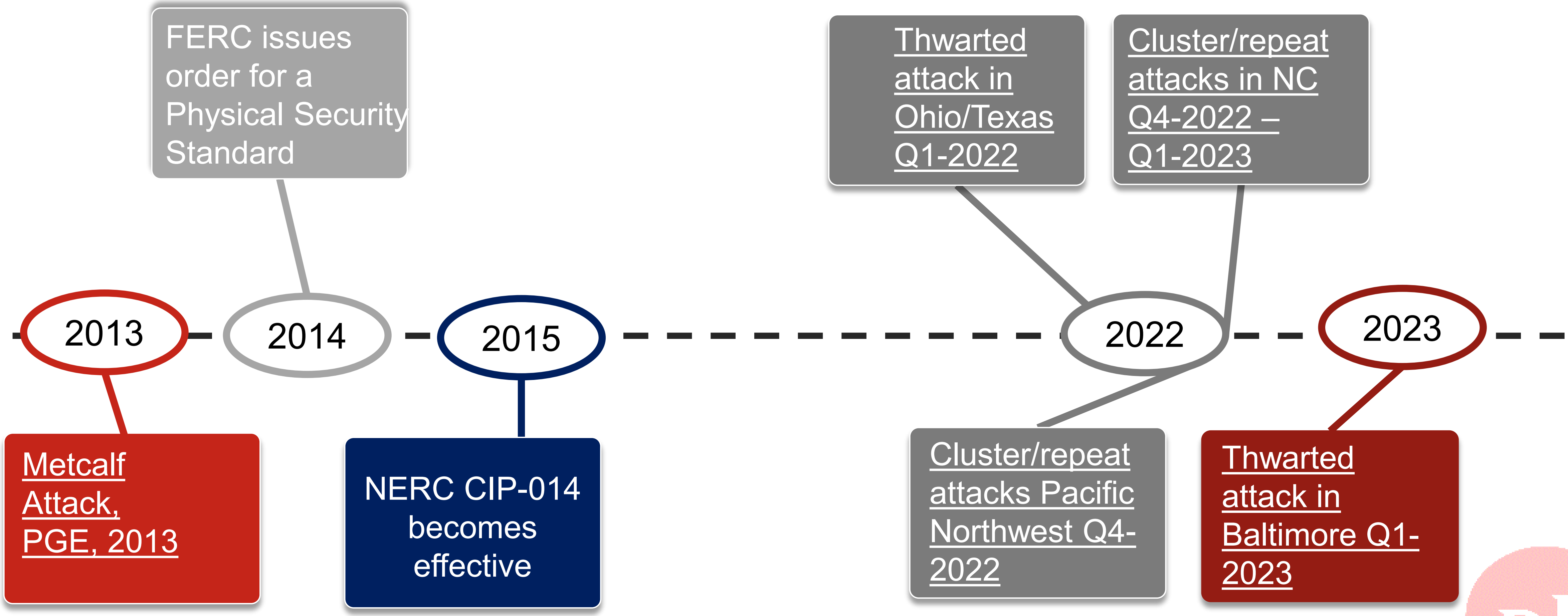
RELIABILITYFIRST

Substation Physical Security

Mike Hughes, PE, CIA, CPP
Manager of Entity Engagement
April 17, 2023
Technical Talk with RF

A Quick Look Back

Annual OE-417 reports list known/reported physical attacks on electric infrastructure, including vandalism and suspicious activity (**over 160 reported in 2022; 41 in January and February 2023**)



2013

Metcalf Attack, PGE, 2013

2014

FERC issues order for a Physical Security Standard

2015

NERC CIP-014 becomes effective

2022

Thwarted attack in Ohio/Texas Q1-2022

Cluster/repeat attacks in NC Q4-2022 – Q1-2023

Cluster/repeat attacks Pacific Northwest Q4-2022

2023

Thwarted attack in Baltimore Q1-2023

Recent Development

Attacks Increase

The industry has experienced a notable increase in repeat and clustered attacks on electric infrastructure in Q3-Q4 2022 compared to baseline trends over the past 18 months.

FERC Inquiry to NERC

FERC directed NERC to study the need for improvements to CIP-014 (Docket No. RD23-2-000, Dec. 15, 2022).

[See links to recent events in the footnotes on page 3 of the Order.]

Basic Security Measures

RF recommends implementation of basic physical security measures for all critical facilities and projects. These actions may be taken or initiated voluntarily while NERC and FERC evaluate changes to the standards.

Which Approach?

Resilience Approach

a. Expanded planning studies to include coordinated security attacks

b. Enhanced Real-time Assessments

c. Enhanced spare equipment pool strategies

d. Readiness scenario training

Basic Security Approach

a. RF recommends basic physical security measures for all critical facilities and projects.

b. The applicability, design, and schedule are at the discretion of the utility.

How do voluntary measures differ from the CIP-014 approach?

CIP-014-3 Approach

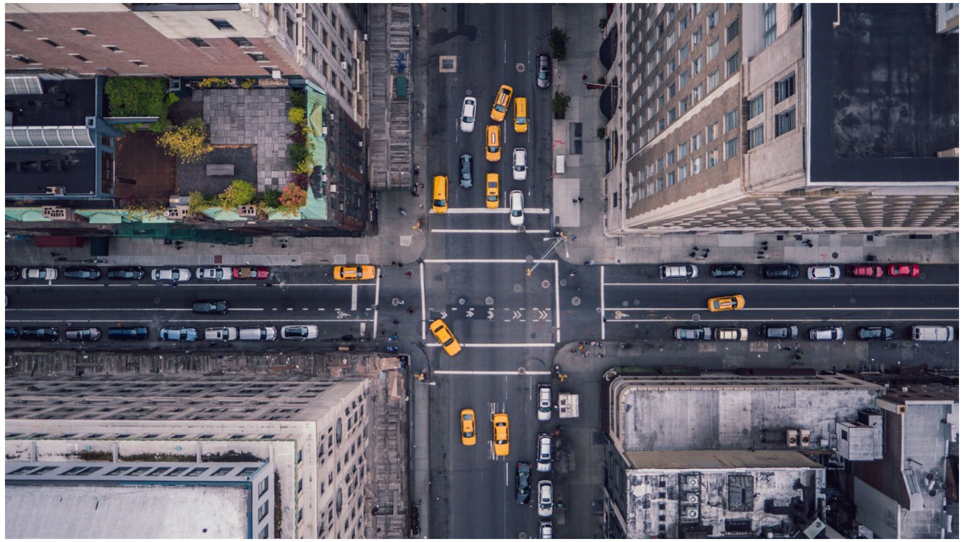
- Not applicable < 200 kV
- Applied to stations that if rendered inoperable, could result in instability, uncontrolled separation, or Cascading
- Commonly uses a Design Basis Threat (DBT) and vulnerability assessment
- DBT definition

Voluntary Approach

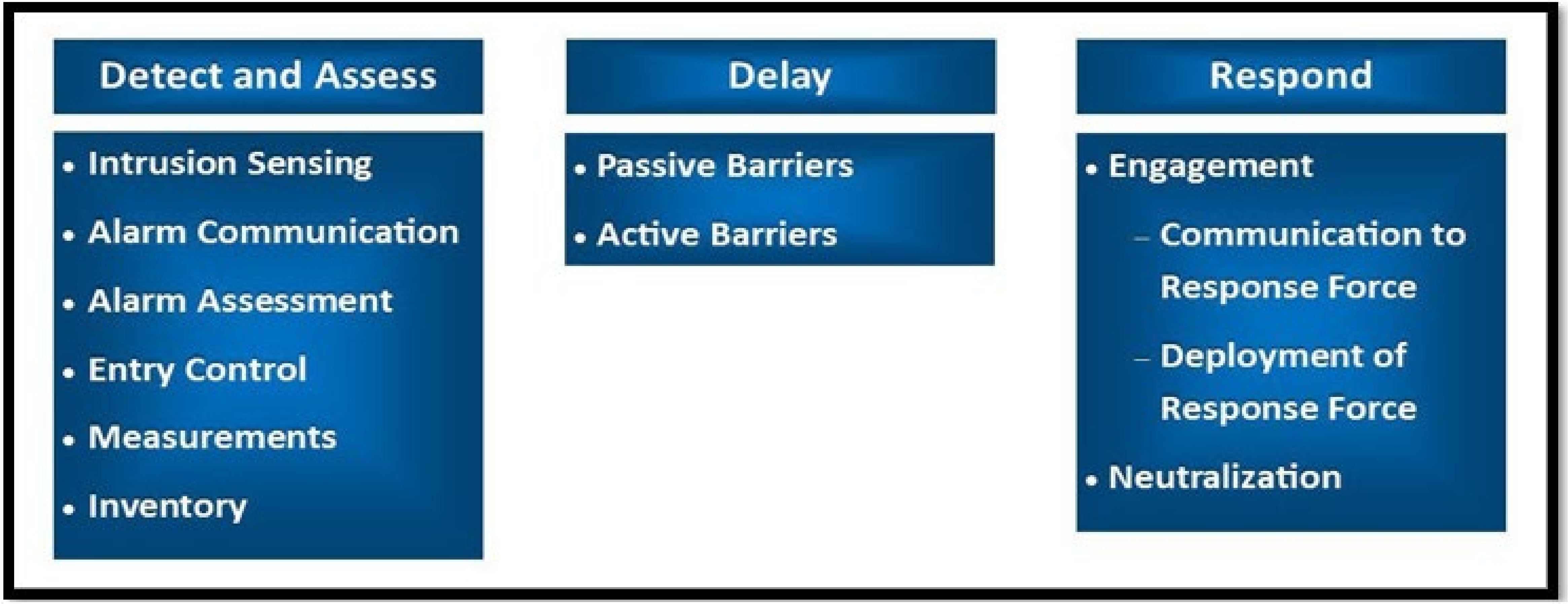
- May be applied at any voltage (beyond CIP-014 requirements), including < 200 kV and distribution
- Utility establishes priorities
- Utility may apply a DBT and vulnerability assessment or may establish and implement baseline physical security measures

Why implement voluntary measures?

- **Physical attacks on critical infrastructure, beyond facilities considered in CIP-014, and beyond traditional planning criteria, can result in sustained outages unacceptable at the local level. Many life-sustaining activities are reliant upon electricity:**
  - Home heating and cooling
  - Water processing, pumping, and delivery
  - Fuel deliveries (gas stations for the public)
  - Grocery stores and home refrigeration
  - Traffic lights
  - Hospitals
  - Fire/EMS/Police Services



The Goal of Baseline Physical Security Measures



Detect and Assess

- Intrusion Sensing
- Alarm Communication
- Alarm Assessment
- Entry Control
- Measurements
- Inventory

Delay

- Passive Barriers
- Active Barriers

Respond

- Engagement
  - Communication to Response Force
  - Deployment of Response Force
- Neutralization

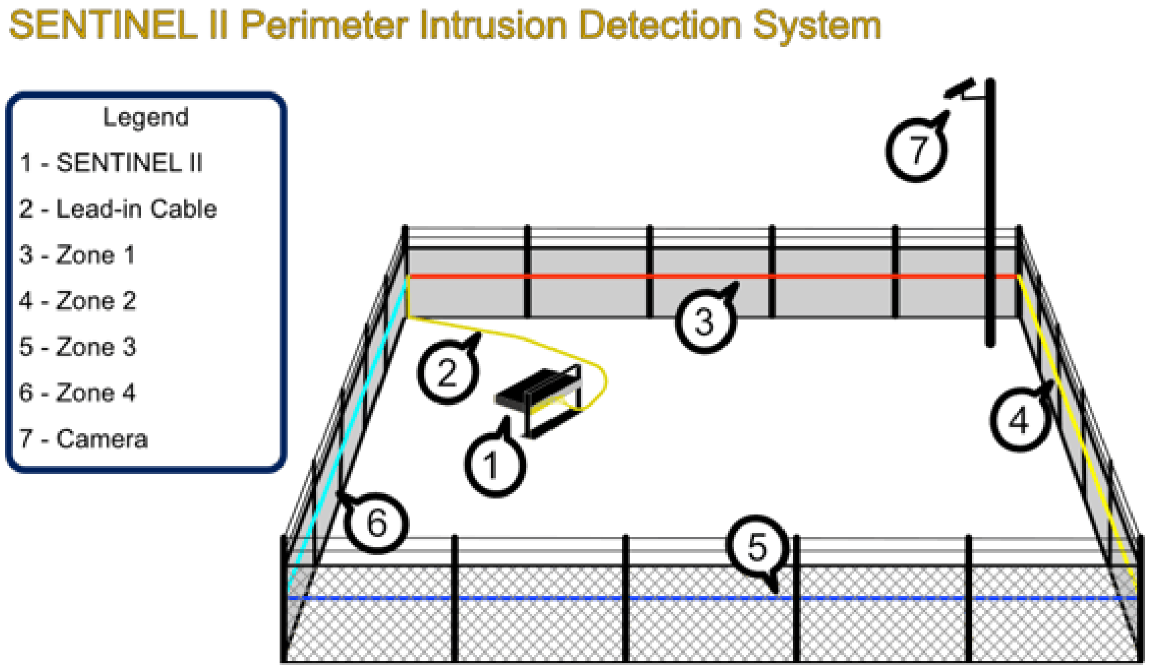
Deter

Before "*Detect and Assess, Delay, Respond*" - - "Deter"

- ➢ **Roadway Entry Gate**
- ➢ **Lighting**
- ➢ **Signage**
  - *Private Property*
  - *No Trespassing*
  - *Utility Personnel Only*
  - *Camera May Be In Use*

Detect and Assess

- **Electronic Entry Control (Badge; Keypad)**
- **Control Center or Security Operations Center (SOC) Check-In**
- **Cameras**
  - Motion Sensor Alarm
  - Fixed and Pan-Tilt-Zoom (PTZ)
  - Infrared
- **Fence Intrusion Detection**
  - *"A barrier without an intrusion detection system is just an inconvenience to intruders"*



Example graphic
(Source: Network Integrity Systems)

Control Buildings

- Restrict and monitor access
  - Card access
  - Call-in procedure
  - Camera monitoring
- Smoke detector
- Fail safe egress

Infrared Camera

Example photo
(Source: Security Alarm)

- ➢ Alarm thermal motion in specific areas such as gate
- ➢ Check for abnormal heating of transformers, breakers, other equipment
- ➢ May need to remove vegetation for clear line of sight around substation
- ➢ Detects fires

Gunshot Detection

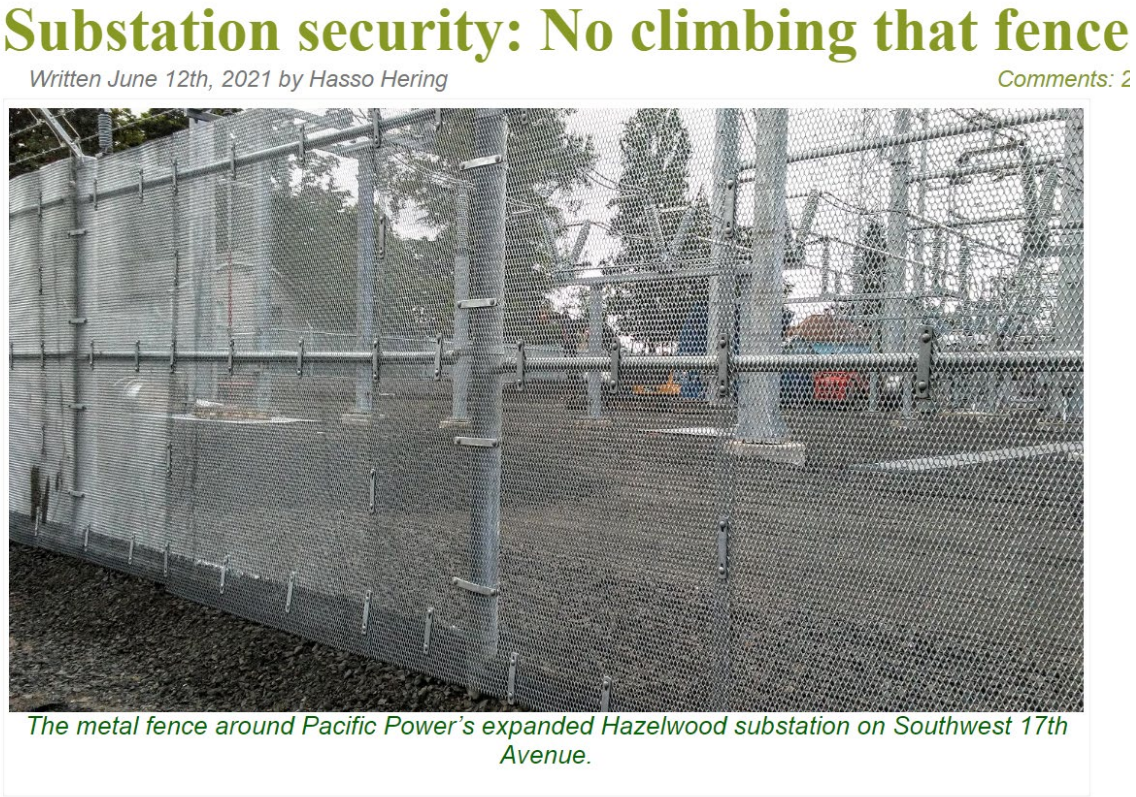
DRAGONFLY EX | 300K

Example product
(Source: EAGL Technology)

- **Example outdoor wireless gunshot sensor**
  - Performs energy capture, waveform analysis and transmits resultant data
  - Often deployed in multiples of two or three to assist with assessment

Delay

- **Expanded metal or mesh fencing**
  - Offers added resistance to cutting and climbing
  - Serves as both a deterrent and a delay measure



Substation security: No climbing that fence

Written June 12th, 2021 by Hasso Hering

Comments: 2

The metal fence around Pacific Power's expanded Hazelwood substation on Southwest 17th Avenue.

Example photo

(Source: https://hh-today.com/substation-security-no-climbing-that-fence/*)*

Delay

Hardened substation with ballistic barrier fence and/or ballistic panels shielding specific equipment.

Example photo
(Source: Presentation by Bill Peterson, SERC)

Example photos
(Source: Southern States)

Respond

Control Center or SOC rapid assessment and communication to dispatch law enforcement

- NERC Lessons Learned for Substation Fires
- Have list of emergency contacts for each substation on-hand for immediate use
  - Law enforcement
  - Fire department
- Establish a working relationship with each local fire department in your territory to discuss the hazards present in substations and exchange information on how to address substation fires. Repeat every one to two years to train new staff at both the utility and the fire department. (P.S. *Lunch is a good draw*.)
- Design, fine-tune, or modify to avoid nuisance alarms
- Nuisance alarms are less common as you progress through perimeters
- Mike Hattery will address alarm apathy in his presentation to follow

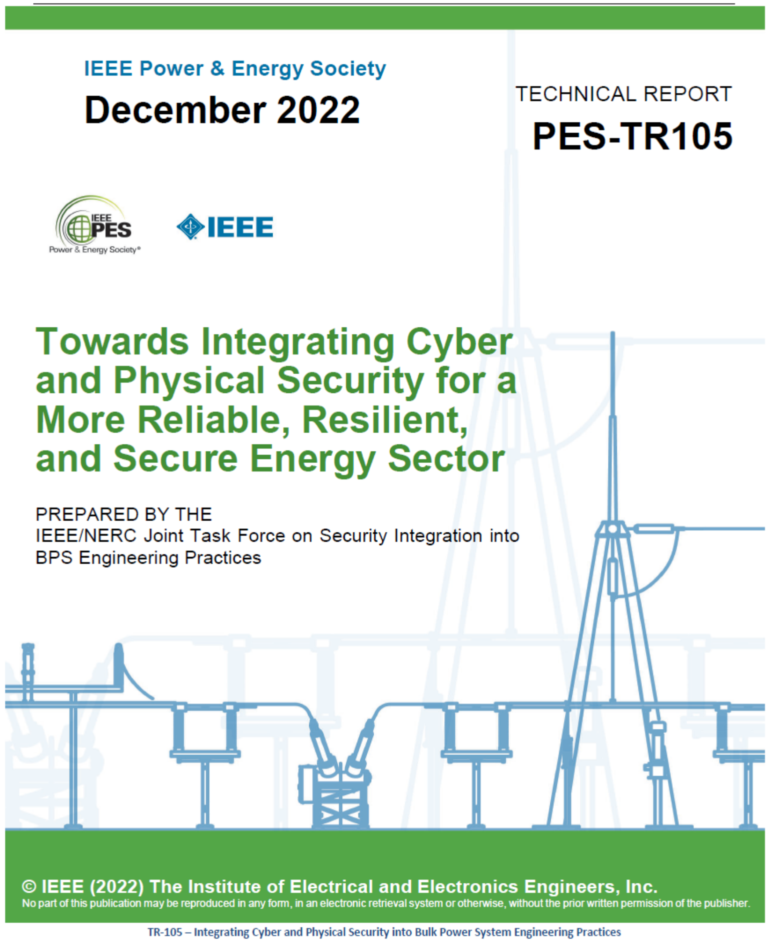
Integrate Cyber and Physical Security

- NERC's New Strategy Seeks to Ensure Reliability by Integrating Cyber and Physical Security into Grid Planning, Design, and Operation

- See the IEEE PES-TR105 Technical Report prepared by the IEEE/NERC Joint Task Force

RF Contributors include:

- Jim Uhrin
- Johnny Gest
- David Sopata



IEEE Power & Energy Society

December 2022

TECHNICAL REPORT

PES-TR105

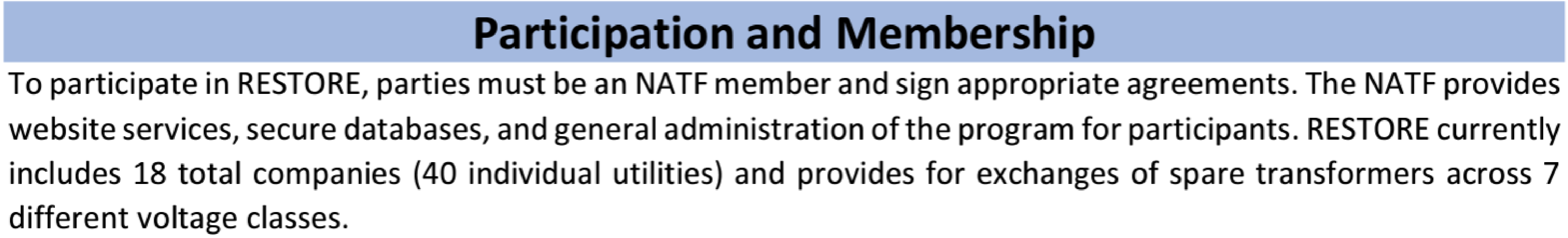
Towards Integrating Cyber and Physical Security for a More Reliable, Resilient, and Secure Energy Sector

PREPARED BY THE
IEEE/NERC Joint Task Force on Security Integration into
BPS Engineering Practices

TR-105 – Integrating Cyber and Physical Security into Bulk Power System Engineering Practices

Spare Parts

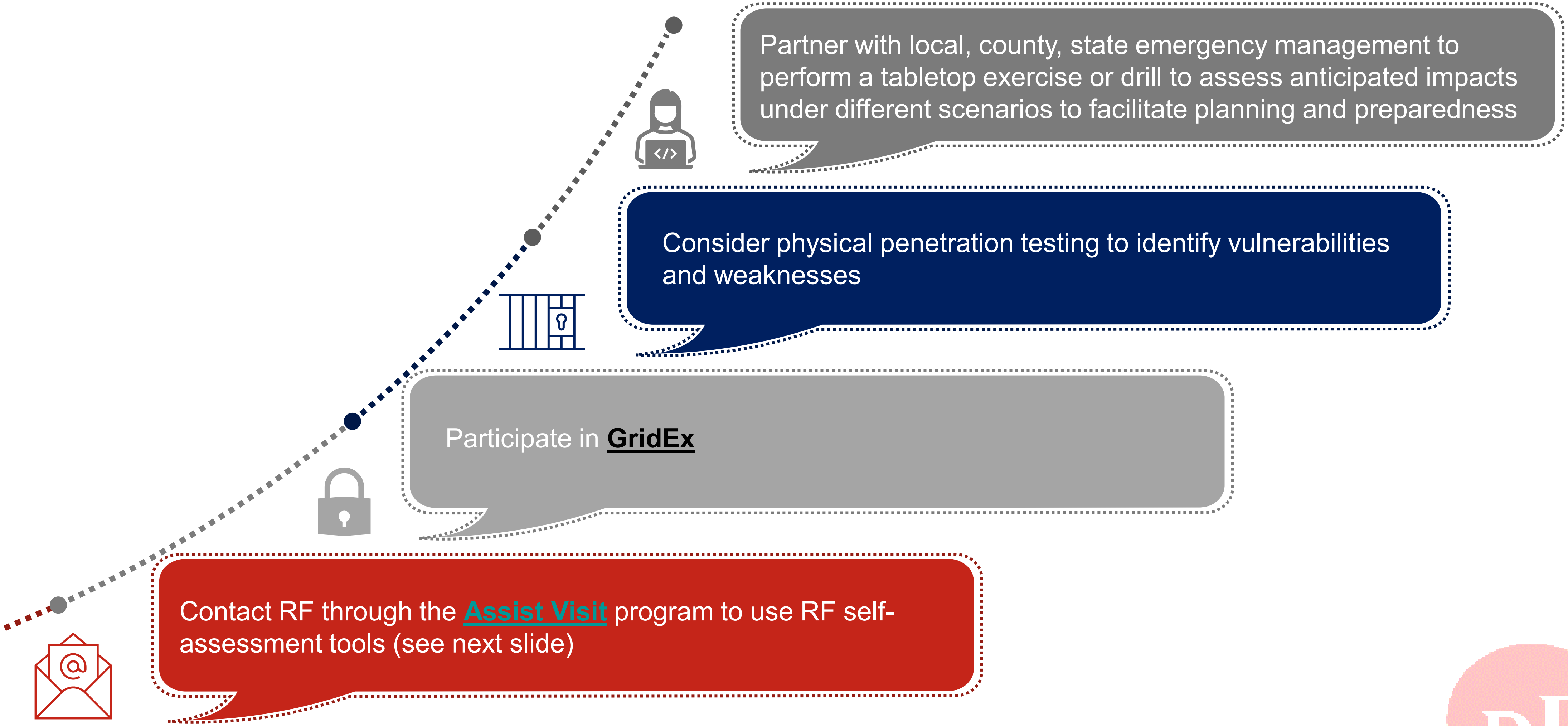
- Plan for, or consider spare parts inventory for loss of equipment at multiple substations
- Consider mutual aid programs such as the NATF Restore Program
- NATF Restore FAQ



Participation and Membership

To participate in RESTORE, parties must be an NATF member and sign appropriate agreements. The NATF provides website services, secure databases, and general administration of the program for participants. RESTORE currently includes 18 total companies (40 individual utilities) and provides for exchanges of spare transformers across 7 different voltage classes.

Tabletop Exercise Drills



Partner with local, county, state emergency management to perform a tabletop exercise or drill to assess anticipated impacts under different scenarios to facilitate planning and preparedness

Consider physical penetration testing to identify vulnerabilities and weaknesses

Participate in **GridEx**

Contact RF through the Assist Visit program to use RF self-assessment tools (see next slide)

RF Self Assessment Tools

01

Cyber Resiliency Assessment Tool (**CRAT)**

- Individual survey-based maturity assessment
- Single point-in-time assessment
- Energy sector focused on cybersecurity

02

Insider Threat Program Maturity Assessment Tool (**InTP**)

- Collaborative survey-based maturity assessment
- Single point-in-time assessment
- Physical and cybersecurity focused, can apply to multiple industries

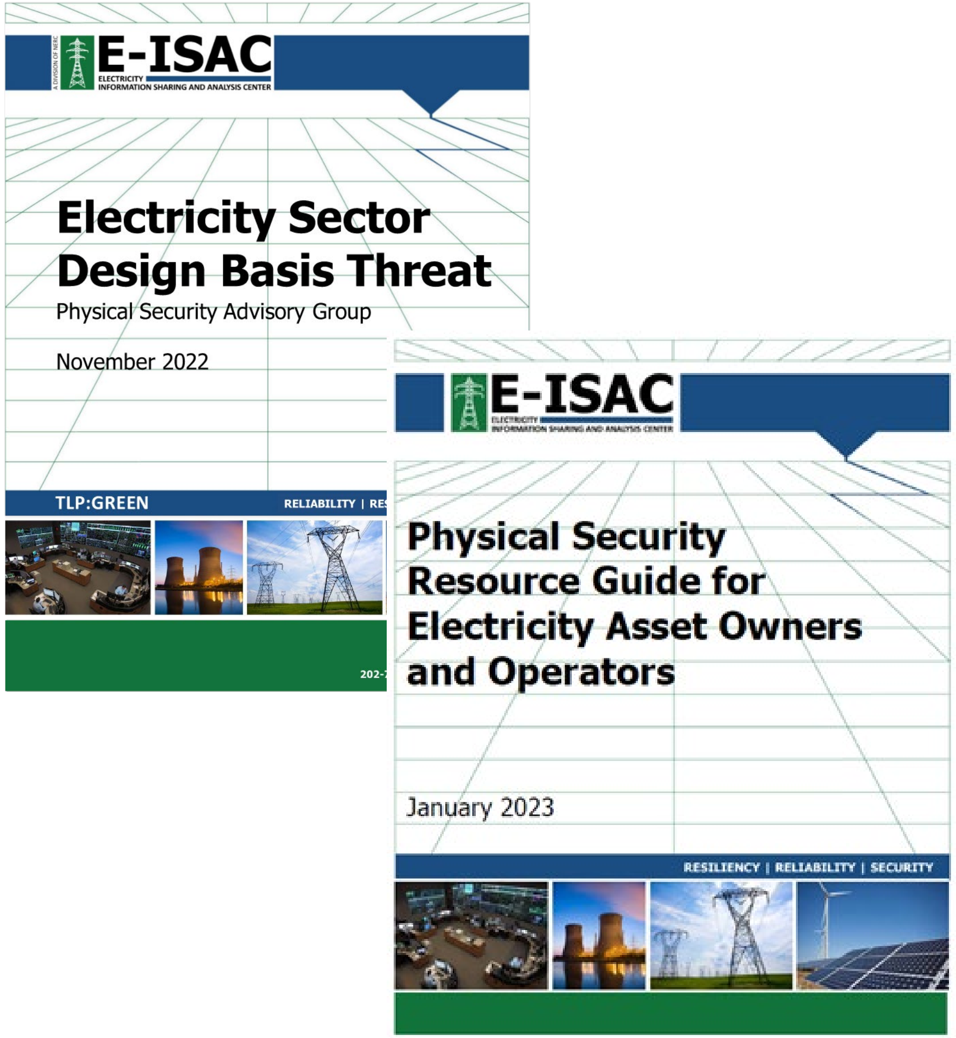
03

Incident Response Preparedness Assessment Tool (**IRPAT**)

- Collaborative survey-based maturity assessment
- On-demand continuous assessment
- Energy sector focus with IT and Industrial Control Systems(ICS) focus

Threat Intelligence and Information Sharing

- Partner with NERC E-ISAC for information sharing
- 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), SERC, and RF.
- For additional resources, program specific questions or additional assistance from RF, contact the Entity Engagement Department through the [Assist Visit]() program.



E-ISAC
ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

Electricity Sector Design Basis Threat

Physical Security Advisory Group

November 2022

TLP:GREEN

RELIABILITY | RES

E-ISAC
ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

Physical Security Resource Guide for Electricity Asset Owners and Operators

January 2023

RESILIENCY | RELIABILITY | SECURITY

Raise the Bar

- Plan, initiate and install basic physical security measures for all critical facilities and projects

Detect and Assess

Delay

Respond

Questions & Answers

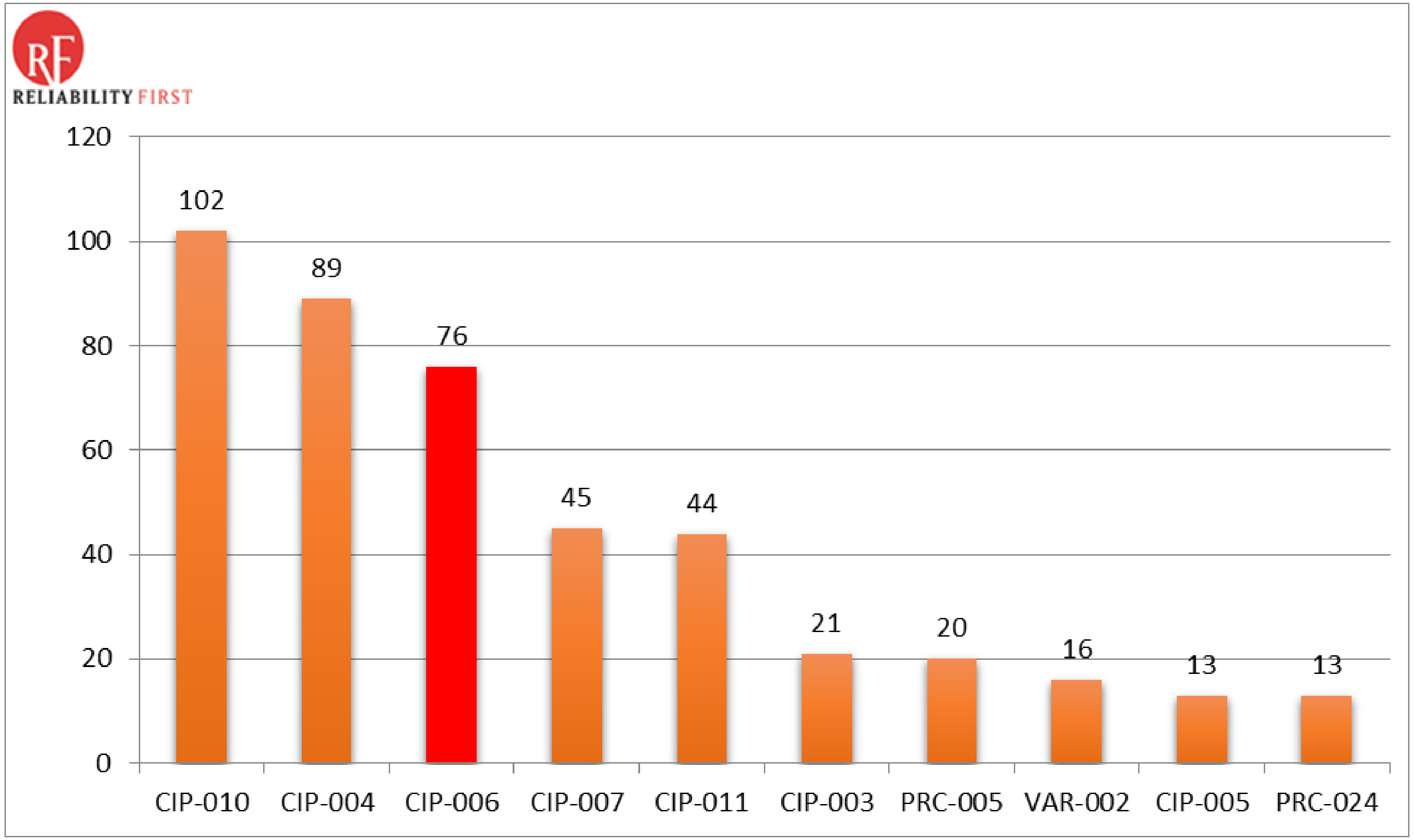
Forward Together ReliabilityFirst

RELIABILITYFIRST

Enforcement Explained: Physical Security Trends

Mike Hattery

Physical Security Intake: 2022 Ten Most Violated Standards



Testing and Reviewing CIP-006 Controls

- **CIP-006-6 is a floor not a ceiling for Physical Access Controls**
- **Where we see CIP-006-6 noncompliances which results in preventative or identification control failures:**
  - Malfunctioning Physical Access Control Systems
    - Power transitions
    - Patch implementation
    - Faulty restarts

Automated Alarms: Avoiding Apathy

Questions & Answers

Forward Together ReliabilityFirst