E-ISAC
ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

NERC E-ISAC Physical Security Briefing

Carl Herron, Senior Manager Physical Security Analyst
California Public Utility Commission
May 31, 2017 San Francisco California

RESILIENCY | RELIABILITY | SECURITY




CIP-014-02 Site Visits

- Voluntary and informal (NERC and Regions)
- Nineteen entities in six different Regions visited, as of August 2016
- Discuss plans and challenges for implementation of CIP-014-02
- Provides opportunity for collaborative discussion regarding the requirements
- **Focus on security plan effectiveness** A1

A1 Is the bold lettering intentional? If so, it's acceptable.
Author, 3/14/2017

CIP-014-02 Site Visits

- Common Theme:
  - Timelines for implementing security and resiliency measures
  - Third-party reviewer – Can third-party participate in R4 and R5
  - Scope of security plans
  - Defining characteristics of the assets identified as required by R1
  - What data and security plan information will be requested
  - Insider threat concerns
  - Confidentiality of CIP-014 sites and information
  - Multiple owners of critical sub stations
  - Tiered approach

ERO to Monitor Implementation

- Number of assets critical under the standard
  - Per Region
  - Q4 2015 – Q1 2016
- Defining characteristics of the assets identified as critical
  - Per Region
  - Q4 2015 – Q1 2016
- Scope of security plans
  - By Q4 2016
  - Information obtained guided self-certs, off-site audits, audits
  - Consider compliance monitoring schedule

R4 Threat and Vulnerabilities Assessment

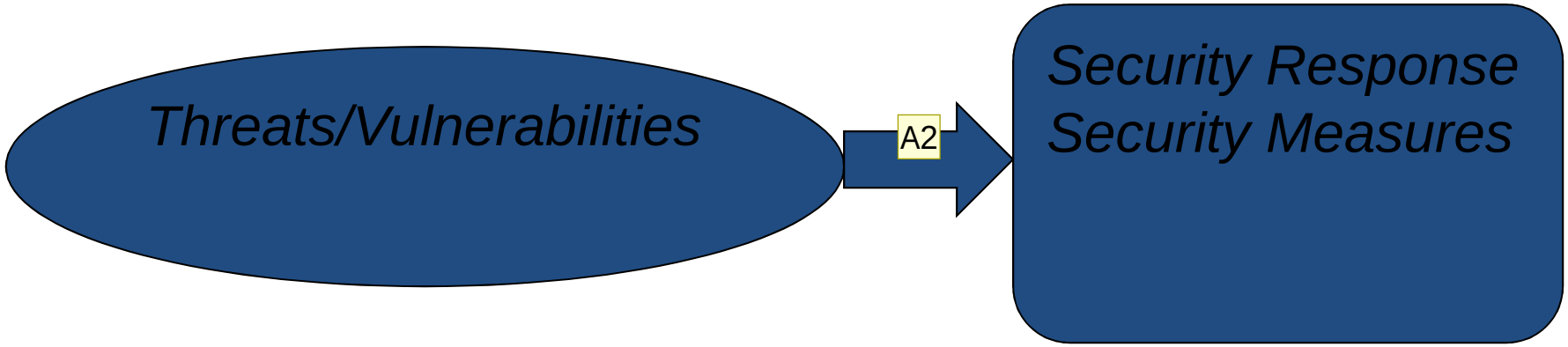
- Threat Assessment – Tools and Methods
  - Industry history
  - Company/Substation history and Incidents
  - Fusion Centers(State, Federal and local)
  - Design Basis Threat (DBT) – E-ISAC
  - OE-417 Electric Disturbance Events Report

R4 Threat and Vulnerabilities Assessment

- Vulnerabilities Assessment – Considerations
  - Security gaps physical/human
  - Substation design
  - Policy and procedures
  - Geographic challenges

R5 Security Plan

- Security Plans should address identified threats and vulnerabilities
- Two-part plan - security response and security measures



- Detection and response

A2 What is this arrow pointing to?

Author, 3/14/2017

Physical Security Characteristics

- Common physical security characteristics observed:
  - Substations located near or adjacent to other sectors (i.e., natural gas pipelines)
  - Substations located in high crime areas
  - Substations located in remote rural areas with limited law enforcement support
  - Geographical challenges in implementing physical security measures
  - Support of other critical infrastructure or national assets
  - Proximity of the facility to unique threats
  - Proximity of roadways and highways for easy vehicular access and egress
  - Multiple transmission lines entering into a substation
  - Substation located close to other substations not owned by critical substation owner

Security Countermeasures

- Some of the security countermeasures being implemented:
  - Intrusion detection systems
  - Video surveillance and analytics
  - Thermal cameras
  - Anti-climb/anti-cut fencing
  - Ballistic resistant fencing
  - Ballistic panels or walls
  - Transformer detection technology
  - Additional lighting
  - Vehicle barriers/bollards/crash gates
  - Use of natural environment
  - Gun shot detection

R4 Threat and Vulnerabilities Assessment

- Criminal Element
- Law Enforcement Response

R4 Threat and Vulnerabilities Assessment

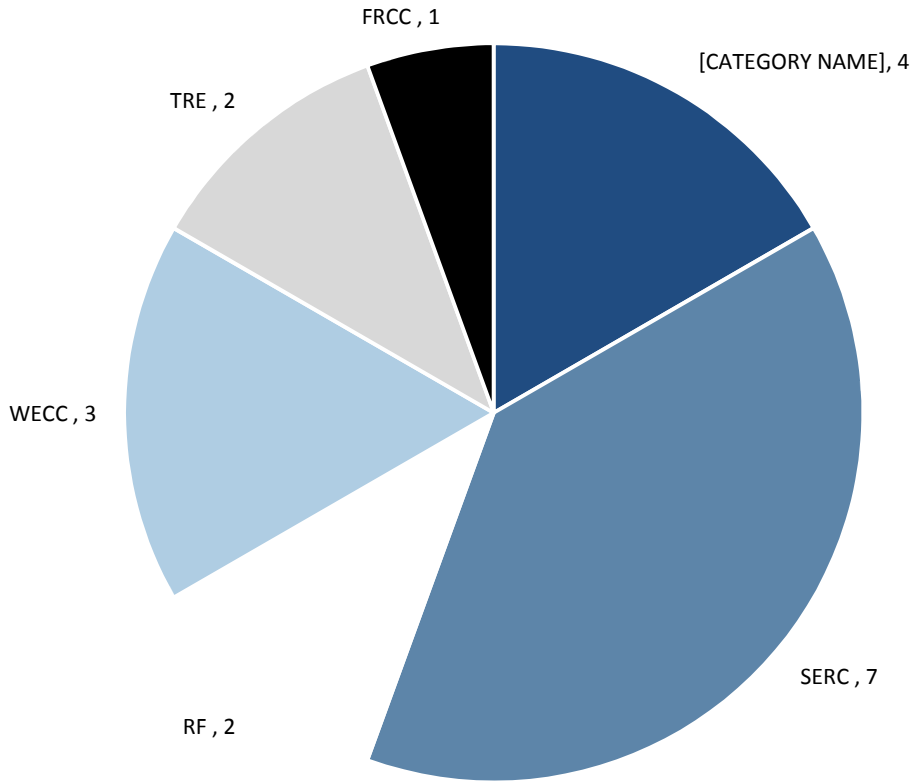
- Geographic Challenges

Quarterly Report to BOT

- Quarterly report to the Board of Trustees on progress and review of industry implantation of CIP-014-2
- Number of assets critical under CIP-014-2
- Defining characteristics of assets identified as critical

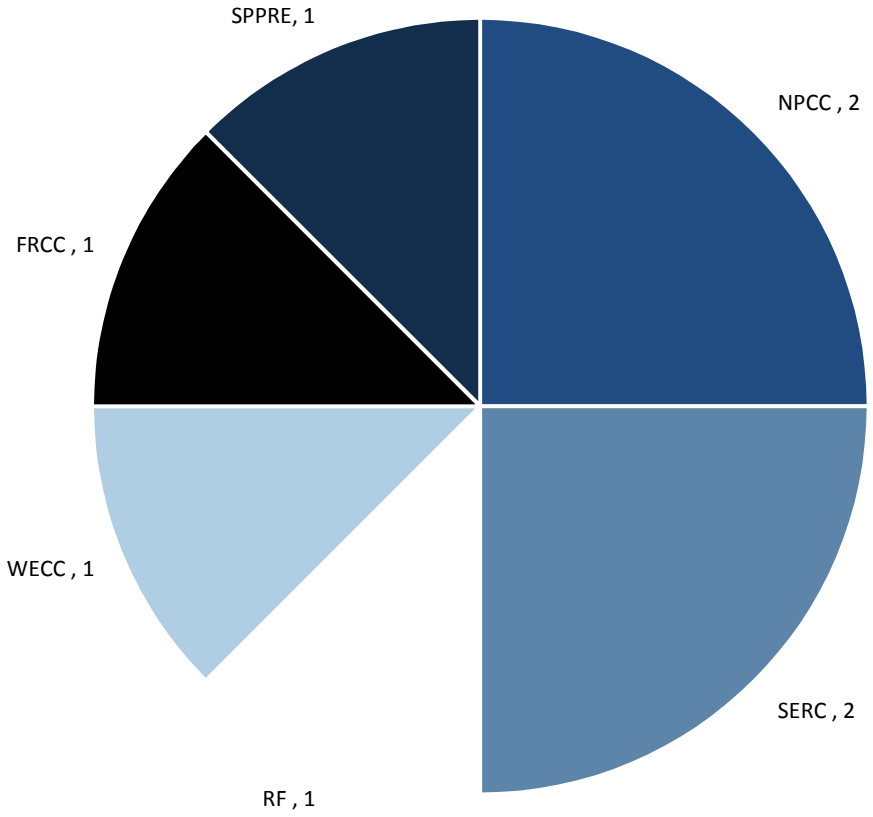
- Scope of security plans (security measures and response)
- Timeline for implementation of security measures
- Industry's progress in implementation of CIP-014-02

CIP-014-02 Visits by Regions



CIP-014-02 Workshop/Outreach

Number of Outreach/Workshops Visited by Regions



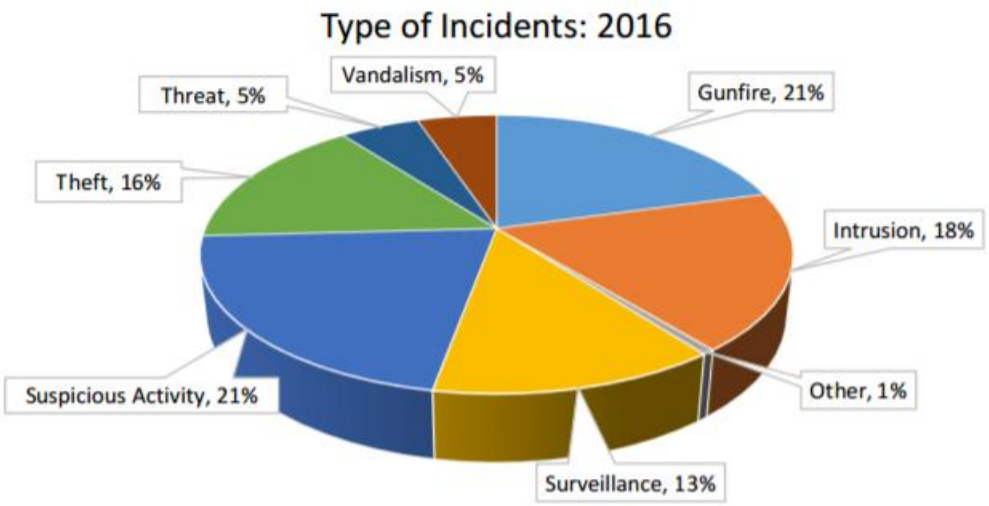
What to Share?

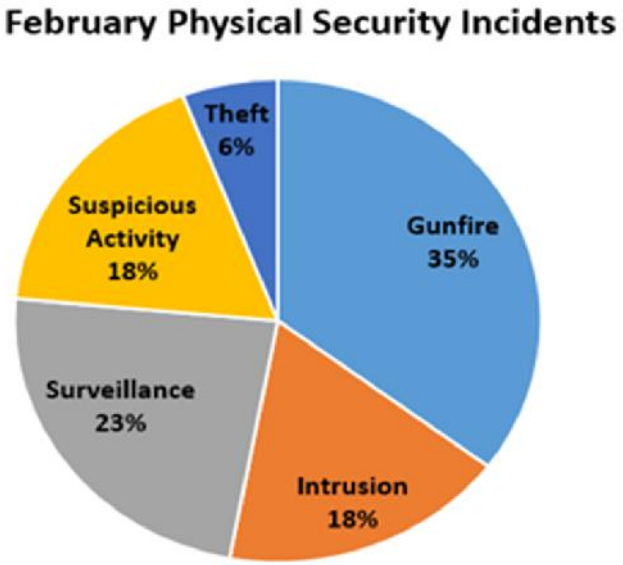
Break-ins/attempted break-ins	Unauthorized personnel **attempting to enter or actually entering** a restricted area, secured protected site, or nonpublic area; impersonation of authorized personnel (e.g., police/security officers, janitors, or other personnel)
Misrepresentation	Presenting **false information** or misusing insignia, documents, identification, etc., to misrepresent affiliation as a means of concealing possible illegal activity
Theft, loss, or diversion	**Stealing or diverting** something associated with a facility/infrastructure or secured protected site (e.g., badges, uniforms, identification, emergency vehicles, technology, or documents), which are proprietary to the facility/infrastructure or secured protected site
Sabotage, tampering or vandalism	Damaging, manipulating, defacing, or destroying part of a facility/infrastructure or secured protected site
Expressed or implied threat	Communicating a spoken or written threat to commit a crime that will result in death or bodily injury to another person(s), or to damage or compromise a facility/infrastructure or secured protected site.

What to share cont'd?

Aviation activity	Unknown UAS **flying** or **hovering** over power plants, substations, or transmission lines
Eliciting information	Questioning individuals or otherwise **soliciting information at a level beyond mere curiosity** about a public or private event; about the particular facets of a facility or building, and its purpose, operations, security procedures, etc. in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.
Observation, surveillance	Demonstrating **unusual or prolonged interest in facilities**, buildings, or infrastructure beyond mere casual (e.g., tourists) or professional (e.g., engineers) interest and doing so in a manner that would arouse **suspicion of terrorism or other criminality** in a reasonable person. Examples include observation through binoculars, taking notes, attempting to mark off or measure distances, etc.
Materials acquisition, storage by an employee or employee's associates	Acquisition/storage of **unusual quantities** of materials, such as cell phones, pagers, radio control toy servos, or controllers, fuel, chemicals, toxic materials, timers, or other triggering devices in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person

Trend Analysis





27%: Current 2017 Q1 percentage of physical security incidents involving surveillance

What's on the Portal?

- Daily, Weekly, Monthly, Semi-Annual reports
- Incident specific & topical Physical and Cyber Bulletins
- Industry sourced reports and analysis
- Discussion with other entities
- Situation reports during ongoing events and incidents

Partners

- The E-ISAC works very closely with Government and Cross-sector partners
  - Government
    - Department of Energy (DOE)
    - National Cybersecurity and Communications Integration Center (NCCIC)
    - National Infrastructure Coordinating Center (NICC)
    - Other Federal agencies (i.e., FBI, DOD,)
  - Cross Sector Partners
  - Other ISACs/ISAOs
  - Private partners

PSAT Roadmap

- 2017 Physical Security Analysis Team Roadmap
  - Analytical products/case studies
    - Regional trend analysis capability
    - One each Quarter
      - 1st Quarter: Environmental Protest
  - Training
    - DBT
    - National Improvised Explosives Familiarization
    - Crime Prevention Through Environmental Design
  - Topics/Discussions
    - UAS
    - Insider Threat
  - Regional Outreach Visits
    - SERC and RF

Reporting A4

A3

- Submit voluntary reporting:
  - E-ISAC portal
  - Email: operations@eisac.com
  - Call us: 202-400-3001
- What to share?
  - Detailed information located in Engaging the E-ISAC document
    - Located in the public document library

Slide 22

A3 Please refrain from using photos of slides. The fonts are skewed due to resizing, and the formatting is not NERC Style Guide.
Author, 3/14/2017

A4 There was no slide title. I just made this up based on the slide content. Feel free to change.
Author, 3/14/2017

Questions and Answers