SPP Southwest Power Pool Regional Entity

CIP-014-2 Physical Security What to Expect

March 28, 2017

Kevin Perry
Director, Critical Infrastructure Protection

Jeff Rooker
Lead Compliance Engineer

Purpose

- To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.
- CIP-014-2 covered in 3 previous workshops

How did we get here?

- April 16, 2013 PGE's Metcalf Substation Attack
- 52,000 gallons of oil
- 16 transformers
- $15M in damages


Metcalf Road
101
PG&E METCALF
TRANSMISSION
SUBSTATION
S. Valley Freeway
Monterey Road
500 feet
METCALF
ENERGY
CENTER
Coyote Ranch Road
Malech Road
101
CALIFORNIA
San
Francisco
DETAIL
San
Jose
Pacific Ocean
20 miles
1
2
3
4
5
6
7

Shots in the Dark

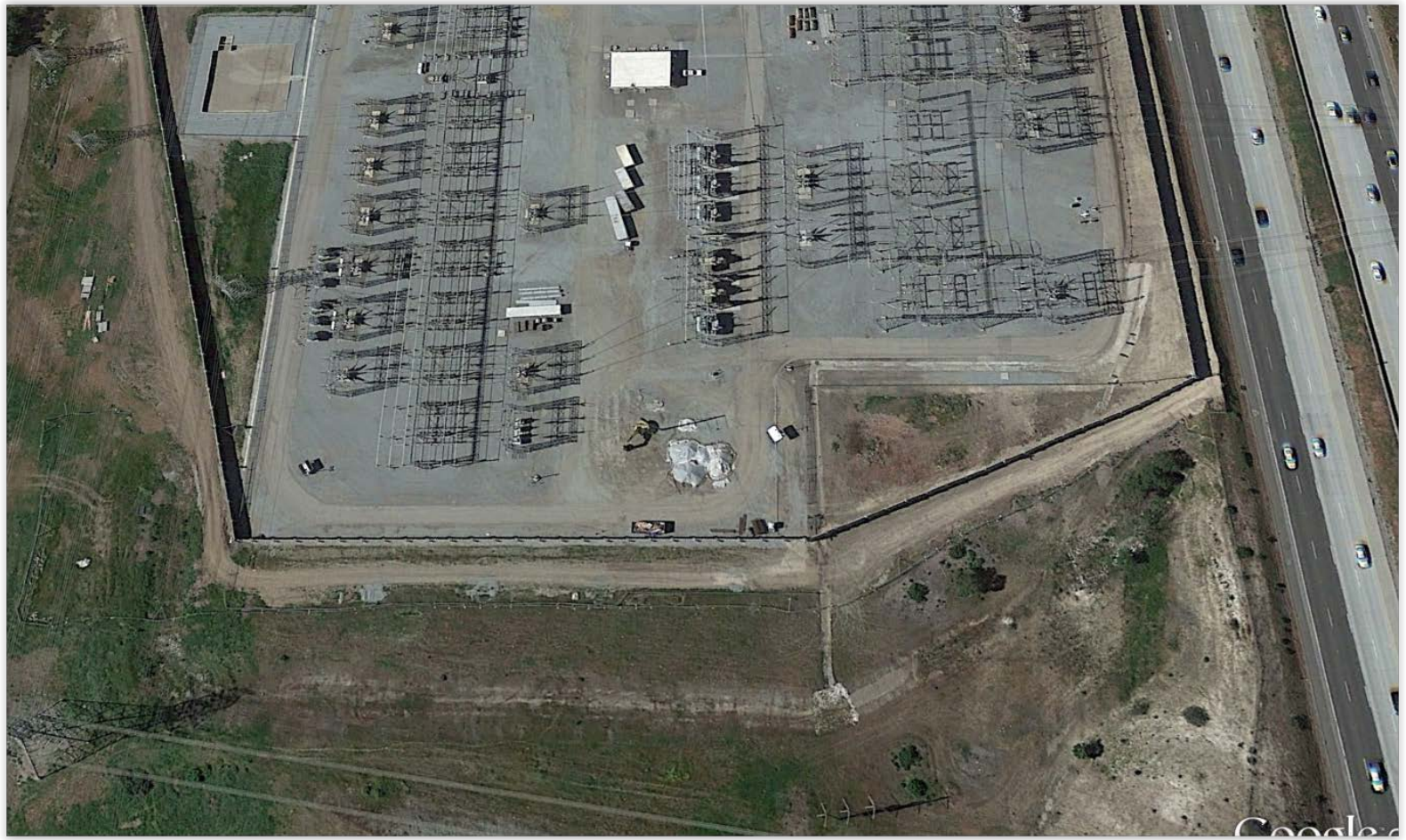
A look at the April 16 attack on PG&E's Metcalf Transmission Substation

Sources: PG&E; Santa Clara County Sheriff's Dept.; California Independent System Operator; California Public Utilities Commission; Google (image)

The Wall Street Journal

What's different from 2013 to…

2015?



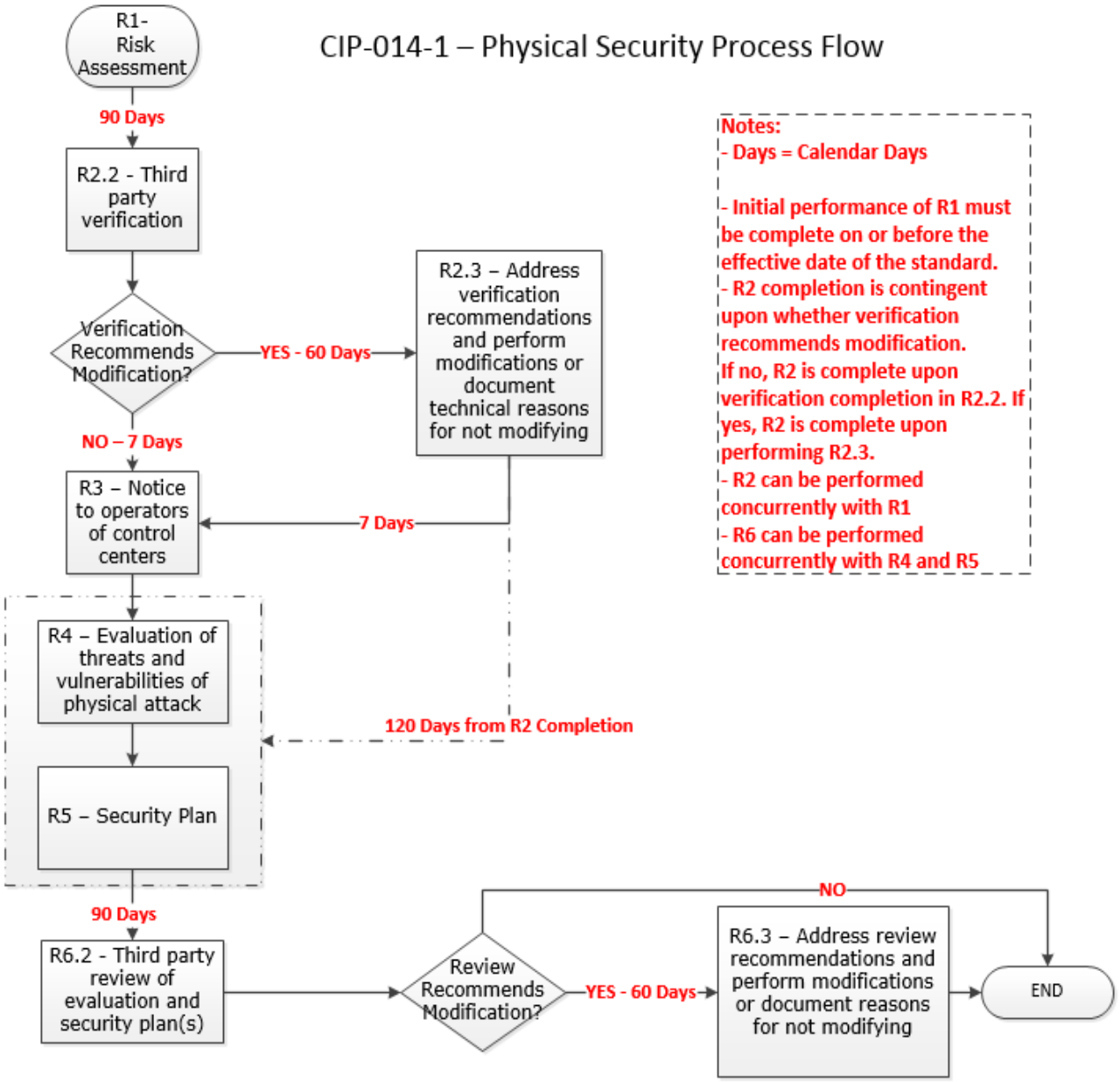
Changes

- Vegetation in close proximity to the substation fence has been removed
- Chain link fence has been replaced with a solid material (e.g. concrete) that restricts exterior line of sight into the substation

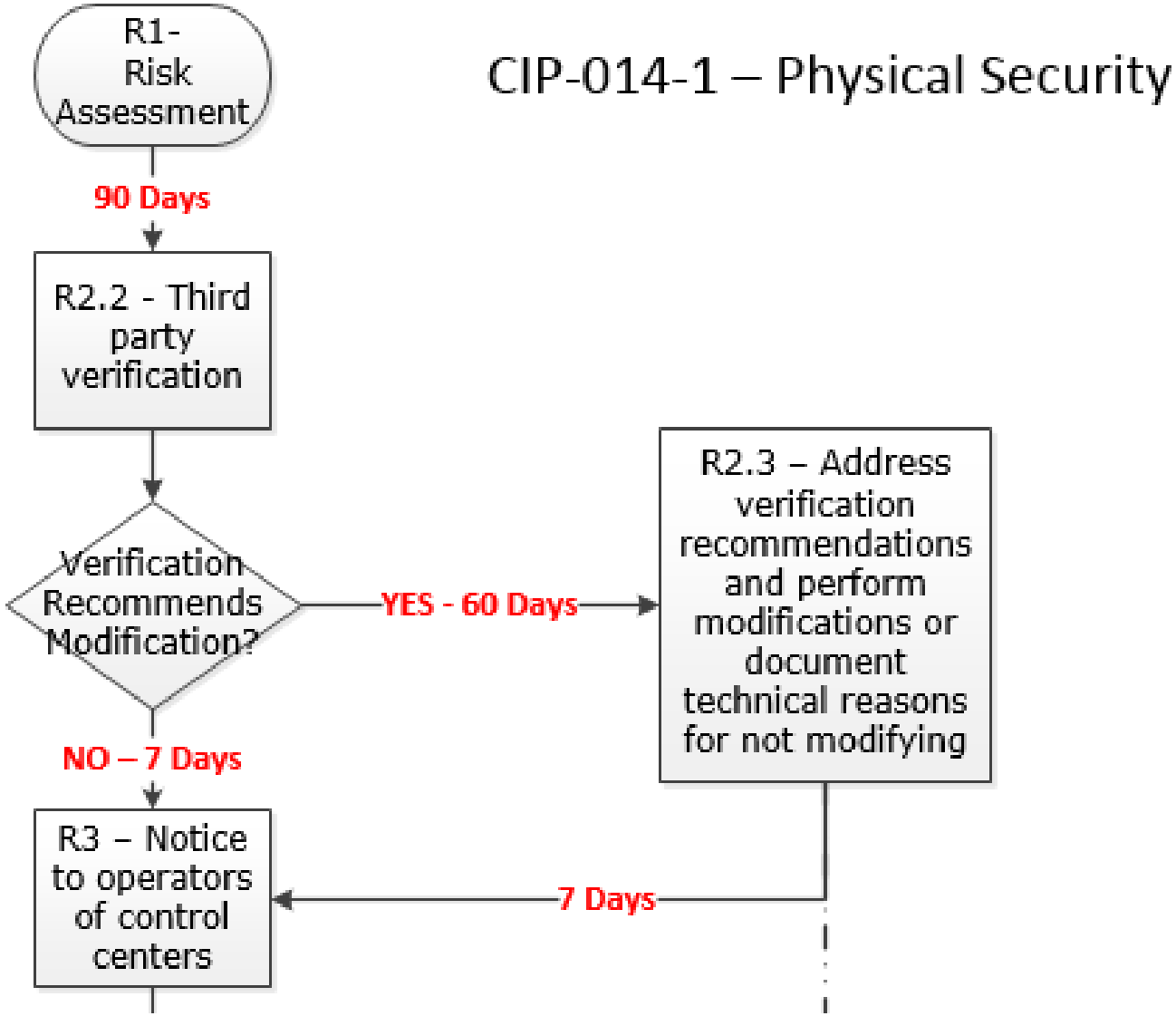
How did we get here?

- April 16, 2013 PGE's Metcalf Substation Attack
- March 7, 2014 FERC directs NERC to submit a physical security reliability standard within 90 days
- May 13, 2014 NERC Board approves CIP-014-1
- CIP-014-2 Effective 10/2/2015

Process Flow



Risk Assessment



Applicable Facilities; CIP-002-5 ¶4.1.1

- Transmission Facilities
  - 500kV or higher
  - 200 kV – 499kV with "aggregate weighted value" > 3000
  - Critical to derivation of IROL identified by RC or PC
  - NPIR
  - Include facilities planned within the next 24 months
  - Exclude generation interconnection facilities
- Primary control center for applicable transmission

CIP-002-5 ¶4.1.1.2 Table

"aggregate weighted value"

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

Population of Transmission Facilities

	A	B	C	D	E	F
1	Confidential					
2		# of lines				Total
3	Asset Name	< 200	200 - 299	300 - 499	> 500	Weight
61	Parsely 230/34.5 kV		2			1400.00
62	Sage 230/34.5 kV		4			2800.00
63	Rosemary 138/34.5 kV			3		3900.00
64	and Thyme 230 kV		5			3500.00
65	Cinnamon 500/161 kV	4			1	3001.00
66	Peppa 230/138 kV	3	1			700.00
67	Salt Road 230 kV		4			2800.00
68	Chipotle 138/34.5 kV	3				0.00

Reduced to Applicable Facilities

	A	B	C	D	E	F
1	Confidential					
2		# of lines				Total
3	Asset Name	< 200	200 - 299	300 - 499	> 500	Weight
63	Rosemary 138/34.5 kV			3		3900.00
64	and Thyme 230 kV		5			3500.00
65	Cinnamon 500/161 kV	4			1	3001.00

SPP RE will …Validate the Population

- Entity system maps/one-lines (TPL; FAC-008 Evidence)
- SPP Transmission Map Viewer
- Verify and document the list of substations planned in the next 24 months

Look for Common Sites

- Multiple ownership
- Close proximity or common line of sight (could pull in stations Registered Entity thought was below the 3000 aggregate weighted value)
- Multiple voltage levels
- Transmission Map Viewer
- Aerial maps

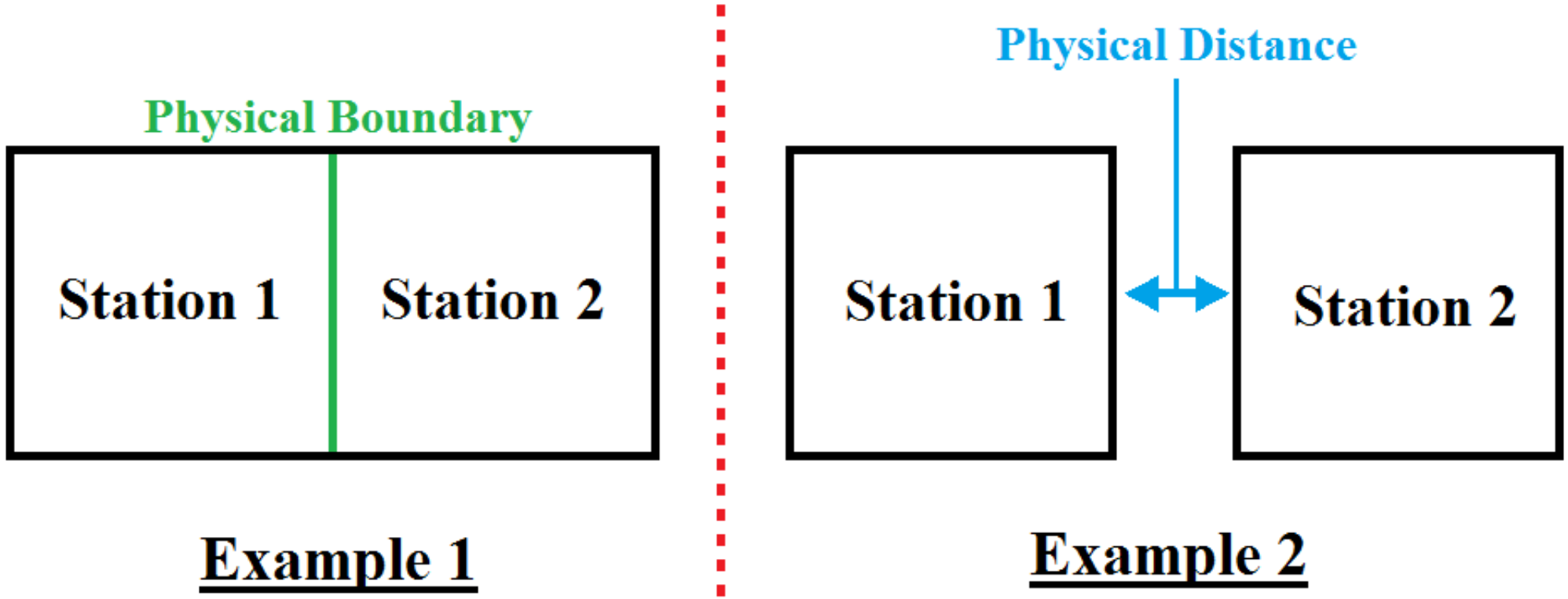
Initial Risk Assessment; R1

- Performed on applicable facilities (500kV or weighted value > 3000) – typically a subset of the overall population
- Specific risk assessment approach is not specified in the standard
- TO may determine criteria for critical impact by considering any of the following per the R1 technical basis:
  - TPL-001-4 R6
  - NERC EOP-004-2 reporting criteria
  - Area of magnitude or potential impact

Risk Assessment Considerations

- Consider loss of communications and the impact on "fast" or "slow", zone 1 or zone 2 trip
- High-speed reclosing (< 1 second) TPL-001-4 R4.3.1.1
- Generator stability
- Cascading outages
- Impact on BES (not just the registered entity's facilities)
- Loss of entire station, including all voltage levels, including adjacent (connected or line of sight) stations

Include other stations with your station if they are both exposed to a common physical attack



Compliance Guidance

NATF CIP-014

Note 3: In performing this analysis, the general approach is to take out one station at a time, not a combination of stations. A Transmission Owner may determine it is appropriate to take out more than one station at a time, as a result of two or more stations being in close proximity to one another. ***An example of the type of factors to consider, when considering close proximity, is where proximity is defined as having two (or more) substations situated such that there is either (i) an easy line-of-sight between all of the substation yards from a single site, (ii) an easy access from a common public roadway that exists between all of the substation yards, or (iii) the substation yards are in close enough proximity that a single event can impact both substations (e.g., the debris field from a reasonable incendiary device set off at one yard will impact the other yard).*** If such conditions exist, consider grouping these substations together before proceeding and treat them as a single substation when performing the next step.

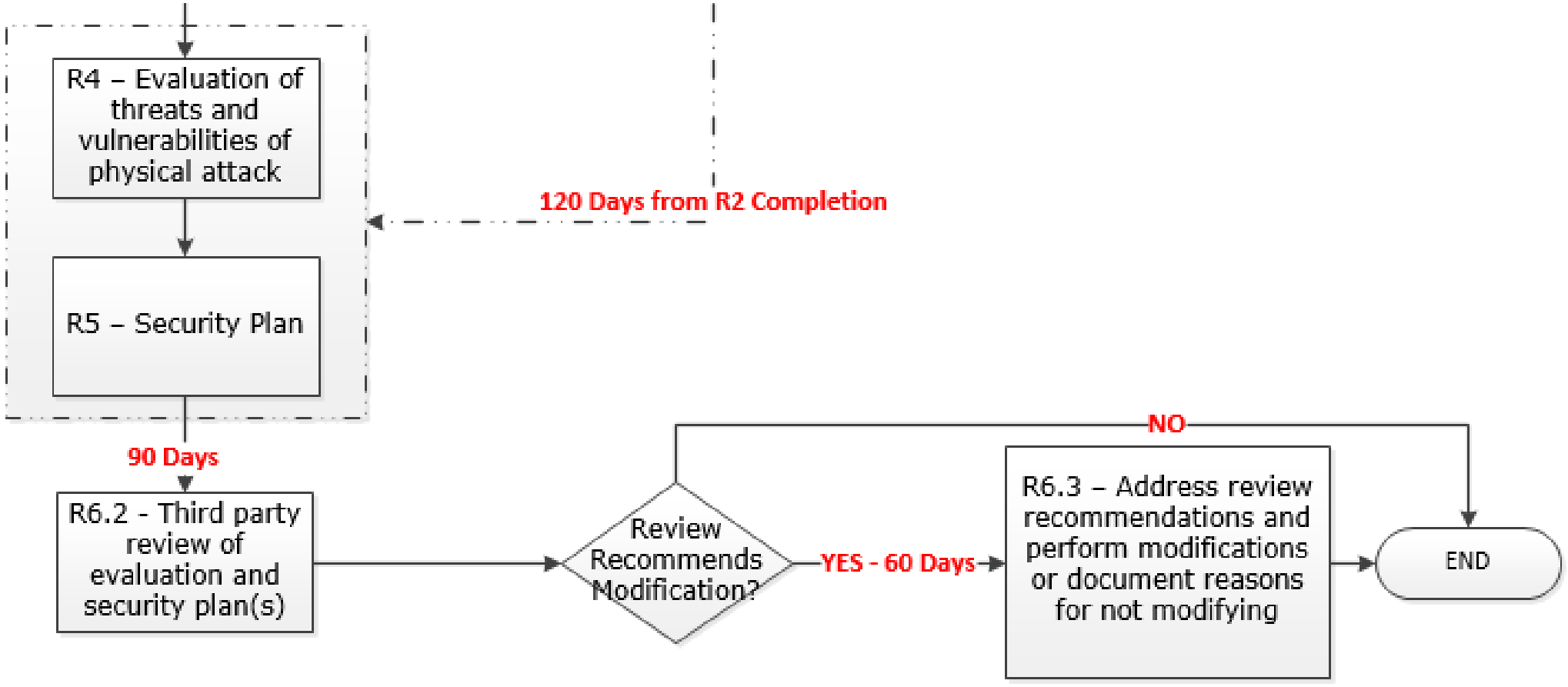
Third Party Verification; R2

- Third party is typically SPP or MISO
- Verify and document data considered by third party
- What documents were provided from the TO to third party?
- If third party has a different finding, the TO may:
  - Modify list or may document the technical basis for not modifying
  - Review and document differences between the TO and third party
  - Review third party non-disclosure agreement

R3- Primary Control Center

- Only applicable if a Transmission Owner that identified substations per R2 is not also the TOP for the identified substation.
- Notification (7 days) required to affected TOP that operationally controls identified station

Process Flow



CIP-014-2, Requirement R4

- **R4** – Each Transmission Owner that identified a Transmission station, Transmission substation, or a primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2. The evaluation shall consider the following:

CIP-014-2, Requirement R4

- **R4.1** – Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(s).
- **R4.2** – Prior history of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events.
- **R4-3** – Intelligence or threat warnings received from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U.S. federal and/or Canadian governmental agencies, or their successors.

CIP-014-2, Requirement R4 Audit Approach

- R4: Verify Entity conducted a threat and vulnerability assessment (TVA) of a physical attack to each of their respective stations, substations and primary control center(s) identified in R1 and verified according to R2.
- R4.1: Does the TVA address unique characteristics of the terrain/elevation of surrounding ground or structures providing line of sight?
  - What can the adversary see?
  - What are the vantage points for surveillance?

CIP-014-2, Requirement R4 Audit Approach

- R4.1: Does the TVA address unique characteristics of the line-of-sight distance from approach avenues (distance and direction that armament can be utilized)?
  - Are there concealment points?
  - How close can the adversary get to the target without being detected?
  - Are there any natural or man-made barriers to approach avenue surveillance or observation of the target?

CIP-014-2, Requirement R4 Audit Approach

- R4.1: Does the TVA address unique characteristics of the proximity to and speed of adjacent vehicular traffic for vehicle-induced damage?
  - How close can an adversary vehicle get to the target (stand-off distance)?
  - Are there any natural or man-made barriers that will prevent an adversary vehicle from approaching the target?
  - Are there any natural or man-made barriers that will prevent penetration of the target by an adversary vehicle?

CIP-014-2, Requirement R4 Audit Approach

- Does the TVA address unique characteristics of the proximity to traffic for easy vehicular access and egress (e.g., "drive-by" access)?
  - How close is the traffic to the target?
  - Is there line-of-sight visibility to the target from nearby publicly accessible roads?
  - Is there any natural or man-made barriers to visibility from nearby publicly accessible roads?

CIP-014-2, Requirement R4 Audit Approach

- R4.1: Does the TVA address unique characteristics of the proximity to other targets of interest or critical load (e.g., number of customers affected, densely populated area, high-profile commercial or governmental entities served, etc.)?
  - How many customers would be impacted by a successful attack of the target?
  - Are there any close-by valuable soft targets?
  - Are there any critical state or federal Government installations served by the target?

CIP-014-2, Requirement R4 Audit Approach

- R4.1: Does the TVA address unique characteristics of the number of operational targets, electrical component assets, etc. at a single site?
  - Are there multiple substations in close proximity to each other (can one attack impact multiple substations)?
  - How many substation Facilities can be targeted from one attack position?
  - How easily can the adversary move around the perimeter of the target(s)?

CIP-014-2, Requirement R4 Audit Approach

- R4.1: Does the TVA address unique characteristics of the proximity to company or other response personnel, may impact target selection and restoration response?
  - How long would it take for a company employee to be dispatched to the target site to investigate an alarm?
  - Are there conditions where multiple employees would need to gather at a rallying point before proceeding to the target site (additional response delay)?
  - Are there conditions where an employee will not be dispatched to the target site?

CIP-014-2, Requirement R4 Audit Approach

- R4.1: Does the TVA address unique characteristics of the proximity to law enforcement or emergency personnel may impact target selection and restoration response?
  - How long will it take for a first responder to arrive on site at the target?
  - Are there any impediments to contacting local first responders?
  - Are the first responders familiar with the target site (perhaps through a site orientation tour)?
  - Are the first responders aware of any hazards or other concerns for their safety that could delay response?

CIP-014-2, Requirement R4 Audit Approach

- R4.2: Does the TVA address historical events that have occurred at this location as well as similar facilities nationwide and the proximity of these events to the facility being assessed?
  - What is the source of the historical information?
  - How recent are the historical events?
  - What impact does current politics and the economy have?
  - Are there any differentiators between the subject site and similar sites that would affect the TVA for the subject site?

CIP-014-2, Requirement R4 Audit Approach

- R4.3: Does the TVA consider Intelligence or threat warnings received from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Information Sharing and Analysis Center (E-ISAC), U.S. federal and/or Canadian governmental agencies
  - What relationships have been established with threat intelligence sources?
  - How current is the threat intelligence used in the TVA?

CIP-014-2, Requirement R5

- **R5** – Each Transmission Owner that identified a Transmission station, Transmission substation, or primary Control Center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary Control Center(s). The physical security plan(s) shall be developed within 120 calendar days following the completion of Requirement R2 and executed according to the timeline specified in the physical security plan(s). The physical security plan(s) shall include the following attributes:

CIP-014-2, Requirement R5

- **R5.1** – Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4.
- **R5.2** – Law enforcement contact and coordination information.
- **R5.3** – A timeline for executing the physical security enhancements and modifications specified in the physical security plan.
- **R5.4** – Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).

CIP-014-2, Requirement R5 Audit Approach

- R5.1: Deterrence
  - Is there prominent and clearly visible and legible signage?
  - Are there natural or man-made perimeter barriers?
    - Non-scalable?
    - Ballistic protection?
    - Obscured visibility?
    - Gates/doors of equal level of protection as fence/walls/cable?
    - Tamper-resistant construction of barriers?

CIP-014-2, Requirement R5 Audit Approach

- R5.1: Deterrence
  - Are there on-site or roving security personnel?
    - Do the security personnel work in teams or solo?
    - Are the security personnel properly trained?
    - Are the security officers armed?
    - Do the security personnel have and know their post orders?
    - Do the security personnel have adequate communication capability?

CIP-014-2, Requirement R5 Audit Approach

- R5.1: Deterrence
  - Has security lighting been installed?
    - Is there lighting facing outward from the site perimeter?
    - Is the lighting continuous or upon motion detection/manual control?
    - Are there areas of insufficient illumination or excessive glare?
    - Are the lamp types used compatible with CCTV cameras used?
    - Is the lighting protected (protective covers, mounting height, placement inside the perimeter barrier, backup power supply)?

CIP-014-2, Requirement R5 Audit Approach

- R5.1: Deterrence
  - Are locks used to secure the perimeter or specific areas within the perimeter?
    - Are acceptable types of locks prescribed?
    - Is there a key control/key management program?
      - Is there a process for issuance and retrieval of keys?
      - Are key periodically inventoried?
      - Is there a process for lost or missing keys?

CIP-014-2, Requirement R5 Audit Approach

- R5.1: Detection
  - Are physical intrusion detection systems installed?
    - Types include security guards, access control systems, mantraps, vehicle traps, motion/vibration sensors, and video surveillance/
    - Are there any gaps in coverage under normal operating conditions?
    - Are there any problems with attenuation in adverse operating conditions (smoke, fog, rain, snow, etc.)?
    - Are there periodic gaps in coverage (e.g., PTZ cameras slave to detected motion leaving a gap in coverage)?

SPP

CIP-014-2, Requirement R5 Audit Approach

- R5.1: Detection
  - Is a sound detection system installed?
    - Does the detection system notify response personnel 24x7?
  - Is there a Security Operations Center?
    - Is the SOC staffed 24x7?
    - Are all field detection systems being monitored in the SOC?
    - Does the SOC staff have the necessary tools/technology to assess the detected activity and initiate the appropriate response?
    - Have response procedures been documented and tested?

CIP-014-2, Requirement R5 Audit Approach

- R5.1: Delay
  - Have vehicle barriers been installed?
    - Energy absorbing barriers
    - Cable systems
    - Hardscaping (benches, planters, bollards, "Target balls")
    - Landscaping
      - Technical excavations
      - Reshaping of perimeter drainage

CIP-014-2, Requirement R5 Audit Approach

- R5.1: Delay
  - Have individual protections been implemented within the substation for critical components?
    - Individual barriers (e.g., cages)
    - Protective coverings or coatings
    - Raising the critical component
  - Have multiple layers of delay been implemented?
    - Numerous sequentially encountered barriers to slow the adversary down or block the path to the intended target

CIP-014-2, Requirement R5 Audit Approach

- R5.1: Delay
  - Is there a buffer zone beyond the primary fence line surrounding the substation or control center?
  - How has fencing / walls / gates been utilized?
    - Are there two or more fence lines to create a dead zone for monitoring where no motion would be expected?
    - Have vehicle traps been installed to prevent tailgating?
    - Has automatic exit capability (IR beams, ground sensors) been removed or disabled?

CIP-014-2, Requirement R5 Audit Approach

- R5.1: Additional Considerations
  - Is there an escort policy/procedure for visitors and personnel not authorized unescorted access?
    - Are all personnel familiar with the escort policy/procedure?
  - Are personnel familiar with the site physical security plan?
  - Do the response procedures include required response plans?
  - Auditors will likely interview staff and test response times.

CIP-014-2, Requirement R5 Audit Approach

- R5.2: Law Enforcement contact information and coordination
  - Does the physical security plan include law enforcement contact and coordination information?
    - Name and/or phone number
    - Coordination meetings to discuss site-specific security and hazard concerns
    - Site-specific orientation training
    - Hosting law enforcement training exercises

CIP-014-2, Requirement R5 Audit Approach

- R5.3: Timeline for implementing physical security enhancements and modifications
  - Project plan with milestone dates
  - Current status of plan execution
- R5.4: Provisions to review evolving physical security threats to CIP-014 assets and corresponding security measures
  - Does the plan include a process to receive threat information?
  - Does the plan include a process to review threat information upon receipt?

CIP-014-2, Requirement R6

- R6 – Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5.

CIP-014-2, Requirement R6

- R6.1 – Each Transmission Owner and Transmission Operator shall select an unaffiliated third party reviewer from the following:
  - An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification.
  - An entity or organization approved by the ERO.
  - A governmental agency with physical security expertise.
  - An entity or organization with demonstrated law enforcement, government, or military physical security expertise.

CIP-014-2, Requirement R6

- 6.2 – The Transmission Owner or Transmission Operator, respectively, shall ensure that the unaffiliated third party review is completed within 90 calendar days of completing the security plan(s) developed in Requirement R5. The unaffiliated third party review may, but is not required to, include recommended changes to the evaluation performed under Requirement R4 or the security plan(s) developed under Requirement R5.

CIP-014-2, Requirement R6

- 6.3 – If the unaffiliated third party reviewer recommends changes to the evaluation performed under Requirement R4 or security plan(s) developed under Requirement R5, the Transmission Owner or Transmission Operator shall, within 60 calendar days of the completion of the unaffiliated third party review, for each recommendation:
  - Modify its evaluation or security plan(s) consistent with the recommendation; or
  - Document the reason(s) for not modifying the evaluation or security plan(s) consistent with the recommendation.

CIP-014-2, Requirement R6

- 6.4 – Each Transmission Owner and Transmission Operator shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated third party reviewer and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

CIP-014-2, Requirement R6 Audit Approach

- R6: Was an unaffiliated third-party review conducted?
- R6.1: Was the review performed by a qualified third party?
- R6.2: Was the third-party review completed no more than 90 calendar days after completing the physical security plan(s) required by R5?
- R6.3: If the third-party review recommended changes…
  - Was the security plan(s) modified accordingly, or
  - Were the reasons for not modifying the security plan(s) documented

CIP-014-2, Requirement R6 Audit Approach

- R6.4: Protection of sensitive or confidential information
  - What procedures were implemented to protect the confidentiality of the physical security plan information?
  - Do the procedures include protections from public disclosure?
    - Document markings
    - Encryption
    - Controlled copies
    - Transmittal and receipt procedures

Questions

Kevin Perry
Director, Critical Infrastructure Protection
501-614-3251
kperry.re@spp.org

Jeff Rooker
Lead Compliance Engineer
501-614-3278
jrooker.re@spp.org