the requirement.

ERO Alignment

Examples:

TPL-001-4 Table 1, P5 Delayed fault clearing due to failure of a **Non-Redundant Relay**.

COP's Compliance Oversight Plans

One Time Attestations

Many of these issues are an outgrowth of CONFUSION in the wording of the standards or in how entities interpret the requirements.

Other Things That May Confuse You

- Why do they put braille dots on the keypad of the drive-up ATM?
- Why does your nose run and your feet smell?
- How come there aren't any “B” batteries?
- Where do people in Hell tell other people to go?

Internal Controls Evaluation

- It's **NOT** all about reduction in Audit Scope!
- An ICE results in opportunities to improve operational effectiveness / efficiency, internal controls resiliency and high reliability attainment through non-binding recommendations.

Internal Controls for Compliance

WHY?

- Incorporating Internal Controls into your operation is the next rational step in furthering Reliability
- Internal Control ARE NOT a separate set of requirements.
- Audits look at evidence for compliance such as procedures, event reporting, maintenance record, etc.
- Controls ensure the procedures and records are up to date.
- More importantly, controls ensure that action is taken when needed and in a timely manner.
- Registered entities with strong internal controls have a high likelihood of recognizing the circumstances that lead to non-compliance.

Internal Controls



ANY QUESTIONS?

FunnyPuppySite.com



Fall NPCC Compliance and Standards Workshop November 7-8, 2018

Reliability Standards Outlook

Guy V. Zito
NPCC AVP - Standards

Discussion Items:

- Overview of Standards Development RSDP
- Standards Efficiency Review
- Cost Effectiveness
- Technical Rationale for Reliability Standards
- Steady State and Periodic Reviews
- Standards Process Manual Revisions
- RISC Emerging Risks and Resilience
- Resilience and HEMP

Discussion Items cont. :

- Process and Stakeholder tools
 - Compliance Policy Guidance
 - Request for Interpretations
 - Approach to addressing DER BES Impact
- NPCC's Regional Standard
- NPCC Criteria Services
- FERC Legal Process for Standards
- NPCC Regional Standards Committee
- Future of Standards and Criteria

NERC Standards Development

- Overview-NERC Reliability Standards Development Plan (RSDP) 2019-2021, NERC Board of Trustees (BOT) Approved
 - High Priority
 - Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting CIP-008-6 (**BA, DP, GOP, GO, RC, TOP, and TO**)
 - Project 2016-02 Modifications to CIP Standards (**BA, DP, GOP, GO, RC, TOP, and TO**)
 - Project 2015-09 Establish and Communicate System Operating Limits - FAC-010, FAC-011, FAC-014 (**PC, RC, TOP, TP,) (GO, TO)**
 - Medium Priority
 - Project 2017-01 Modifications to the BAL-003-1.1 (**BA and FRSG**)
 - Project 2018-01 Canadian-specific Revisions to TPL-007-2 (**PC, TP, TO, GO**)
 - Low Priority
 - Project 2017-07 Standards Alignment with Registration
 - Project 2017-05 Periodic Review of NUC-001-3
 - Project 2017-04 Periodic Review of Interchange Scheduling and Coordination Standards - INT-004-3.1, INT-006-4, INT-009-2.1 and INT-010-2.1
 - Project 2017-03 Periodic Review of FAC-008-3

NERC Standards Development

– Additional Considerations

- Reliability Issues Steering Committee (RISC)
- Essential Reliability Services Task Force (ERSTF) recommendations
- Industry Feedback Loops (e.g. Events Analysis, Compliance, RAPA)
- IEEE 1547 and VER Modeling
- Standards Efficiency Review
- Standards Grading
- DOE Report and NOPR to FERC (Resiliency concerns)
- High Impact Low Frequency events

Standards Efficiency Review (SER)

Two Phase Approach

- Phase 1:
 - Focused primarily on retirements
 - More straight-forward retirements
 - Draft SAR posted for informal industry comment proposed ~114 requirements for retirement
 - Phase 1 work complete for team upon submitting SAR
- Phase 2:
 - Alternatives to retirement
 - Consolidation of requirements
 - Modifications of requirement or dependent on another
 - CCC and SC members to supplement SER team

Standards Efficiency Review

Phase 1

- Revised SAR submitted to Standards Committee
- SAR posted for formal comment
- Appoint Project 2018-03 SER Drafting Team – (October 17, 2018 - SC)
- Industry ballots on proposed retirements to standards (2018 Q4 – 2019 Q1)
- Propose balloted standards to NERC Board of Trustees – 2019 Q2

Standards Efficiency Review

Phase 2

- Form SER Phase 2 team by supplementing with new CCC & SC members (complete)
- Clarify scope of work for Phase 2 (complete)
- Identify key issues to address with Advisory Group (complete)
- Review alternatives and concepts proposed by Phase 1 (2018 Q4)
- Develop new efficiency concepts (2018 Q4 to 2019 Q2)
- Evaluate and identify best efficiency concepts (2019 Q2-Q3)
- Draft SAR(s) or implement concepts (2019 Q4)

Cost Effectiveness

- Cost Effectiveness:
 - Analysis of the Risk being reduced
 - Cost associated with reducing that risk
 - Cost associated with not reducing the risk (reliability and societal if possible)
 - Standards Drafting Teams, Periodic Review Teams, and Standards Grading
 - **Drafting Teams asked to develop alternatives**
 - **Add question(s) to the Comment forms**
 - Application to all Standards projects

Technical Rationale for Reliability Standards

- Technical Rationale Transition Plan
 - Track 1 and 2 (CGP?)
- Remove from Reliability Standards (supporting documentation)
 - Guidelines and Technical Basis
 - Technical Rationale
 - Implementation Guidance
- FERC Approved parts of the Standard (mandatory and enforceable)
 - **Applicability**
 - **Requirements**
 - **Implementation Plan**
 - **Effective Date**
 - **VRFs and VSLs**
- May contain Compliance Guidance but not processed through the CGP
- Supporting Documents Section 11 of the SPM
- To be located with Standards to which they apply but as separate documents
- All standards going forward
- GTB Teams will begin the process of review of supporting documentation from the standards.

Steady State and Periodic Review

- Steady State
 - Core set of Results-based Standards
 - All previous FERC Directives addressed
 - Independent Expert Review Panel recommendations considered
 - Meets “Ten Benchmarks of Excellence”
 - All Paragraph 81 identified issues addressed
- Periodic Reviews
 - Cross Functional Team of NERC Standing Committee Chairs, Staff, Regional Entities, and others to review standards
 - All enforceable standards in effect for a year or more
 - Subject Matter Expert Teams as required
 - Expedited, efficient and effective period review of standards
 - Regional Standards-Variations? Retirements?
 - Costs

Steady State and Periodic Review

- Grading in 2018- 53 Requirements
 - CIP-014-2 Physical Security
 - COM-002-4 Operating Personnel Communications Protocols
 - FAC-003-4 Transmission Vegetation Management
 - FAC-013-2 Assessment of Transfer Capability for the Near-Term Transmission Planning Horizon
 - IRO-006-5 Reliability Coordination — Transmission Loading Relief (TLR)
 - MOD-020-0 Providing Interruptible Demands and Direct Control Load Management Data to System Operators and Reliability Coordinators
 - MOD-025-2 Verification and Data Reporting of Generator Real and Reactive Power Capability and Synchronous Condenser Reactive Power Capability
 - MOD-026-1 Verification of Models and Data for Generator Excitation Control System or Plant Volt/Var Control Functions
 - MOD-027-1 Verification of Models and Data for Turbine/Governor and Load Control or Active Power/Frequency Control Functions
 - MOD-028-2 Area Interchange Methodology
- 2018 Final grades – 2019-2021 Reliability Standards Development Plan

Standards Process Manual Revisions

- **Sections with substantive revisions:**
 - Section 6 “Process for Conducting Field Tests”
 - Section 7 “Process for Developing an Interpretation”
 - Section 11 “Process for Approving Supporting Documents”
- **Sections with minor revisions:**
 - Section 2.1 “Definition of a Reliability Standard”
 - Section 3.7 “Governmental Authorities”
 - Section 8 “Process for Appealing an Action or Inaction”

Reliability Issues Steering Committee (RISC) and Emerging Risks

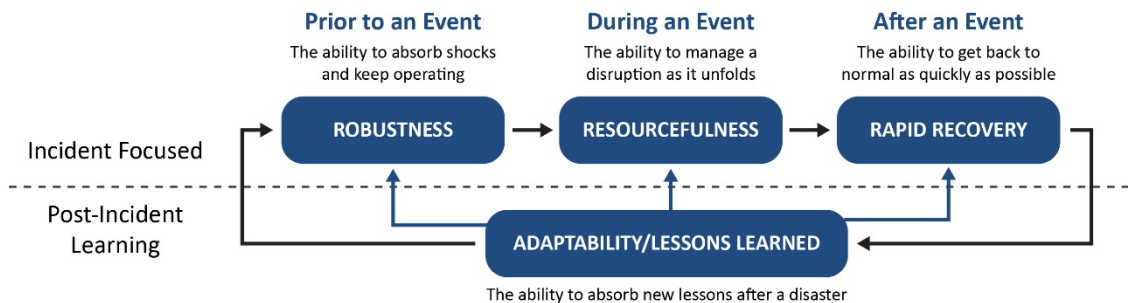
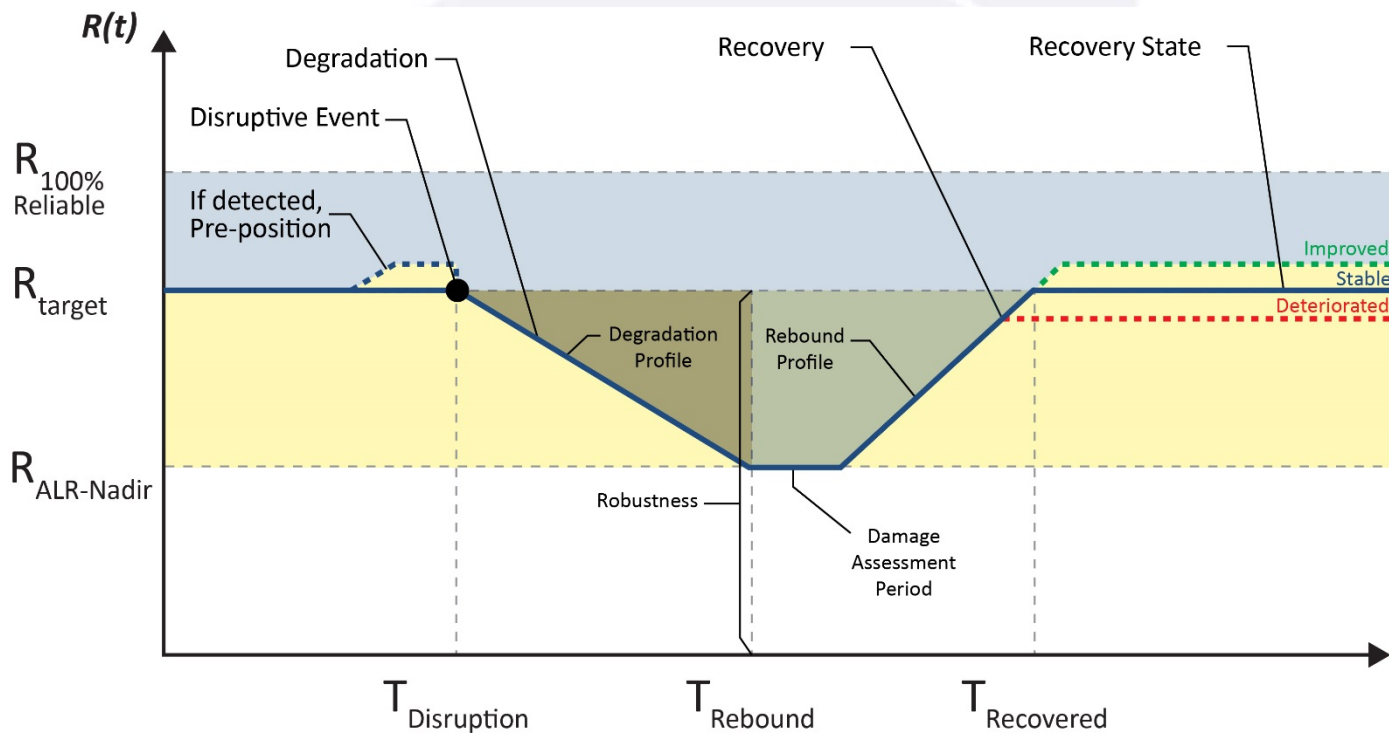
“ERO Reliability Risk Priorities,” – 2018 BOT Approved Report - Risks Identified and a potential framework for Resilience

- Risk Profile #1: Changing Resource Mix (**High**)
- Risk Profile #2: Bulk-Power System Planning (**High**)
- Risk Profile #3: Resource Adequacy and Performance (**High**)
- Risk Profile #9: Cybersecurity Vulnerabilities (**High**)
- Risk Profile #4: Increasing Complexity in Protection and Control Systems and Asset Management (**Moderate**)
- Risk Profile #6: Loss of Situational Awareness (**Moderate**)
- Risk Profile #7: Extreme Natural Events (**Moderate**)
- Risk Profile #8: Physical Security Vulnerabilities (**Moderate**)
- Risk Profile #5: Human Performance and Skilled Workforce (**Low**)

Resilience

- Four outcome-based abilities of resilience (framework) are as follows:
 - **Robustness** – the ability to absorb shocks and continue operating
 - **Resourcefulness** – the ability to **detect and manage a crisis as it unfolds**
 - **Rapid recovery** – the ability to get services back as quickly as possible **in a coordinated and controlled manner and taking into consideration the extent of the damage**
 - **Adaptability** – the ability to incorporate lessons learned from past events to improve resilience
- Ken McIntyre – FERC Chairman-“Top priority of the Commission” address concerns- DOE Staff Report and NOPR”
- FERC terminated the DOE NOPR and developed a FERC NOPR
 - what resilience of the bulk power system means and requires;
 - understand how each RTO and ISO assesses resilience in its geographic footprint; and
 - use this information to evaluate whether additional Commission action regarding resilience is appropriate at this time.
- RISC Report on Resilience

Resilience



Resilience and HILF

Electromagnetic Pulse (High Altitude “HEMP”)

- Three components of a HEMP E1, E2, and E3
- The E1 component is a very brief but intense electromagnetic field that can quickly induce very high voltages in electrical conductors. Most destructive.
- The E2 and E3 generally well understood; E2 similar to lightning and E3 similar to GMD. Starfish Prime studies in 1962. E3 understanding resulted in revision to TPL-007 and supplemental analysis-increase in the studied electric field.
- Creates an artificial radiation belt (Satellite risk)

Electromagnetic Pulse (High Altitude “HEMP”)

- Electric Power Research Institute EPRI Study of E1
 - Study to be released Spring 2019
 - Study uses wave guides and direct injection
 - Study will recommend cost effective mitigation methods to harden the grid against E1
- FERC
 - Waiting for study
 - Potential for a NOPR to address possible BES E1 risks
 - Potential for a similar approach as GMD, one for operational and one for planning (i.e. EOP-010 and TPL-007)
 - Critical facility list development identifying where potential weaknesses may exist

Compliance Guidance Policy

Compliance Guidance Policy-a Standards perspective:

- Process for developing approaches useful in providing guidance for implementing standards
- November 4-5, 2015 BOT approvals (NERC Comp. and Enf. Webpage)
- Two Types of Guidance:
 - CMEP Implementation Guidance:
 - Approaches on how entities could comply with standards
 - Led and developed by SME; vetted by pre-approved organizations, not NERC
 - Not necessarily the only approach to comply with a standard
 - Endorsed for Deference by the ERO
 - CMEP Practice Guide-Auditor Instructions
 - Initiated by ERO Policy
 - Initiated by ERO in response to a specific issue
- Section 11-"Process for Approving Supporting Documents" of the SPM under revision
- Upon ERO approval, provides compliance deference

Compliance Guidance Policy Pre-approved Orgs.

- American Public Power Association (APPA)
- Canadian Electricity Association (CEA)
- Edison Electric Institute (EEI)
- Electricity Consumers Resource Council (ELCON)
- Electric Power Supply Association (EPSA)
- ISO/RTO Council
- Large Public Power Council (LPPC)
- National Association of Regulatory Utility Commissioners (NARUC)
- National Rural Electric Cooperative Association (NRECA)
- North American Generator Forum (NAGF)
- North American Transmission Forum (NATF)
- Northwest Public Power Association (NWPPA)
- Transmission Access Policy Study Group (TAPS)
- Western Interconnection Compliance Forum (WICF)
- NERC Planning Committee (PC)
- NERC Operating Committee (OC)
- NERC Critical Infrastructure Protection Committee (CIPC)
- Regional Entity Stakeholder Committees

Standards Interpretations

Request for Interpretation (RFI):

- Standard Processes Manual (SPM) Section 7 outlines the process for developing an interpretation. Eight criteria for rejecting a request.
- A valid interpretation provides additional clarity about one or more requirements, but does not expand on any requirement and does not explain how to comply with any requirement.
- Any entity that is directly and materially affected by the reliability of the North American Bulk Power Systems may request an interpretation.
- The NERC Standards and Legal staff shall make a recommendation to the Standards Committee whether to accept the Request for Interpretation (RFI).

Standards Interpretations

Request for Interpretation (RFI) cont.:

- Reasons to reject RFIs Section 7 SPM
 - Requests approval of a particular compliance approach;
 - Identifies a gap or perceived weakness in the approved Reliability Standard;
 - Where an issue can be addressed by an active standard drafting team;
 - Where it requests clarification of any element of a Reliability Standard other than a Requirement;
 - Where a question has **already been addressed in the record**;
 - Where the Interpretation identifies an issue and proposes the development of a new or modified Reliability Standard, (such issues should be addressed via submission of a SAR);
 - Where an Interpretation seeks to expand the scope of a Reliability Standard; or
 - Where the meaning of a Reliability Standard is **plain on its face**.

Approach to Addressing DER

Stakeholder tool developed by the Regional Standards Committee to document DER issues identified and pursue how they be addressed. Posted on NPCC Website.

- 1) Issue Identification (Stakeholder, RAPA, or Event Analysis)- Form
- 2) Evaluation (Preliminary screen, Scope, Type, Importance)- RSC and RCC
- 3) NERC or Regional solution, Recommendation (NPCC action taken?)

NPCC Regional Standards

- PRC-006-NPCC-1 Revision to:
 - Review for potential revisions made necessary by:
 - NERC PRC-006-1/PRC-006-2 Automatic Underfrequency Load Shedding
 - NERC PRC-024-1/PRC-024-2 Generator Frequency and Voltage Protective Relay Settings standards.
 - Review for Dispersed Generation (DG) issues
 - Draft developed to enable retirement of NPCC Directory 12 on UFLS
 - Three 45-day formal postings for comments
 - 30 day pre-Ballot Review and 10 + day ballot in fourth quarter 2018

Criteria Services Program Area 2018 Initiatives

- A-10 Classification of BPS Elements
- Strategic Review of NPCC Criteria
- Remedial Action Schemes (RAS)

A-10 BPS Classification

Scope of Review:

- Identify critical facilities for the applicability of NPCC criteria
- Simplify the existing methodology to make it less labor intensive Improve consistency across areas in application and outcomes

Phase #1 2017:

- Review Existing Methodology
- Propose Improvements
- Propose New Methodologies
- Recommendation to the RCC for Testing of three methodologies.

Phase #2 2018:

- Testing of 3 RCC Approved Methodologies.
- RCC Endorsement of a Preferred Methodology December 2018

Anticipated 2019 Activity:

- Revise A-10 Document
- Open Process Postings
- Full Member Ballot

Strategic Review of NPCC Criteria

- Strategic Review of the Need for NPCC More Stringent Criteria.
 - Directed by the NPCC Board of Directors.
 - Arranged by Focus Area
 - Operations
 - Planning
 - Protection
 - High Level
 - Not Directory Specific or Requirement by Requirement.
- Action Plan and Scope Approved April 2018.
 - Task Force Review August 2018.
- RCC and RSC Review and Comment September 2018.
- Final Report to RCC and RSC December 2018.

NPCC Transition from SPS to Remedial Action Schemes (RAS)

- NPCC Transition to RAS (PRC-012-2, Remedial Action Schemes- replaces PRC-012-2 will replace PRC-015-1 and PRC-016-1, PRC-012-1, PRC-013-1, and PRC-014-1):
 - Existing NPCC RAS/SPS List:
 - SPS that conform to Revised Definition of RAS
 - SPS does not conform
 - Newly Identified RAS
 - Regional Review.
 - NPCC Glossary Term SPS (proposed)
 - ‘See NERC RAS’
 - NPCC Directory #7 –Appendix B
 - Other NPCC Documents
 - Posting Revised Glossary term and Directory 7, Spring 2019

Legal Procedural Information for Standards (US)

- NERC Board of Trustees (BOT) Approves Standard
- NERC Files a Petition with FERC and Canadian Regulatory Authorities.
- FERC elects RM or RD (RM Rulemaking-NOPR) no time requirement for FERC to act
- NOPR – **60 days to comment**
- FERC Final Order Date (Date the Order is Issued)
- Federal Register Publication Date – Effective Date of the ORDER (not the Standard) . This is the “Commission Approval Date”
- Effective Date of the Standard is usually defined in the Petition filed by NERC, e.g. “effective on the first day of the first calendar quarter that is XXX months after Commission Approval Date”
- Implementation Plan
- **Request for Rehearing of a Final Order can be requested within 30 days of FERC Final Order Date** (not Commission approval date)
 - FERC must act on a rehearing request within 30 days and if no action is taken the rehearing request is deemed denied
 - FERC can delay its action on this indefinitely
 - FERC almost always delays action
 - Request for rehearing does not impact the Commission approval date
 - **Preserves right to appeal to Court**

NPCC Regional Standards Committee

- Interface with RISC- emerging issue identification
- Review and comments on NERC/ERO and Eastern Interconnection Regional Standards
- Develops Ballot Recommendations for NERC/ ERO Standards and Interpretations
- Participates in NERC Standards drafting and influence processes through various groups-formal and informal
- Oversees the Development and Maintenance of NPCC Regional Standards
- Oversees the Development and Maintenance of NPCC Regional Directories
- Regional Delegation Agreement-Standards Program Area
- Review all FERC Orders, Rulings, NOPRs and Petitions related to Standards
- Participates in Feedback loop mechanisms to improve standards

Future of Standards and Criteria

- Standards will all undergo EPR and be graded
- Standards will be reviewed for “efficiency”
- Increased emphasis on cost and justification of standard-based solutions
- Standards Metrics-are standards improving? Is reliability improving? Feedback Loops and consistency
- Risk “informed” solutions
- Increased Continent-wide vs. Regional solutions
- Increased informal consensus building and development
- As standards improve-less Regional criteria
- Criteria review will include cost effectiveness analysis

“Intelligence is the ability to adapt to change.”- Stephen Hawking



Stephen Hawking (Jan 1942-March 2018)

Questions or Comments ?



Engaging the Unengaged

Attain extreme employee engagement for your compliance program.



Northeast Power Coordinating Council, Inc.

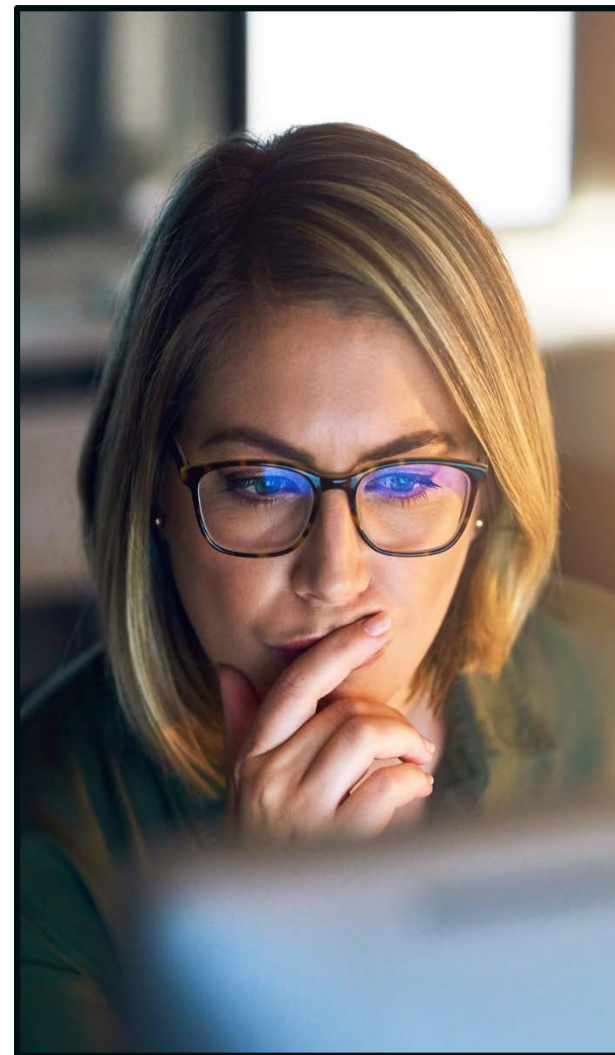
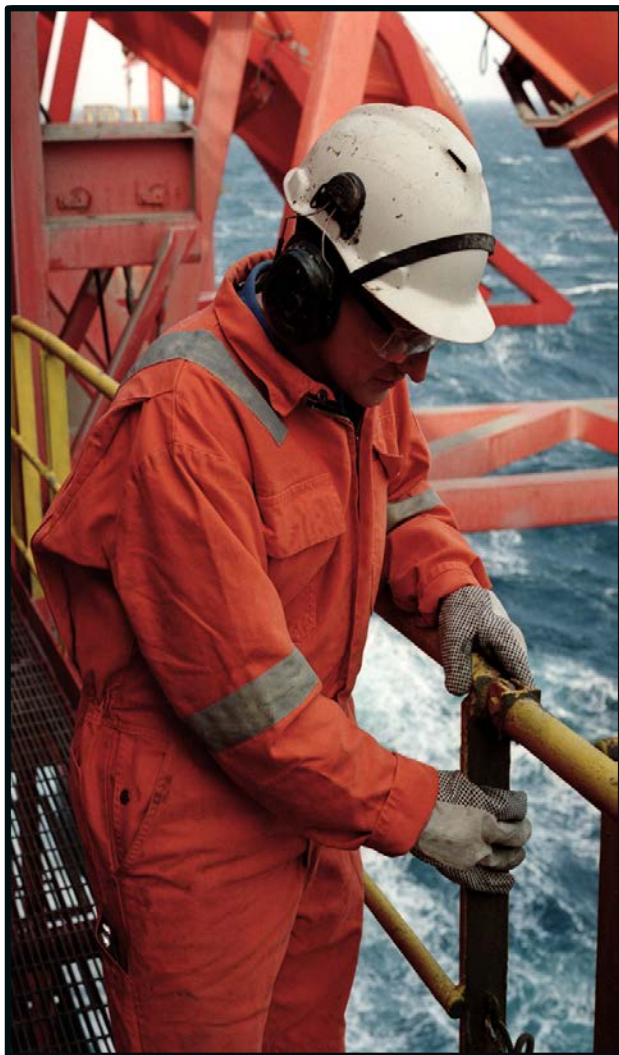
Fall 2018 NPCC Compliance and Standards Workshop

Who is MetaMythic?



We equip and engage people
when it really counts







Agenda

Let's get those neurons prepped

My Mission – To Equip You

Case Studies – A Tale of Two Utilities

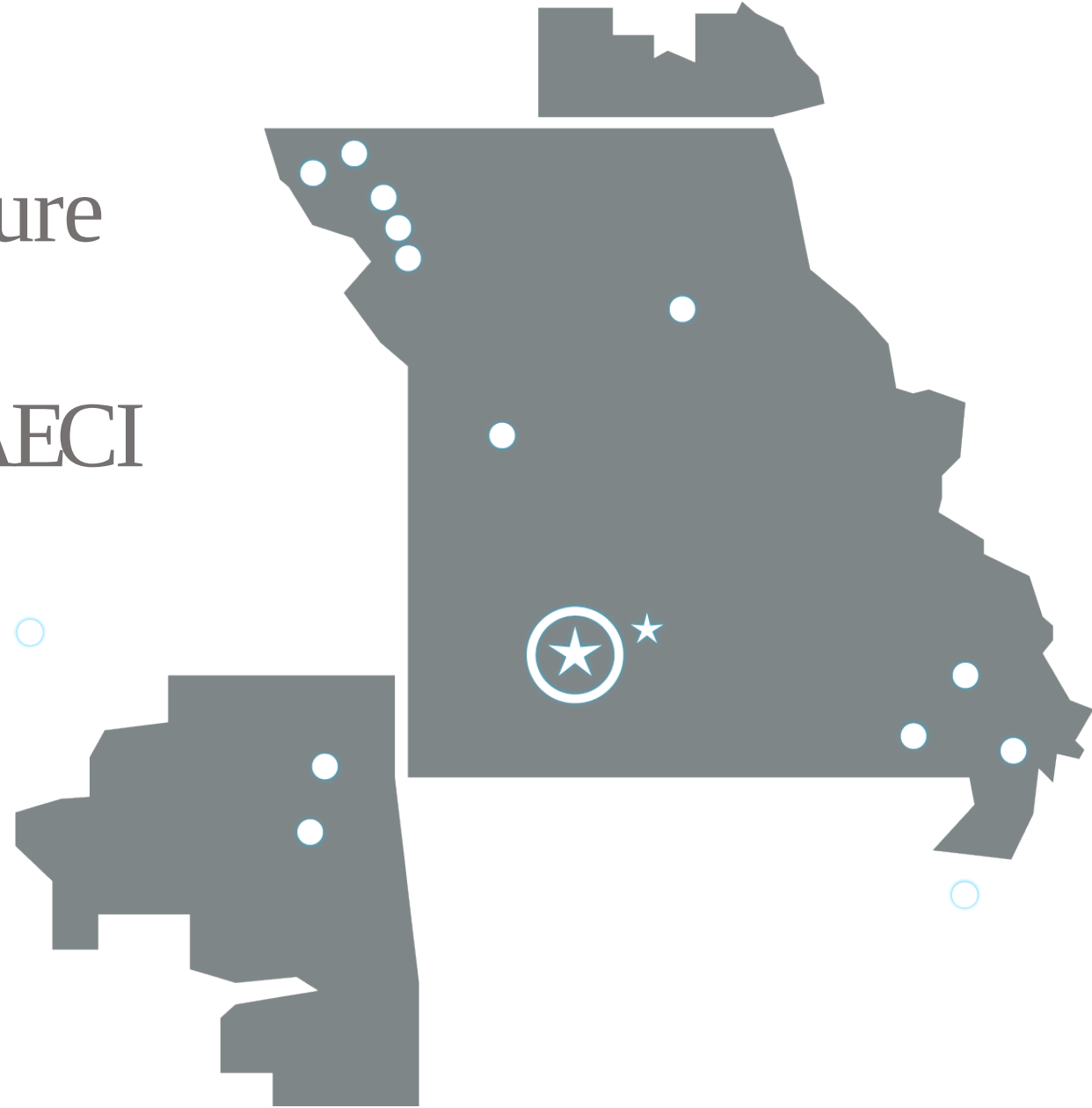
Take-Homes - From our Methodology



THE PROBLEM

The new Critical Infrastructure Protection (CIP) Standards have severe penalties for AECl non-compliance...

...and we're making mistakes because employees are **fearful and ill-equipped**



THE RESULTS

0 Self-Reports

0 Violations

0 Findings

For 5 years

employees are fearful

engaged and

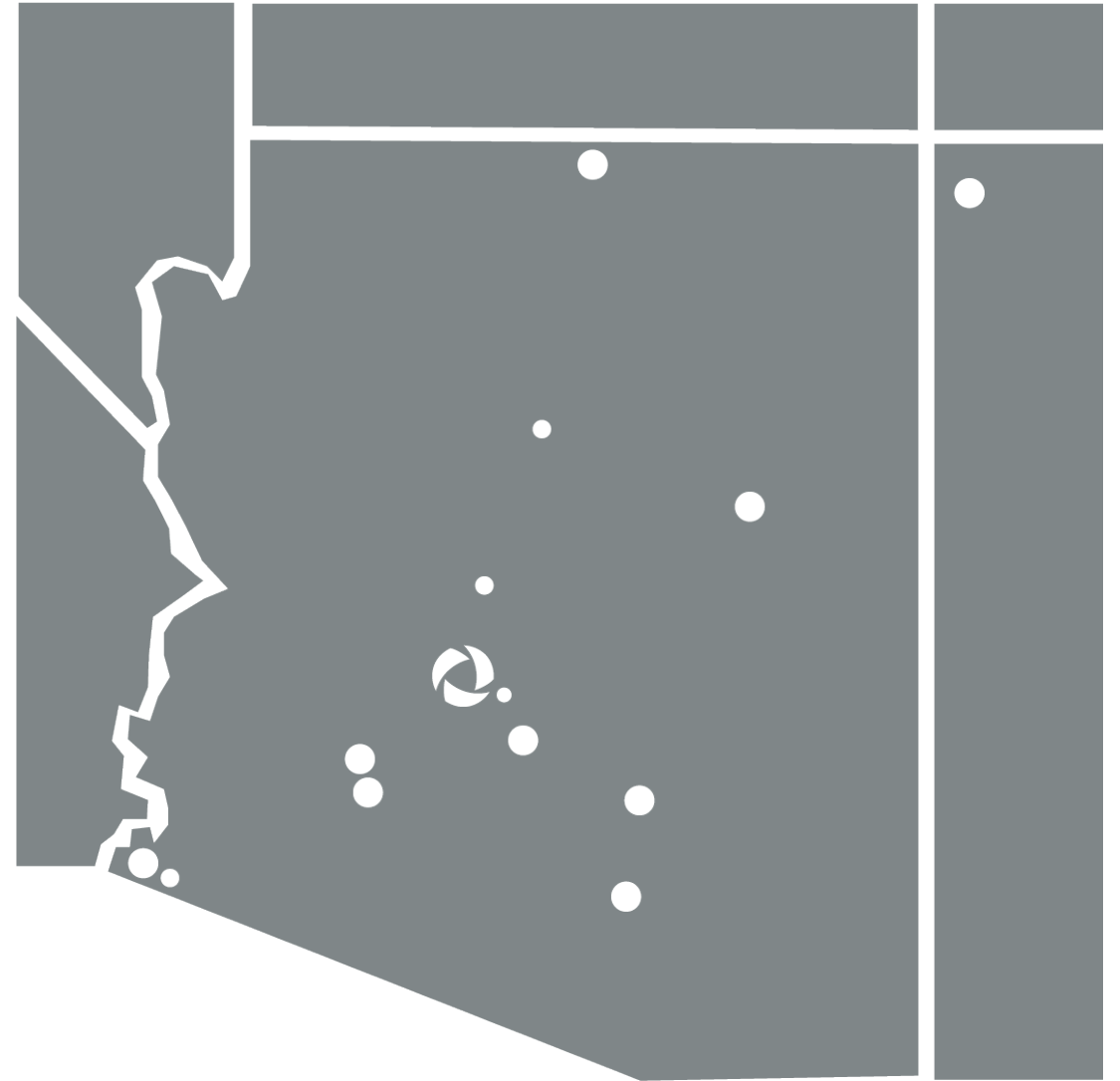
equipped



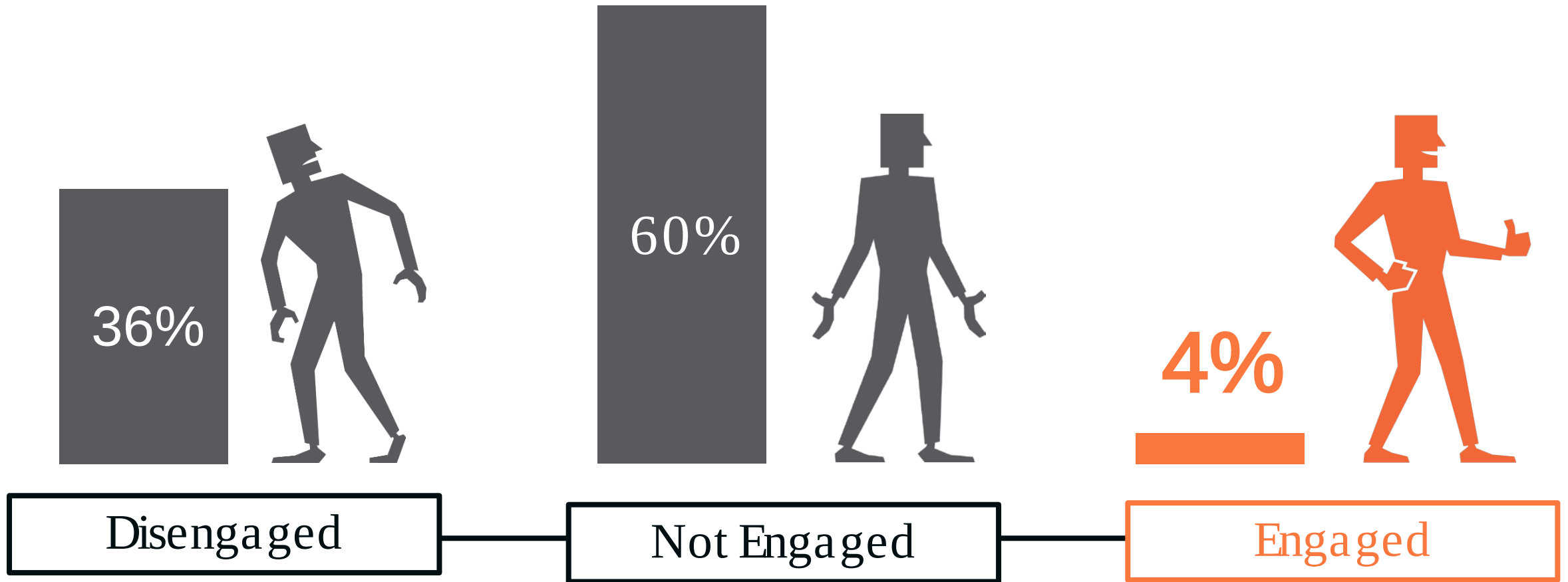
THE PROBLEM

The new Critical Infrastructure Protection (CIP) Standards have severe penalties for APS non-compliance...

...and we're making mistakes because employees are **apathetic and hostile**



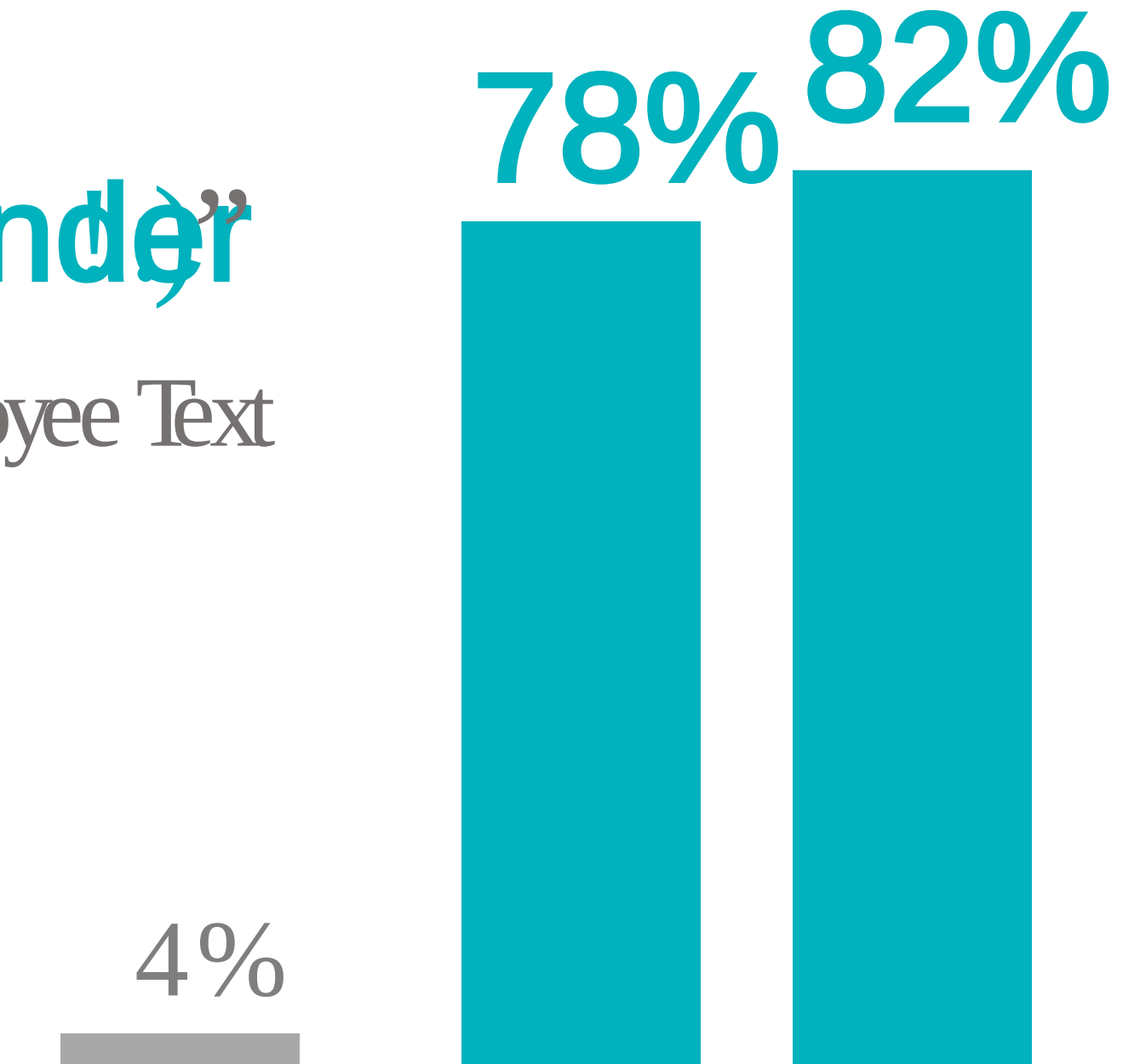
THE RESULT BEFORE



THE RESULT-SAFTER

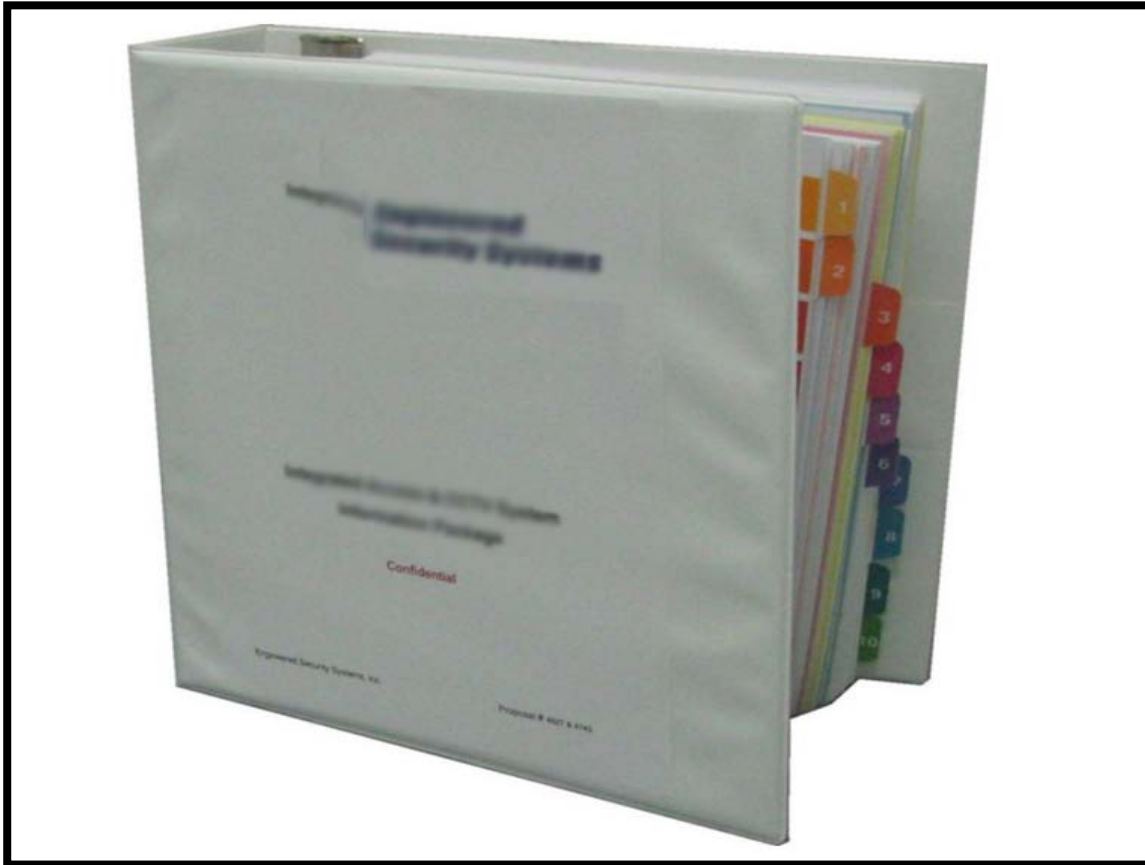
“I am a **CIP Defender**”

—Actual Employee Text



STANDARD TRAINING

Company Handbook



Company E-Learning

Security Management Controls

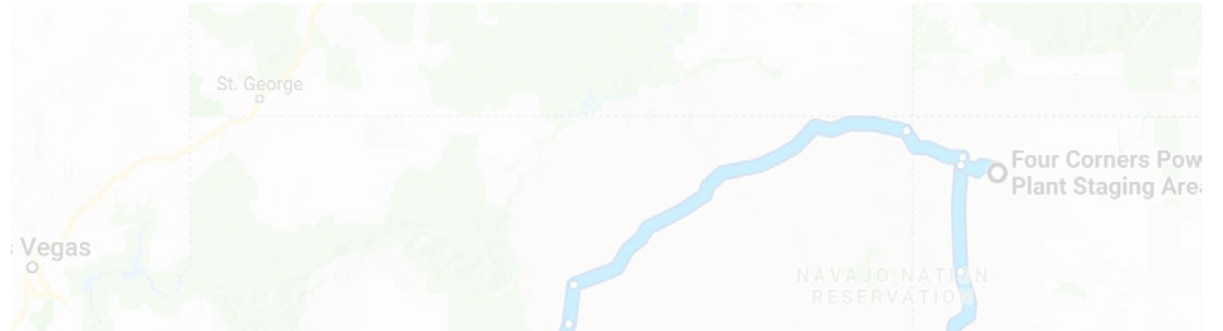
Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:

- R1.1.** The cyber security policy addresses the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.
- R1.2.** The cyber security policy is readily **available to all personnel** who have access to, or are responsible for, Critical Cyber Assets.
- R1.3.** **Annual review and approval** of the cyber security policy by the senior manager assigned pursuant to R2.



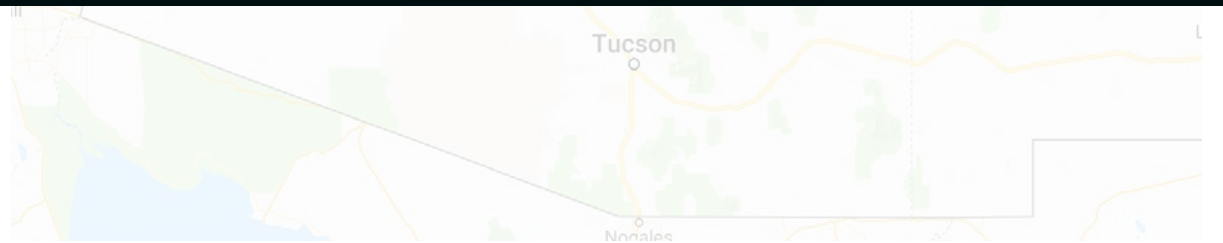
THE QUEST

825 Miles



E-LEARNING!

And we had the answer....



THE SOLUTION

E-Learning & a handbook!

No seriously...

Security Management Controls

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 through CIP-009, including provision for emergency situations.
- R1.2.** The cyber security policy is readily **available to all personnel** who have access to, or are responsible for, Critical Cyber Assets.
- R1.3.** **Annual review and approval** of the cyber security policy by the senior manager assigned pursuant to R2.



THE SOLUTION

THE DUTY ROSTER

A booklet included with this Guide catalogues the CIP responsibilities specific to each chapter. After completing a chapter, look up the corresponding duty roster to see your current status.



the PSP

Immediate Buff to All Physical Defenses
+5 against Boot Force Attack, Ion-Gattling Pistol, and Articulated Finger Lance



the ESP

Shkazow! Fortify the Void!
+5 Defense against VirusBots, Electromagnetic Punch, and Ether Trunkets



How To Plan A Romantic Update



1. Install in Test System



2. Compliance Documentation



3. Install in Production



Hardware: EliteStation 754
OS: Encom12
Software:
OperatorVision Control System v6.8
KillBot AntiVirus v11.4

4. Update Baseline Configuration

To the Duty Roster!



TAKEHOME INSIGHT

Discover the Cast



“**We** should help people see themselves as the **hero** of achieving a great **business objective**”

- Chad Hodge, Screenwriter

Your People

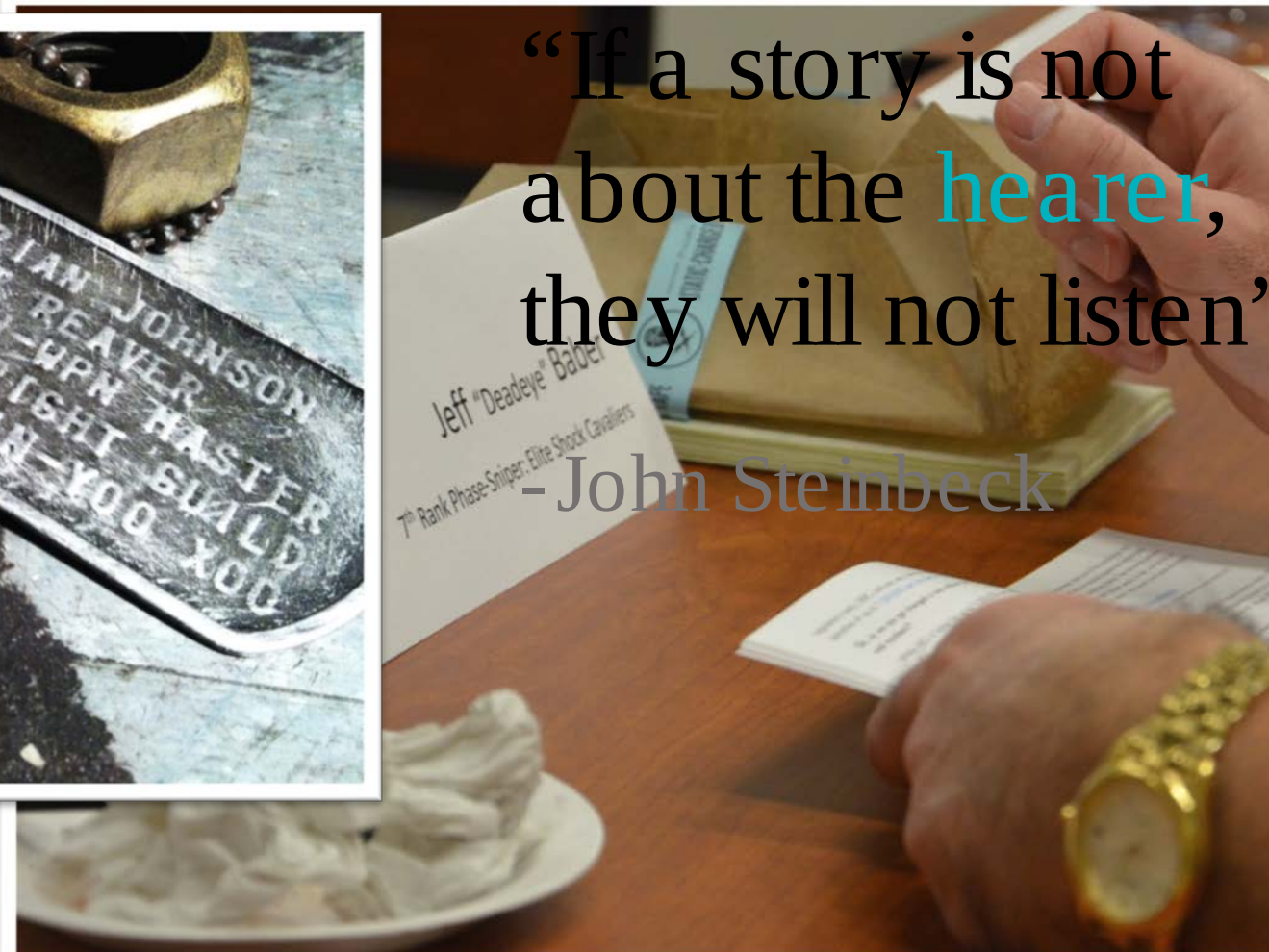
You





“If a story is not about the **hearer**, they will not listen”

- John Steinbeck



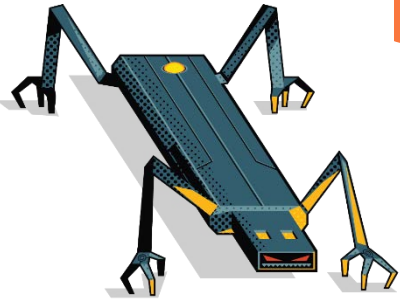
“A villain must excite
our aversion, arouse
our fear, and awaken
some transient gleam
of sympathy.”

- Agnes Repplier





“All your access are
belong to me.”



“I’ll show you
my source code
if you show me
yours...”



“critical
cyber assets
..nom nom
nom”





TAKEHOME INSIGHT

Map the Learning Journey





Start Big

① THE BIG TRUTH

The CIP standards are an opportunity for APS to equip our people to protect the infrastructure we've built over 100 years to deliver reliable power to the people of Arizona.

③ THE BIG GOAL

Everyone believes CIP positively impacts the reliability and security of our power grid, and knows their role in the cyber-security mission.

② THE BIG PROBLEM

Employees are apathetic or hostile about CIP: they are concerned about increased workload, afraid of making a mistake, and distrustful of the CIP team.

④ THE BIG MEASURE

Everyone can explain how their role is critical for the reliability/security of our power grid through CIP, and then demonstrate their CIP duties.





The Who

HEROES

IT Engineers

Design and support infrastructure for enabling operations of the grid.

Plant Operators

Operate and monitor the plant, perform rounds, work in the plant control room, plant floor and switchyard.

SAGES

Lisa Carrington

Responsible for ongoing related comms, tasked with implementing CIPv5 at APS.

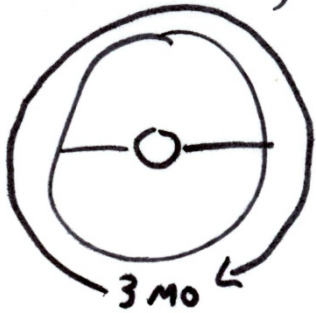
Cyber-Security Team

Provides interpretation of CIP standards and support defining duties for job roles

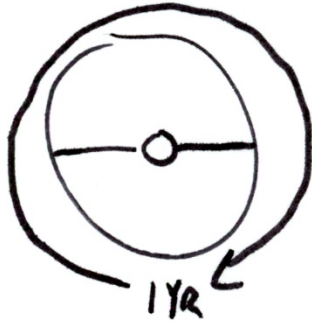


The How

NEWSLETTER
(QUARTERLY)



E-LEARNING
(LMS)

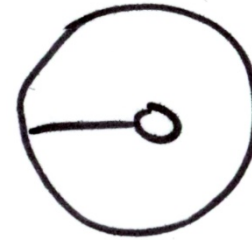


SIGNAGE
(PHYSICAL + DIGITAL)



UPDATED QUARTERLY

CREW CARDS

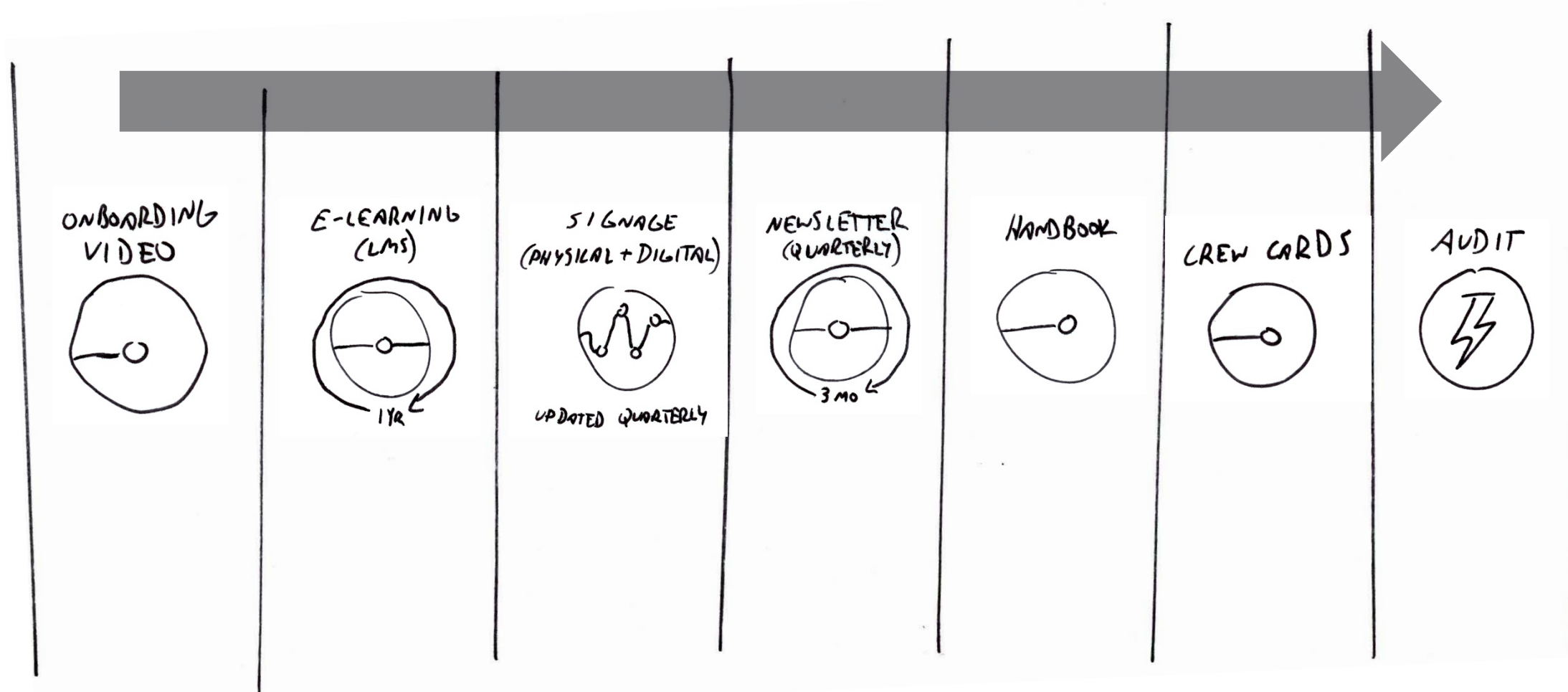


AUDIT





The Learning Journey





The Learning Map

① THE BIG TRUTH

The CIP standards are an opportunity for APS to equip our people to protect the infrastructure we've built over 100 years to deliver reliable power to the people of Arizona.

③ THE BIG GOAL

Everyone believes CIP positively impacts the reliability and security of our system, and knows their role in the cyber-security mission.

② THE BIG PROBLEM

Employees are apathetic or hostile about CIP: they are concerned about increased workload, afraid of making a mistake, and distrustful of the CIP team.

④ THE BIG MEASURE

Can positively explain how their role increases the reliability/security of our power grid through CIP, and then demonstrate their new abilities.

HEROES

IT Engineers

Design and support infrastructure for enabling operations of the grid.

Plant Operators

Operate and monitor the plant, perform rounds, work in the plant control room, plant floor and switchyard.

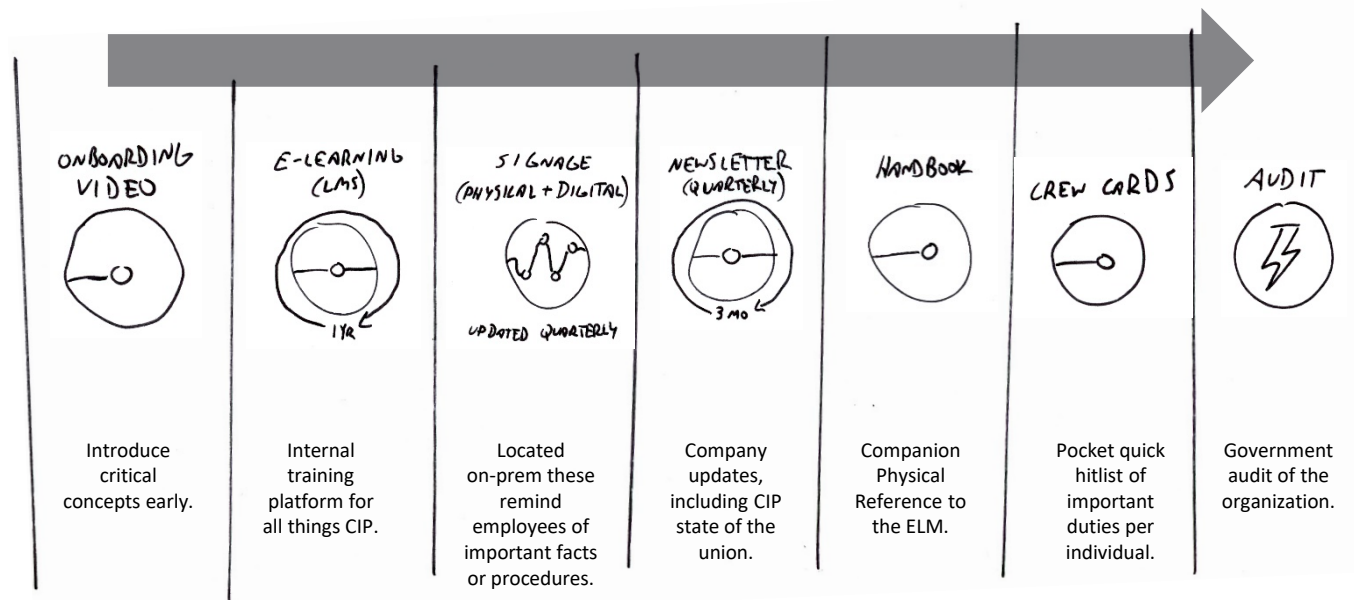
SAGES

Lisa Carrington

Responsible for ongoing related comms, tasked with implementing CIPv5 at APS.

HR and Marketing

In charge of the LMS/corporate training and internal comms respectively.





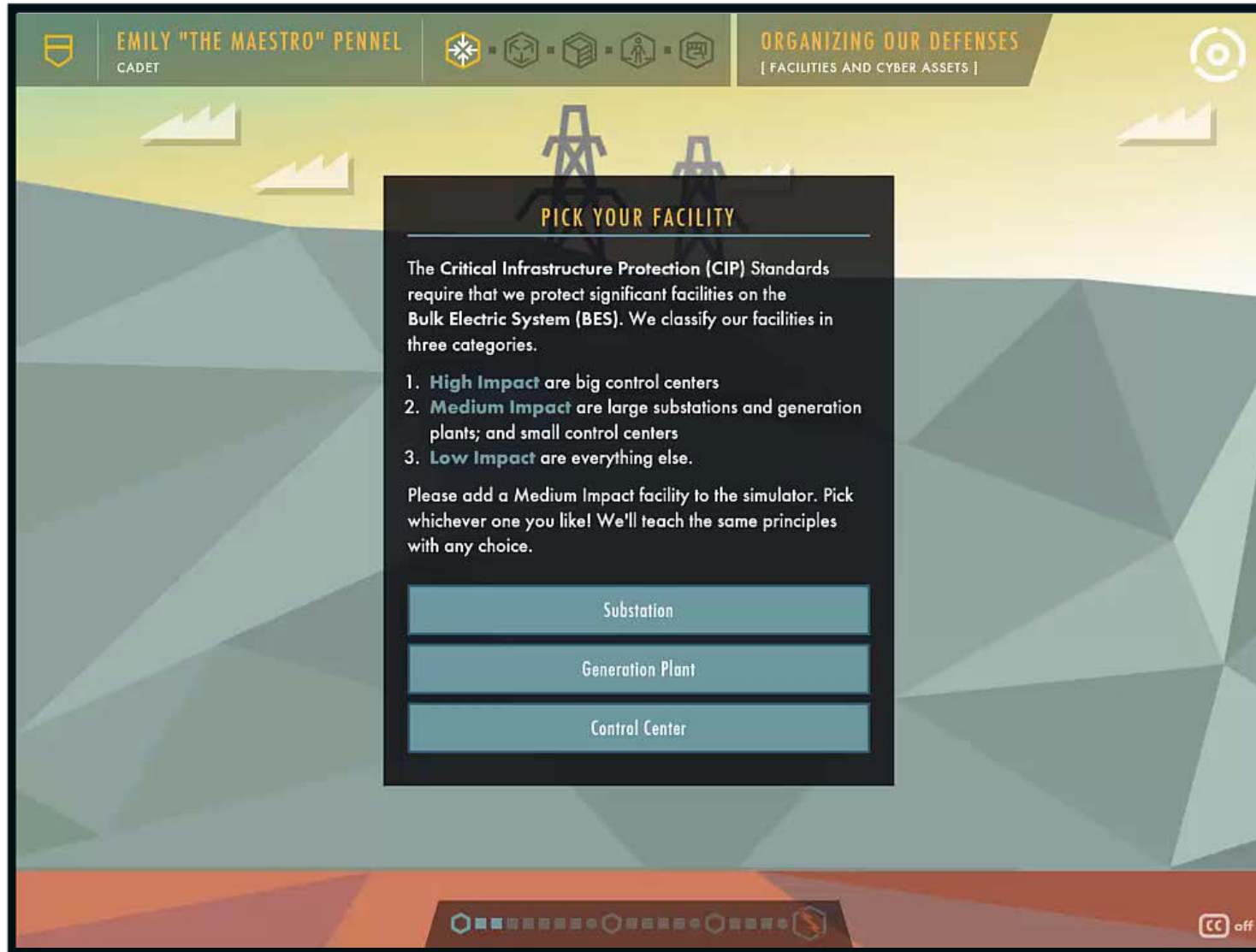
TAKEHOME INSIGHT

Design Each Experience From the Hero-Out

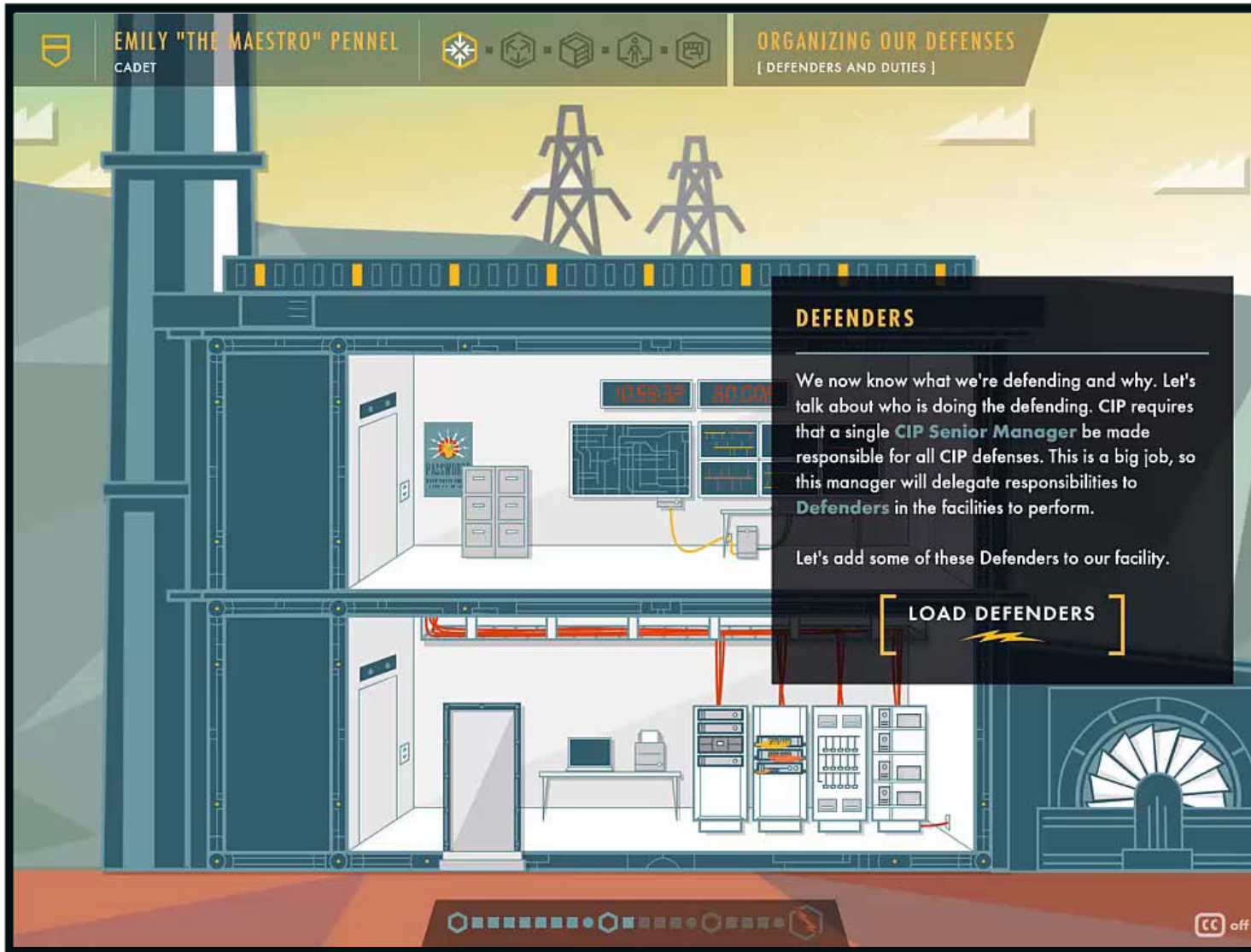




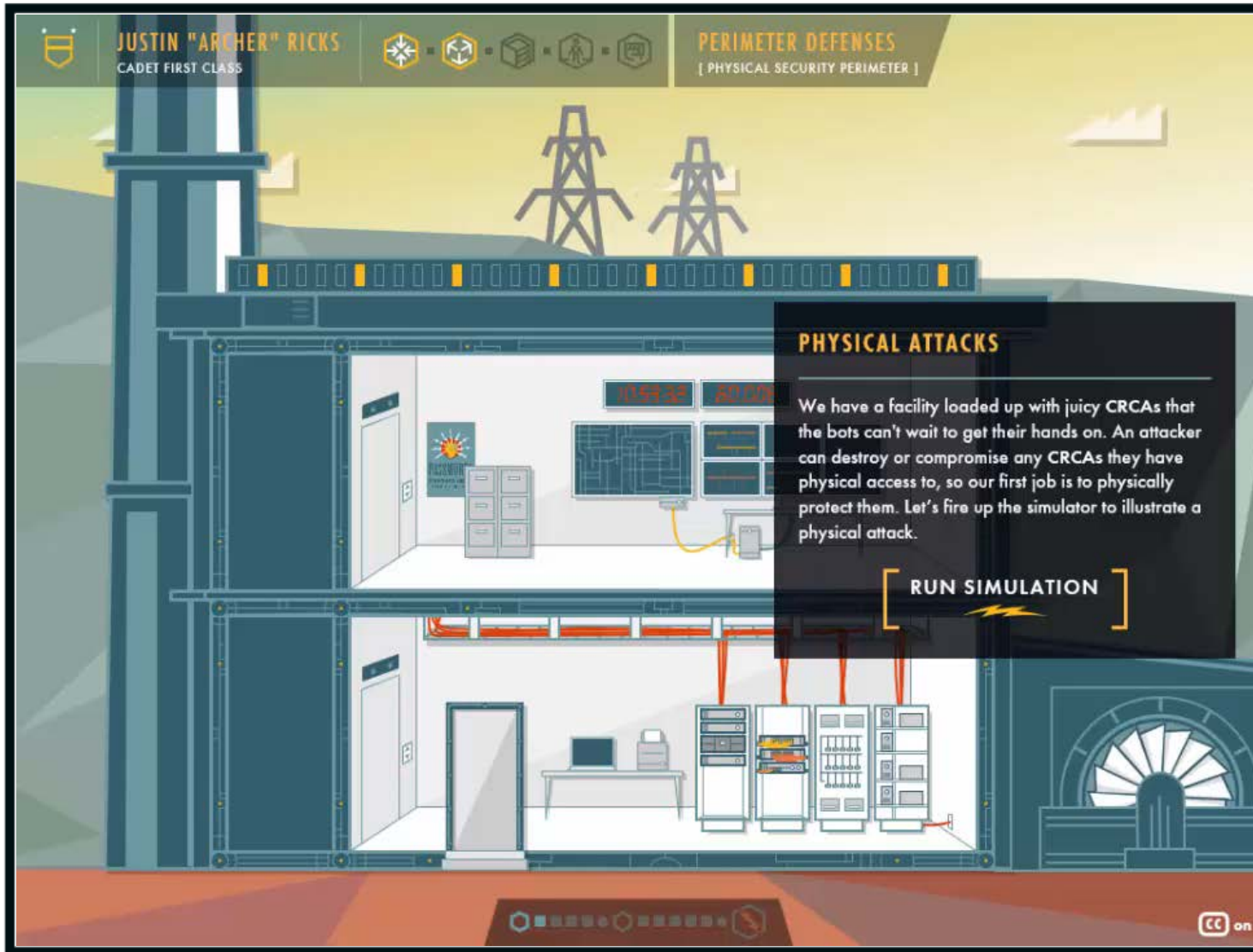
**Give clarity on
the hero and
sage identities
up-front**



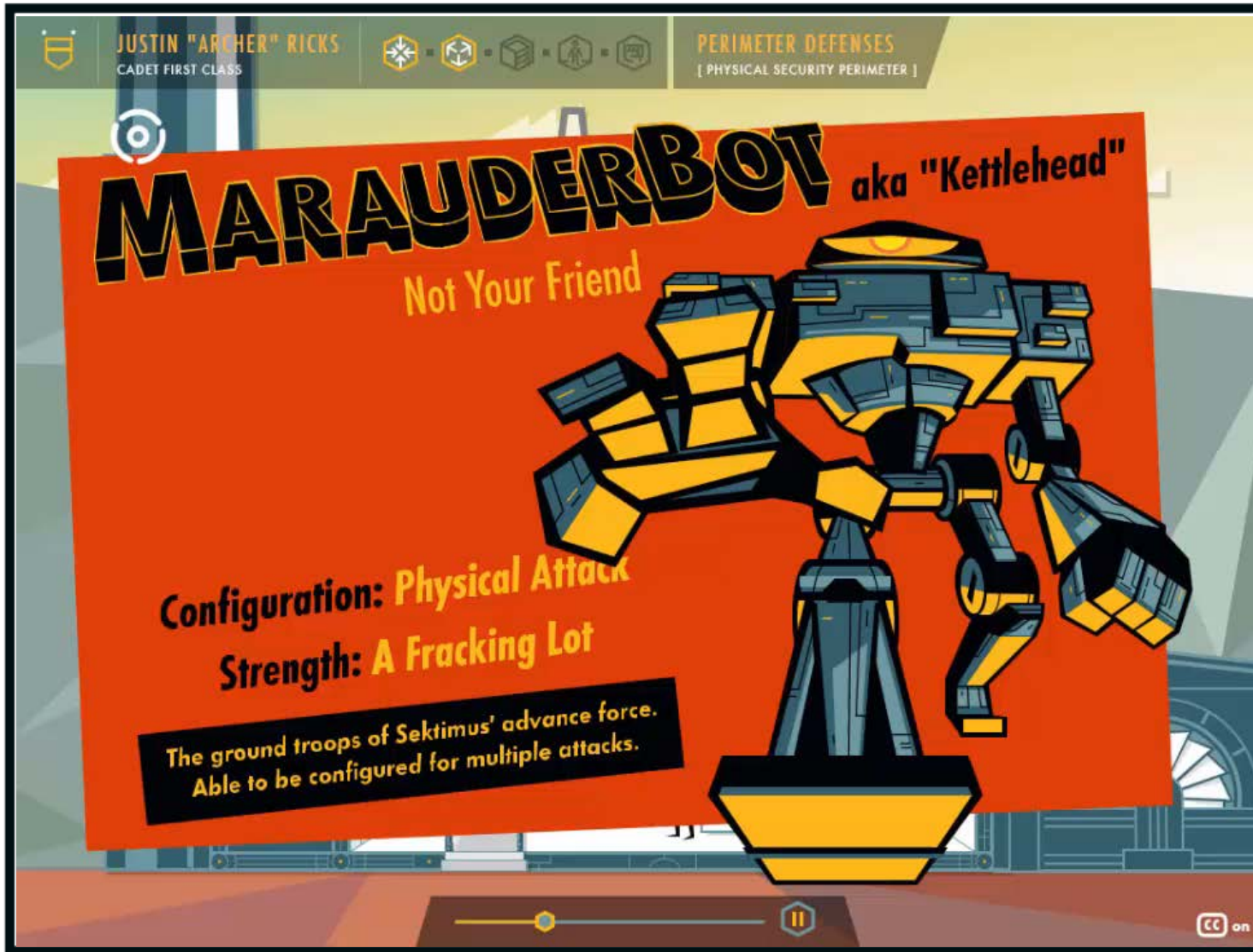
Use hero insights to connect and give credibility



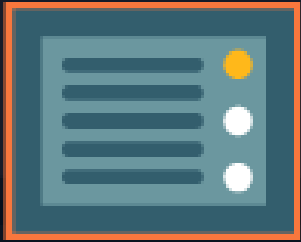
Create
emotional
attachment
with humans,
not facts or
objects



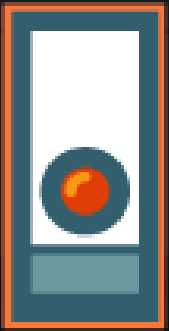
**Introduce your
conflict to the
hero and make
it personal**



Show the
“why” using
your story and
your villains



#1 – Employee Badge Scanner

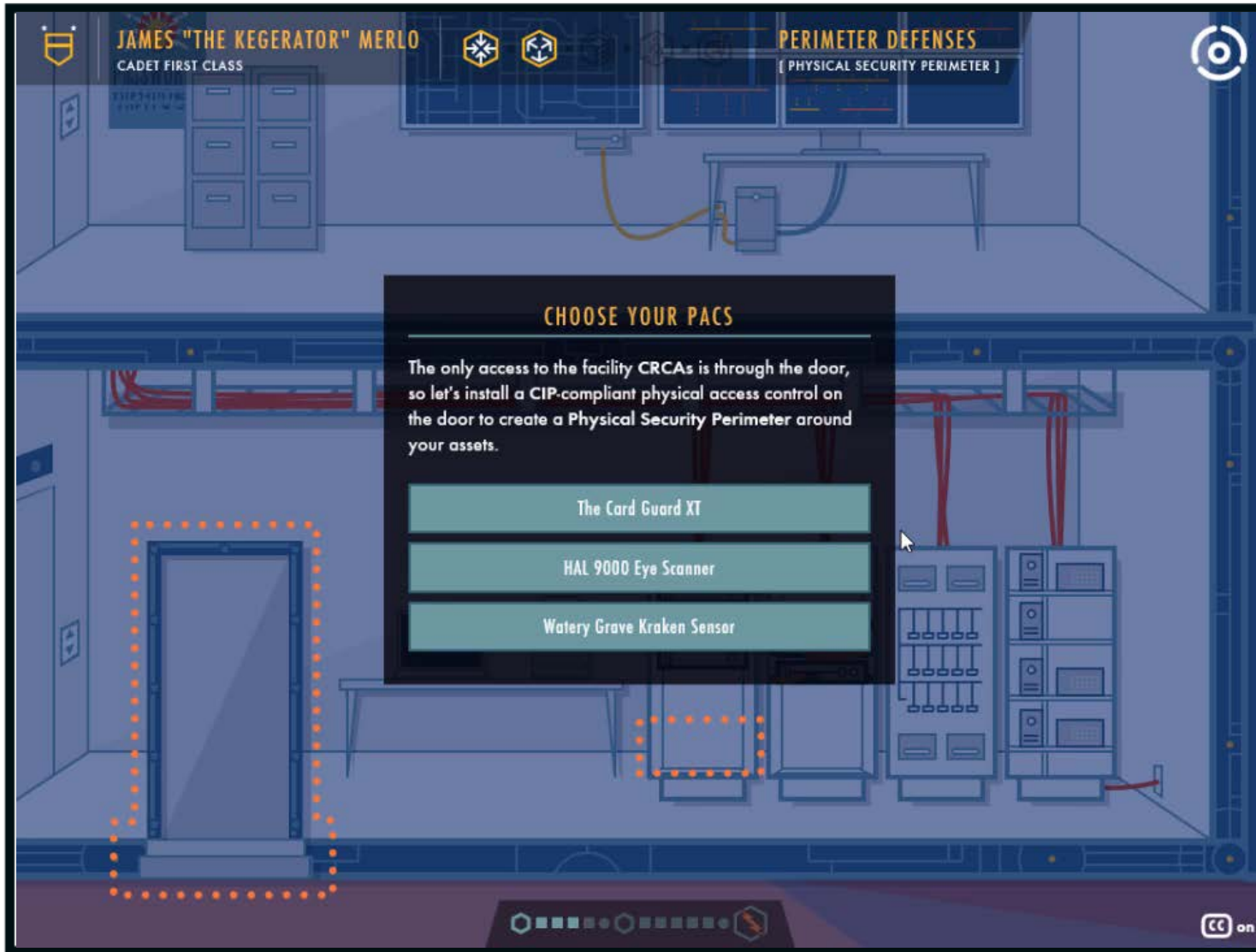


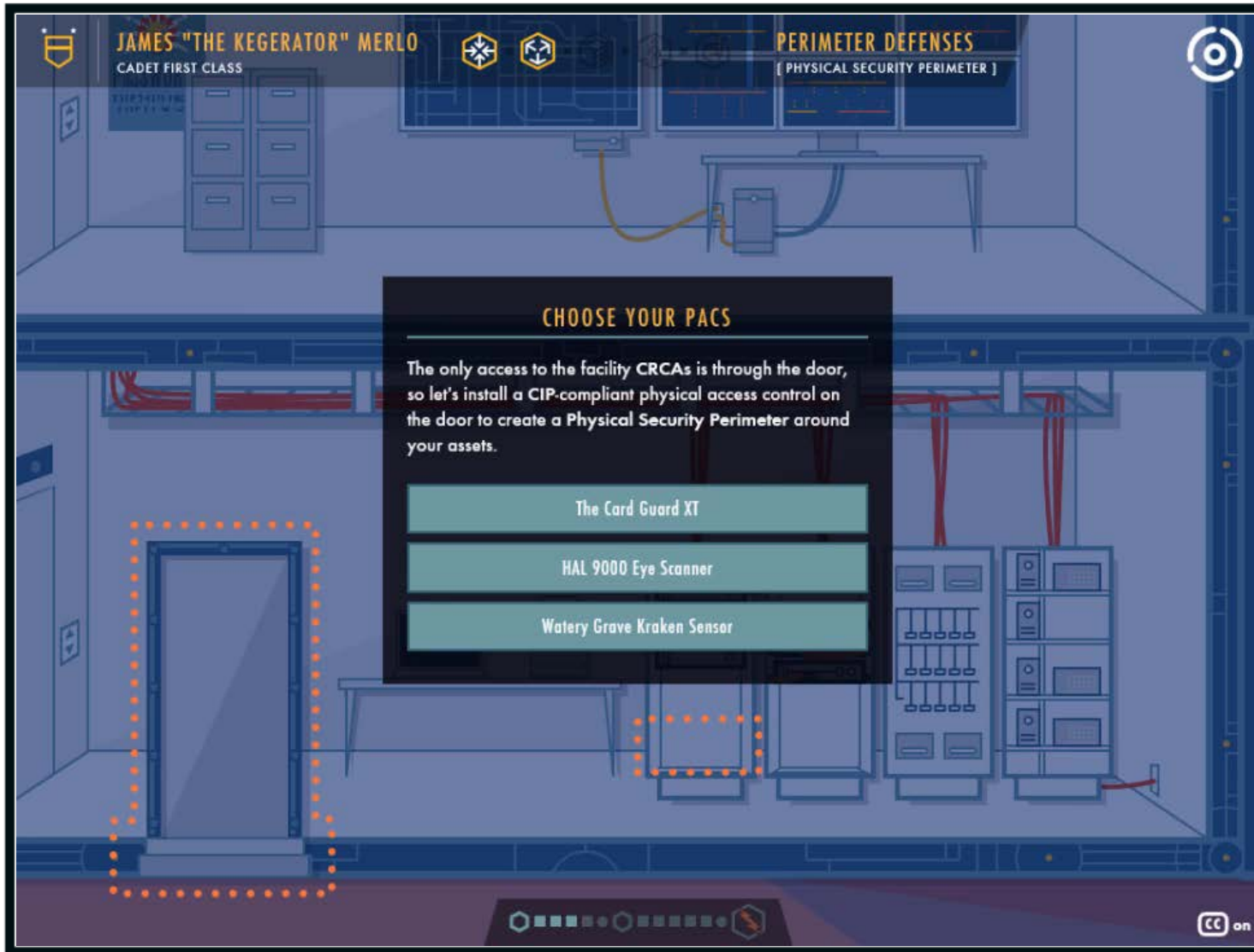
#2 – HAL 9000 Eye Scanner

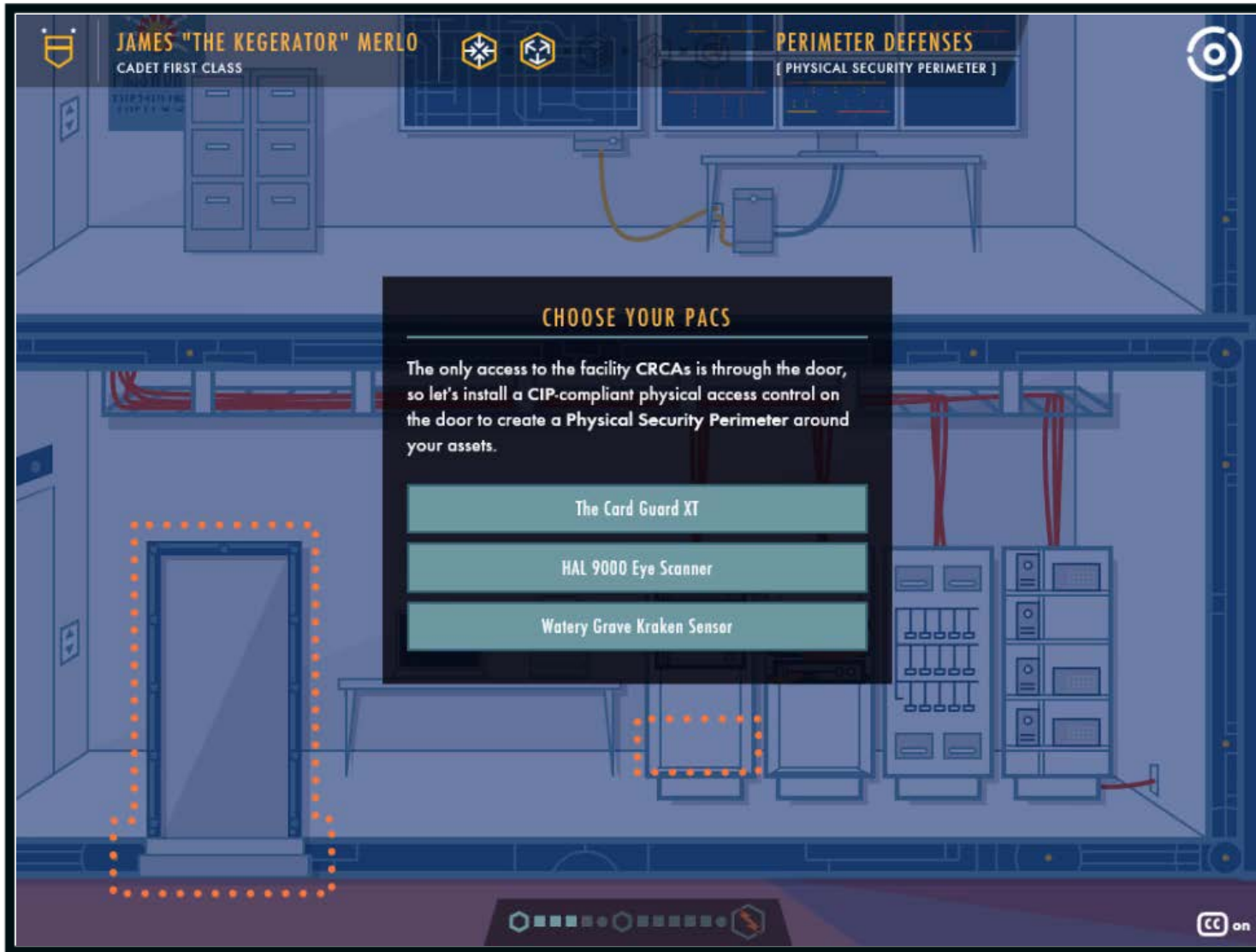


#3 – K.R.A.K.E.N. Body Shape Sensor

**Give people
choices that
matter**

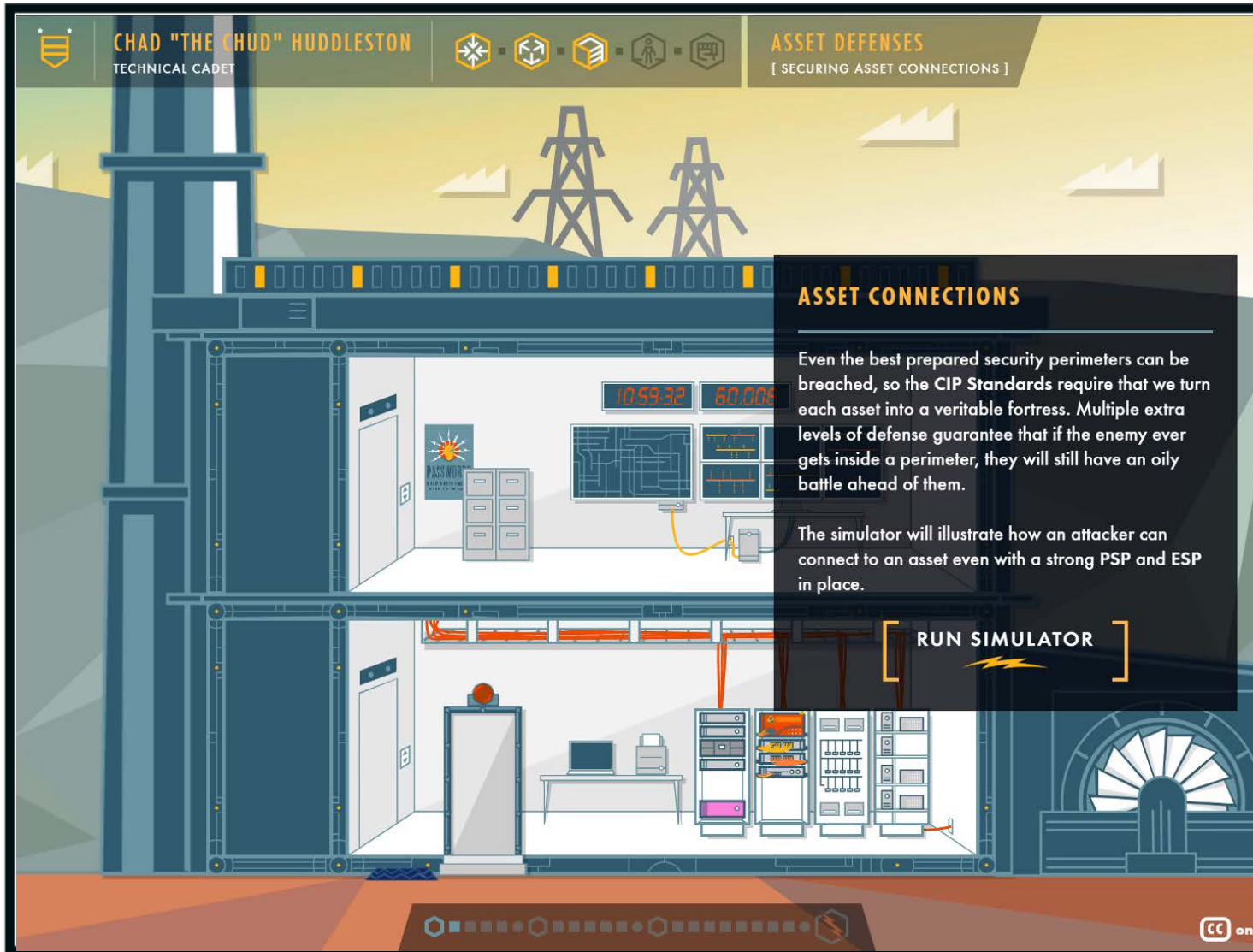








The hero's choice should teach the principle and resolve the conflict



Use the micro
conflict
pattern to
provide
continual
engagement



Question Total Score

Question 1:

What are MondoPower's High Impact Facilities? (pick 2)

20+ Large Substations

Tesseract Power Plant

HQ Building

Control Center

Backup Control Center



Testing is to
collect insight,
not to force
understanding
or retention



TAKEHOME INNOVATION SUMMARY

Discover the Story - Treat your people as heroes, yourselves as the sages, and create adversaries.

Map the Learning Journey Heroes, sages, villains, and learning experiences. Grab pencil & paper and map it out.

Design Each Experience from the Her@ut – Use the tools and technology at hand to make your people feel like heroes through every experience.





Thank you



Northeast Power Coordinating Council, Inc.

Fall 2018 NPCC Compliance and Standards Workshop

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Oversight of Effective Risk- based Compliance Monitoring

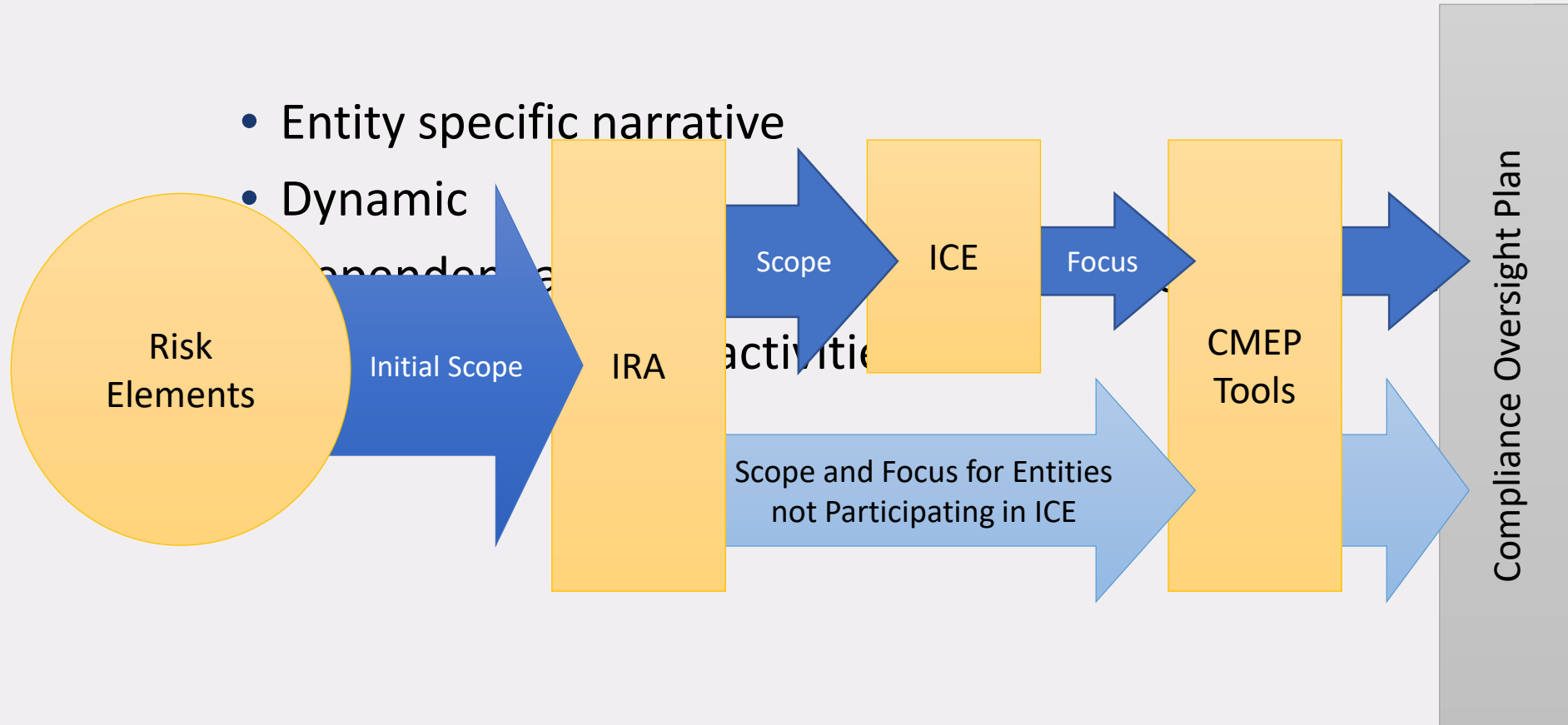
2018 Status Update

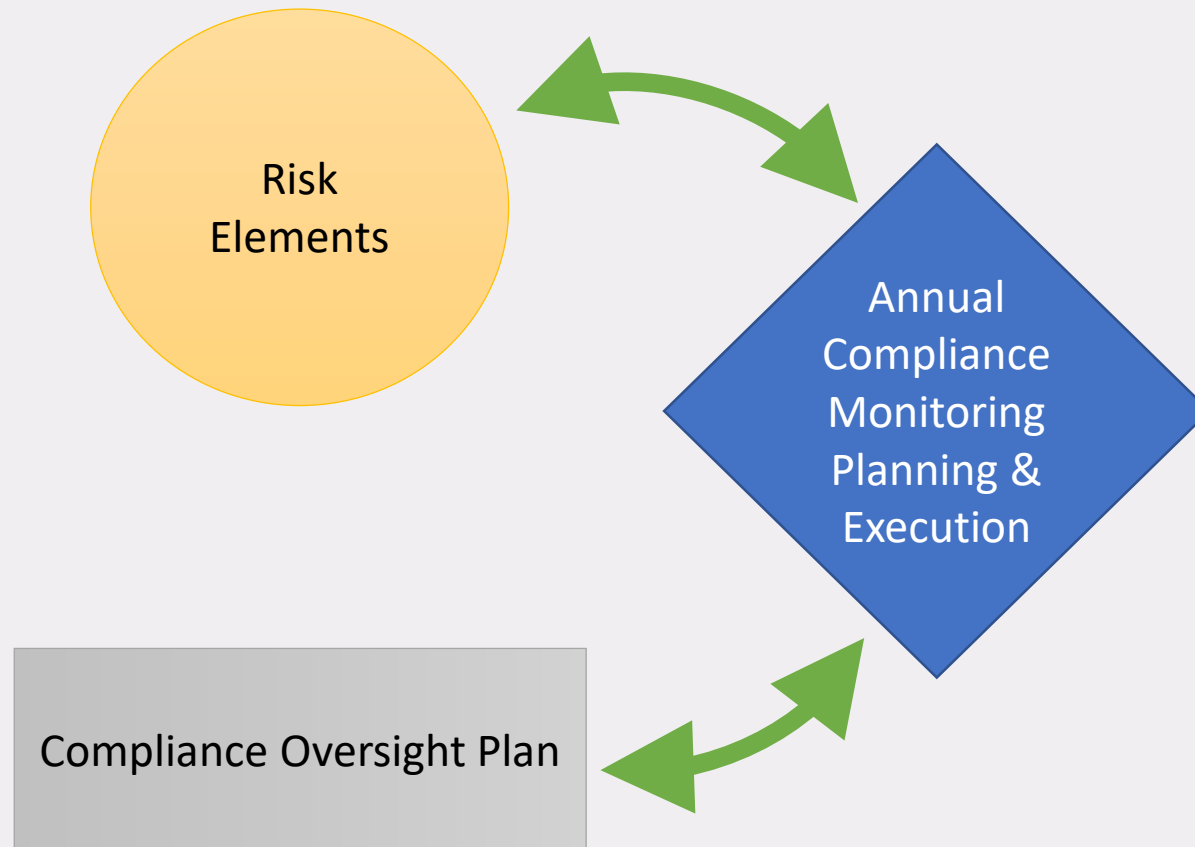
RELIABILITY | ACCOUNTABILITY



Primary Oversight Objectives

- Support reliability and security
- Identify and monitor reliability and security risks
- Alignment of compliance monitoring activities across ERO Enterprise
- Adherence to governing documents





**2014-
2015**

Design
Guidance and
Processes



**2016-
2017**

Implement
Program
Improvements



**2018-
2019**

Assess
Alignment and
Effectiveness





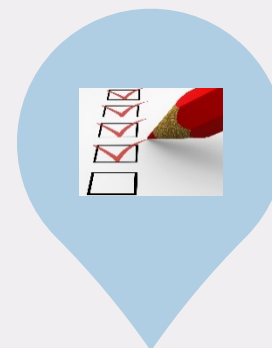
2014/2015

Foundation



2016/2017

Calibration



2018/2019

Maturation



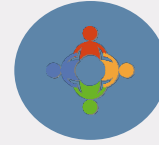
**NERC Compliance
Assurance**



**NERC and RE Management
Groups**



**ERO Enterprise
Reporting**



**NERC and RE Task
Forces**



**FERC
Coordination**



Other Inputs



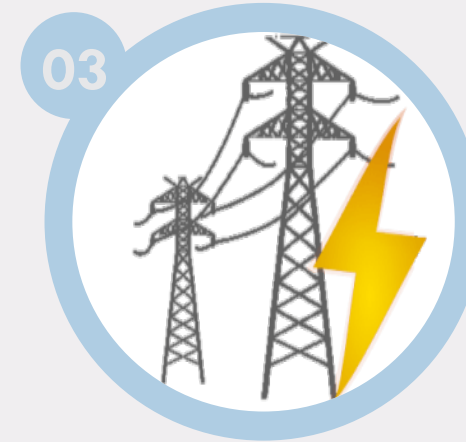
RE Oversight

NERC oversight of RE
implementation of risk-
based compliance
monitoring



Training & Outreach

ERO Enterprise
training and industry
outreach



Reliability & Security Assurance

Alignment around
Reliability Standards,
focus on key reliability
and security risks to BPS



**NERC
Website**



**Compliance
Assurance Email**



Analysis of continent wide 2015-16-17-18q3 impact comparison using EAP Categories vs eSR categories

November 7, 2018

Agenda

- Correlation between eSR categories & Events Analysis Program (EAP) Categories
 - Background
 - Review Summary
 - Conclusions

All Events

	Category Tier							
Year	0	1	2	3	4	5	tbd	
2010	114	13	5	2	0	0	0	134
2011	839	81	42	4	2	0	0	968
2012	436	78	33	2	1	1	0	551
2013	332	102	32	6	0	0	0	472
2014	331	145	23	1	0	1	0	501
2015	238	131	21	1	0	0	0	391
2016	267	168	6	2	0	0	0	443
2017	312	174	4	0	1	2	0	493
2018	224	122	4	0	0	0	18	368
	3093	1014	170	18	4	4	18	4321

Filter 2015-6-7-8q3

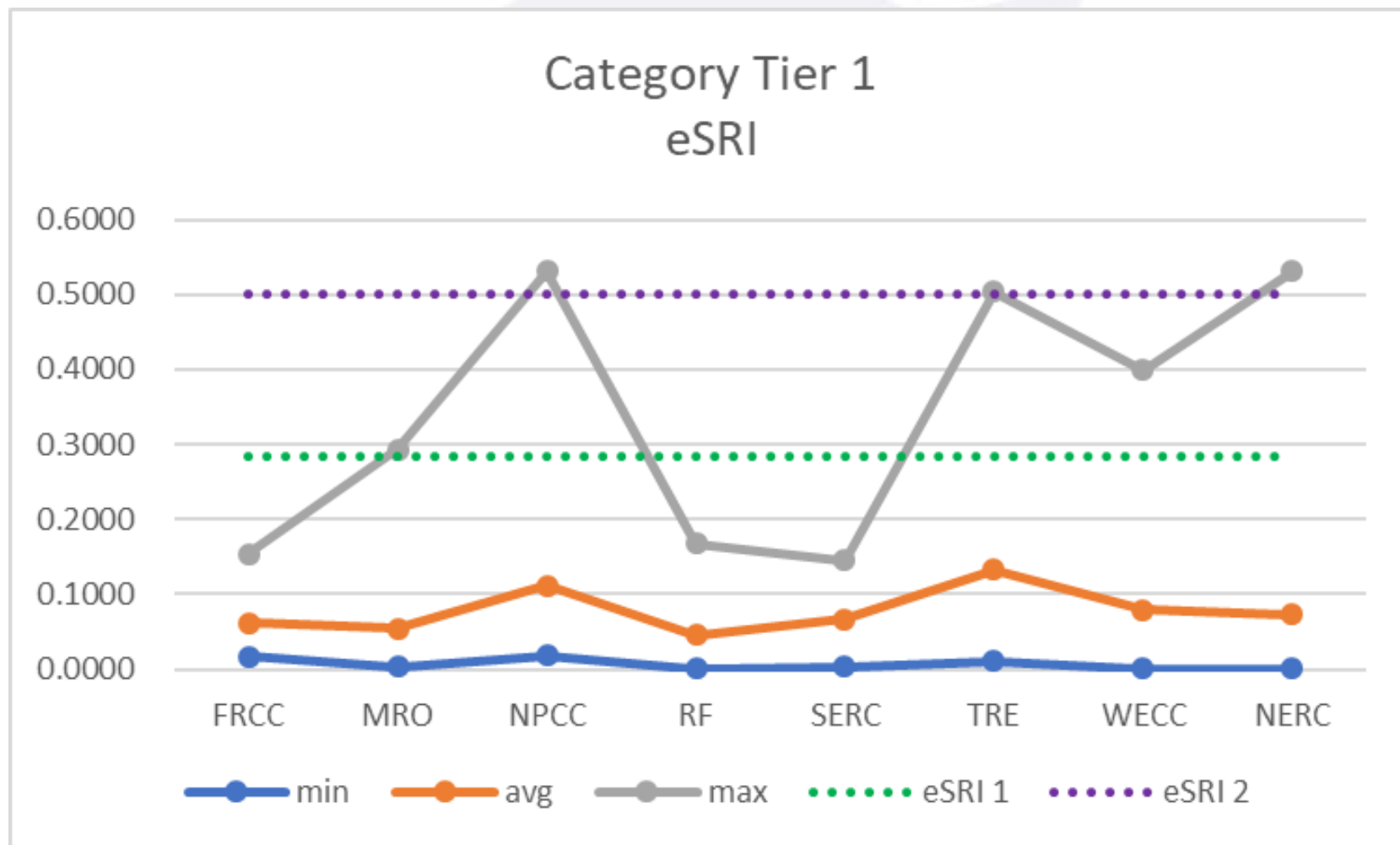
	Category Tier							
Year	0	1	2	3	4	5	tbd	
2015	238	131	21	1	0	0	0	391
2016	267	168	6	2	0	0	0	443
2017	312	174	4	0	1	2	0	493
2018	219	122	4	0	0	0	13	358
	1036	595	35	3	1	2	13	1685

Reviewable Events

Year	Category Tier					
	0	1	2	3	5	
2015	5	49	5	1	0	60
2016	3	73	6	2	0	84
2017	2	58	2	0	2	64
2018	2	46	1	0	0	49
	12	226	14	3	2	257

eSRIcategory Ranges

eSRI Category	min(eSRI)	max(eSRI)
1	0.00000	0.28489
2	0.28490	0.49999
3	0.50000	3.79999
4	3.80000	9.00000
5	9.00001	999.99999



Variations

The following slides separate variations from the expected eSRI values

Outliers and in some cases a different system design comprise the variations

Variations

continued

The following legends explain slides 11 - 13

- MRO* means MRO without its outlier event
- MRO^ is the MRO outlier event
- NPCC* is NPCC without variations
- NPCC^ are those events where the system design, results in higher eSRI values
- NPCC~ is an outlier event
- WECC* means WECC without outliers
- WECC^ is three WECC outlier events

Variations

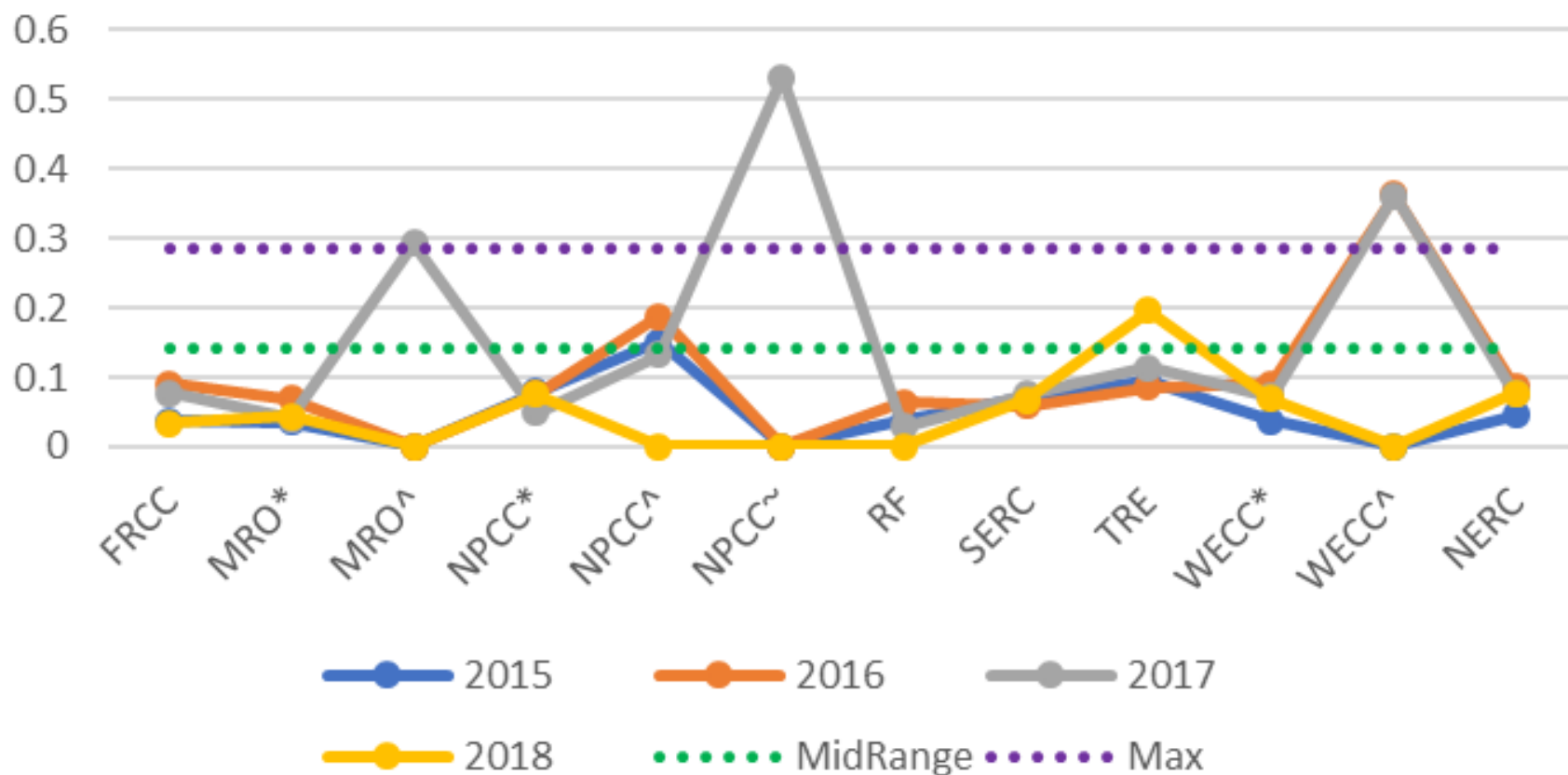
continued

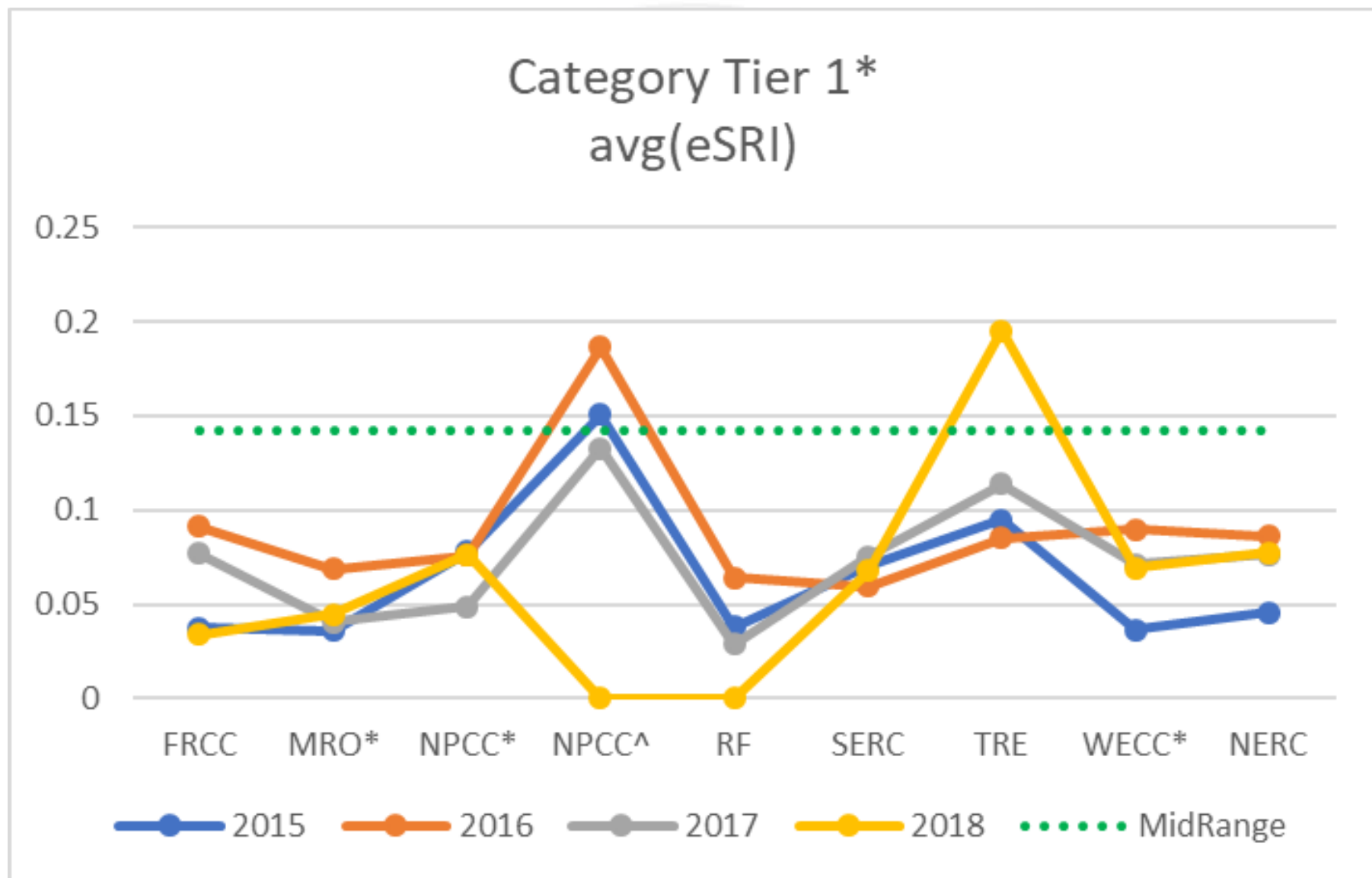
The following Slides 11 – 13 show an analysis of EA Category 1 events. (Since categories 2 through 5 samples are statistically insufficient)

Outliers are where the Category 1 event's eSRI is greater than the eSRIcategory 1 range

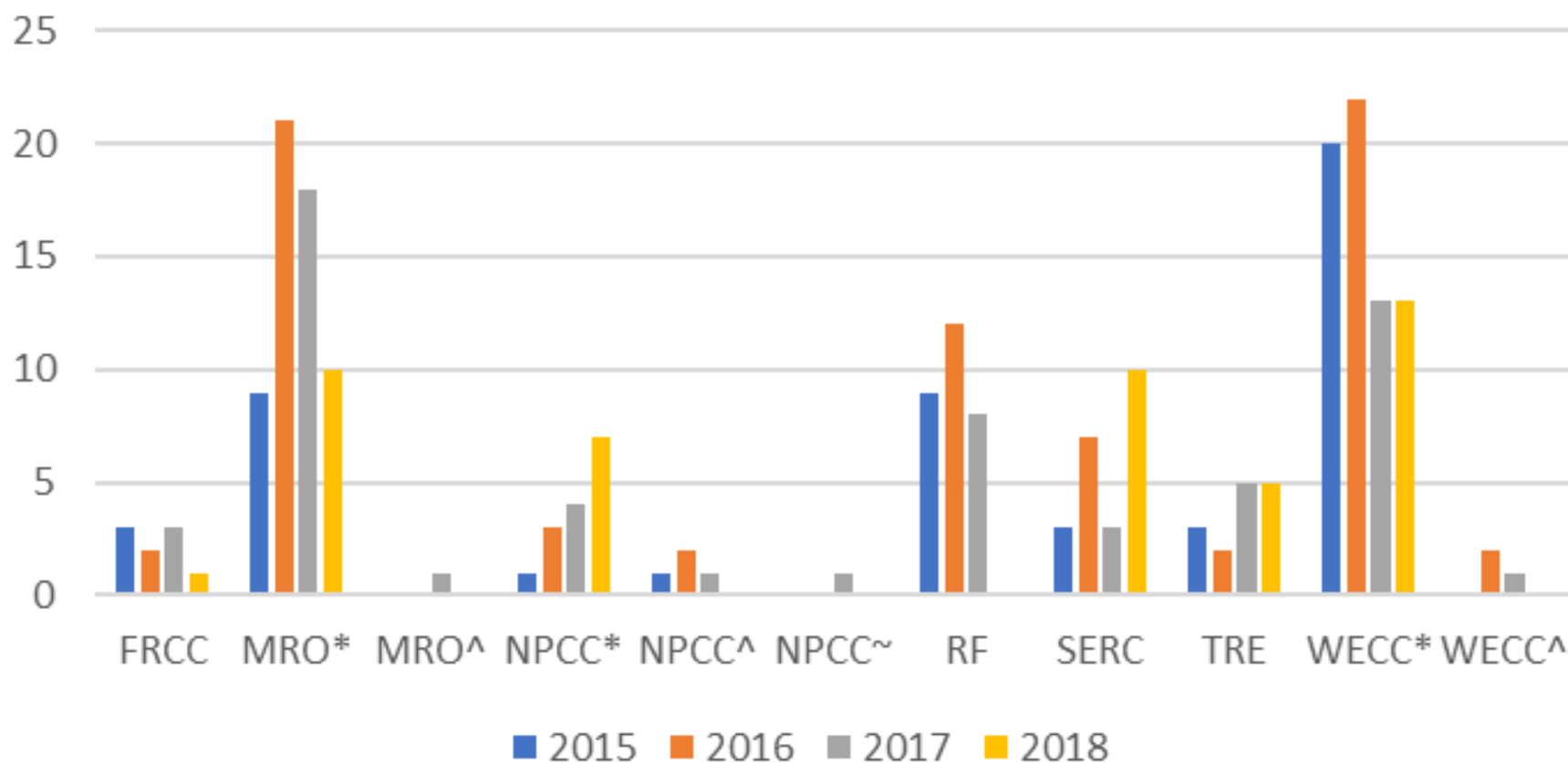
Since including outliers skews the scale of slide 11, slide 12 is the same data with the outliers removed

Category Tier 1* avg(eSRI)

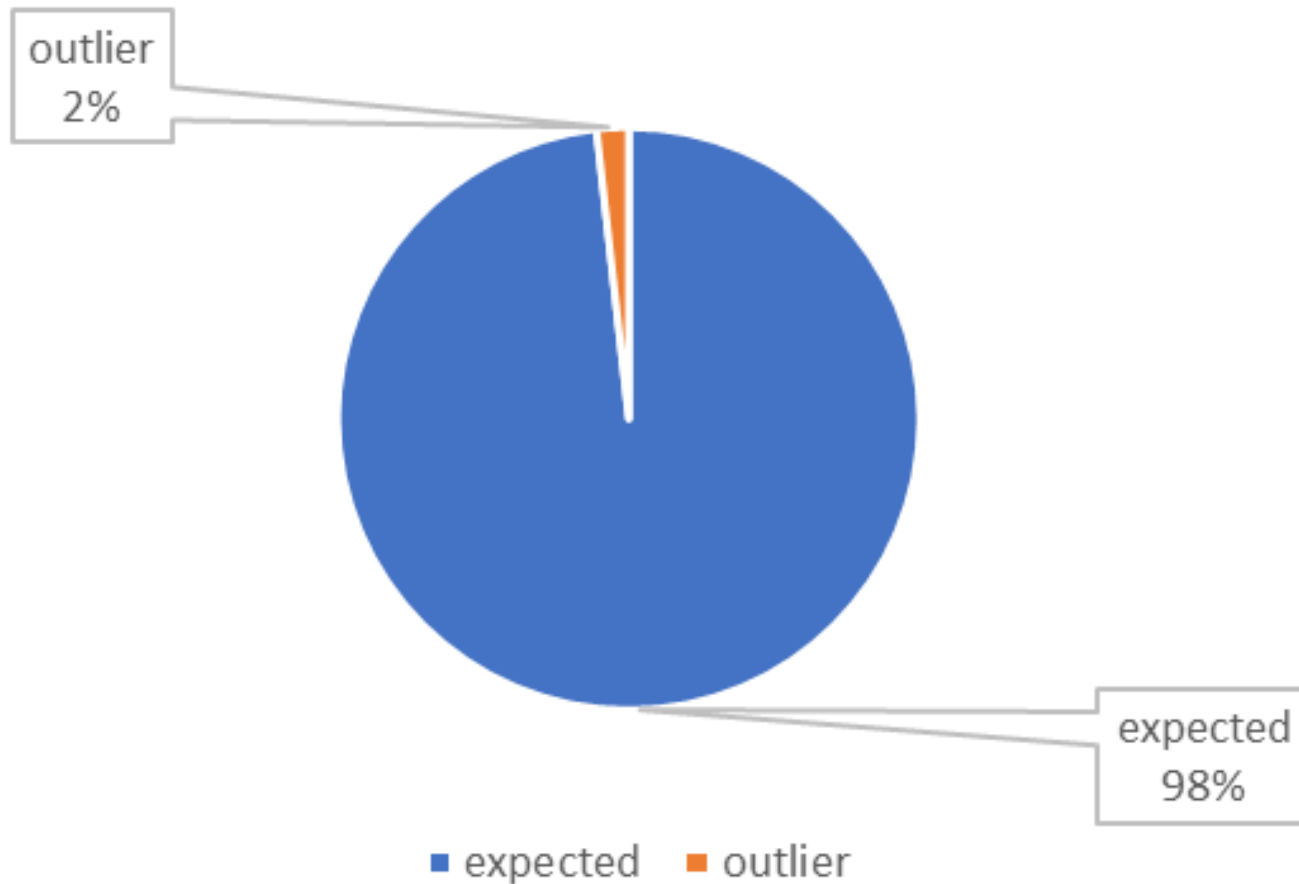




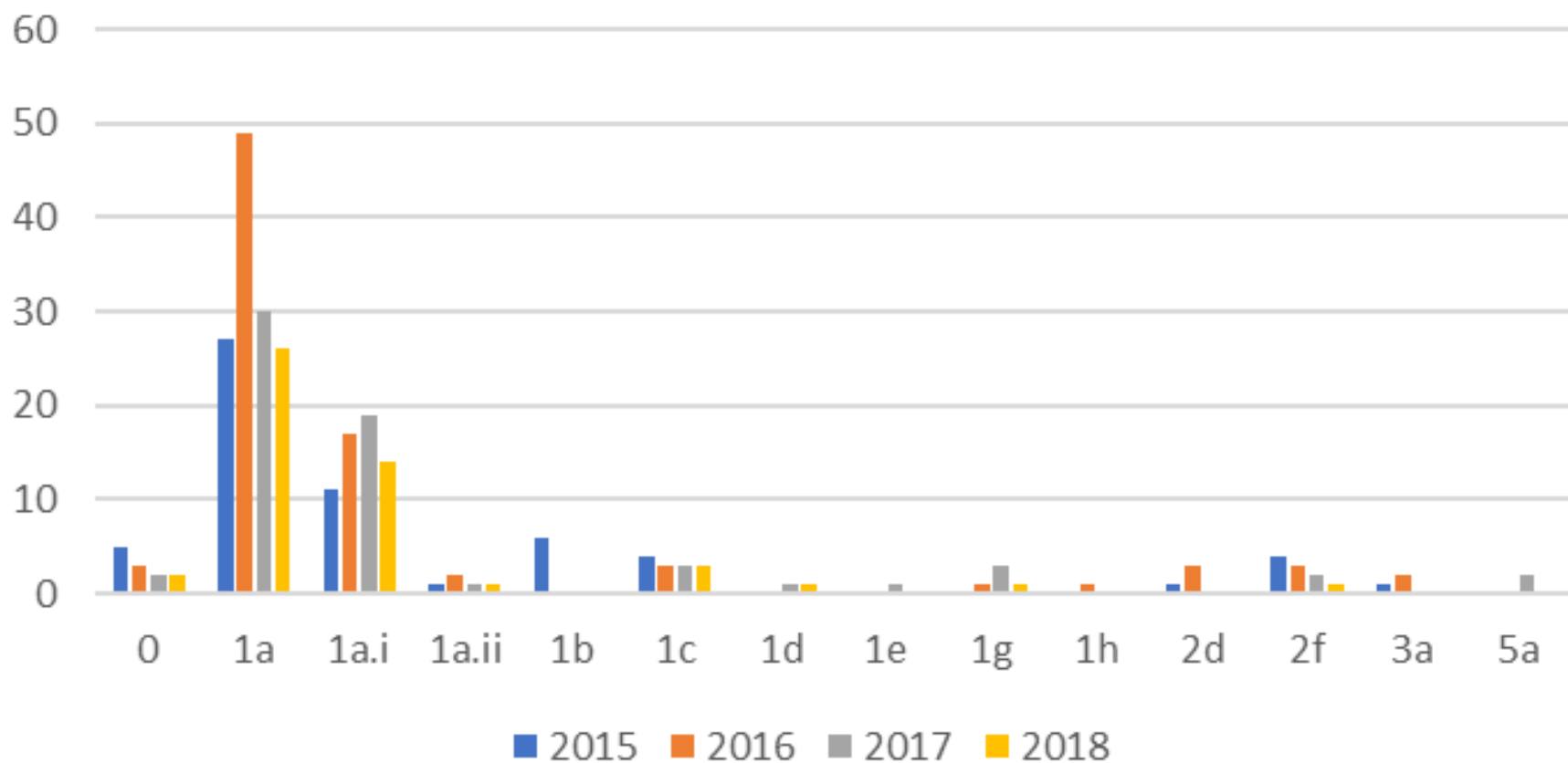
Category Tier 1* # events



Category Tier 1 # events



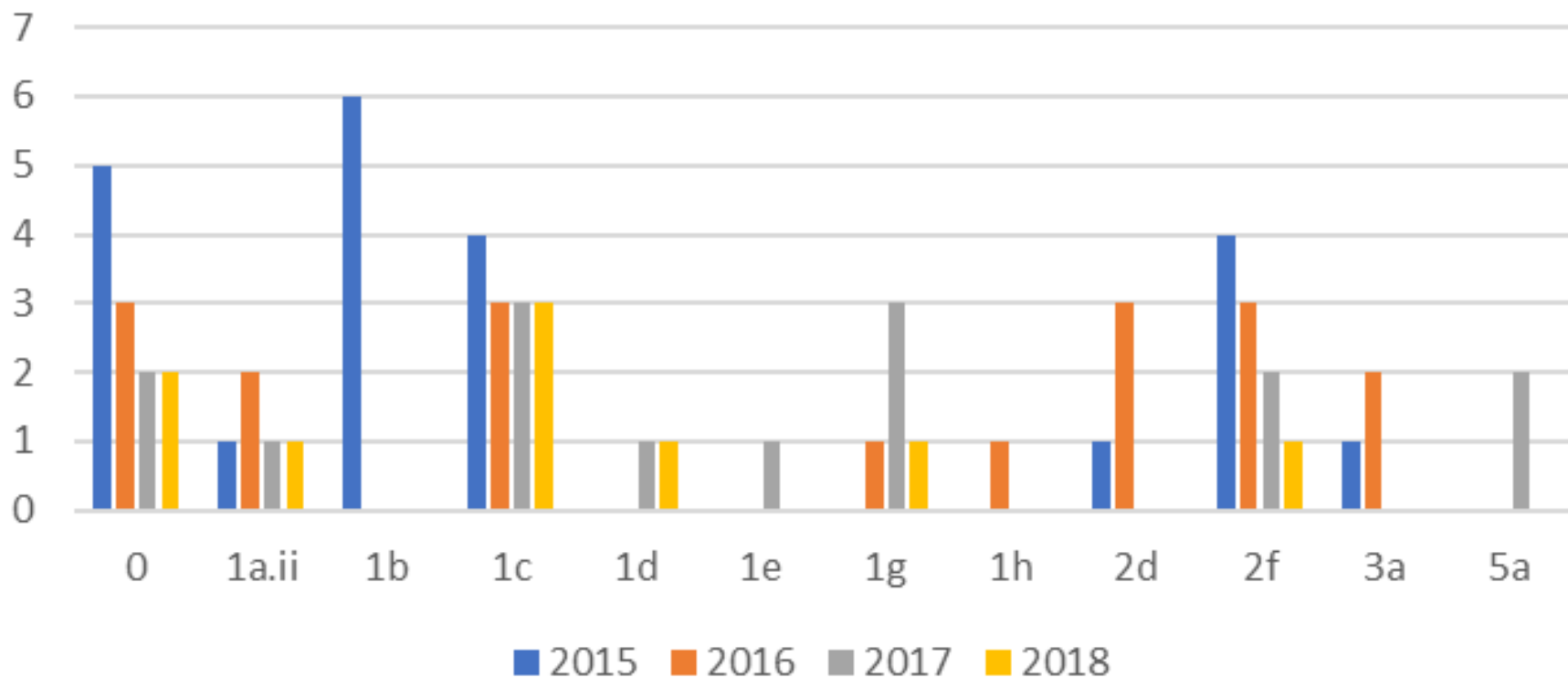
events by Category



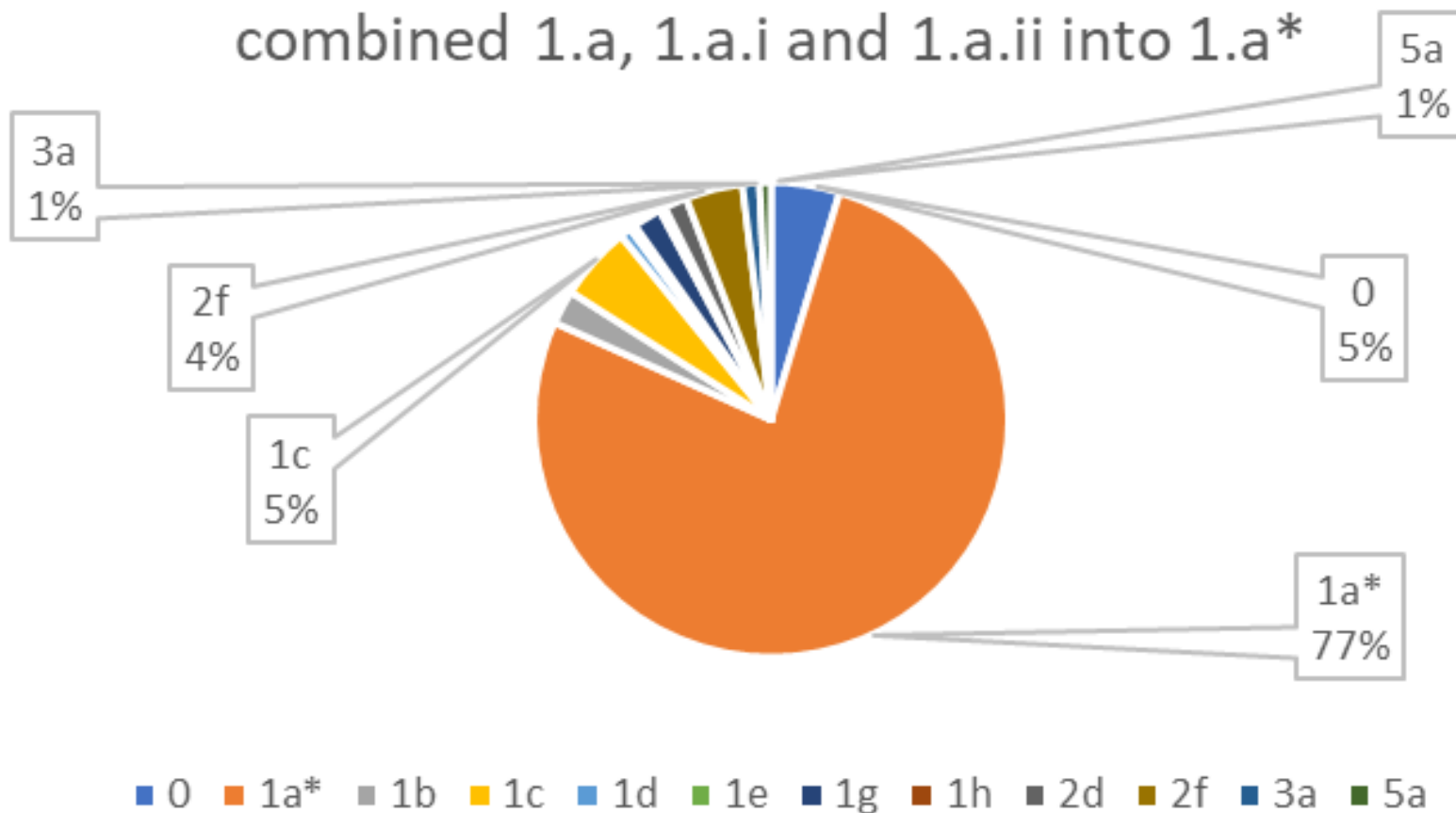
Category 1.a definitions

- a. an unexpected outage that is contrary to design of three or more BES Facilities caused by a common disturbance:
 - i. The sustained outage of a combination of three or more BES Facilities
 - ii. The outage of an entire generation station of three or more generators (aggregate generation of 500 MW to 1,999 MW); each combined-cycle unit is counted as one generator

events by Category without 1.a and 1.a.i



events by Category combined 1.a, 1.a.i and 1.a.ii into 1.a*



Service Offered

The What-If methodology is a fast way to quickly determine an event's worst case BES impact.

If you have an event whose eSRI value is above the midpoint of the eSRI category range and you would like to see if a worst case scenario (i.e. on a high load day, or dispatch or possible misoperation condition) could cause that event to have jumped categories.

Please contact Ralph Rufrano at rrufrano@npcc.org for more information.

Questions

