CIP-014
Incident Response Planning

John Puccioni
Staff Auditor, WECC

Frank Gauthier
Critical Infrastructure Protection, Principle, Pacific Gas & Electric

Electric Reliability & Security for the West

October 15, 2025

Purpose

- The purpose of this presentation is to provide a basis for a discussion regarding CIP-014 Incident Response and Preparation
- Think about what works for your program
- Open discussion and idea sharing
- Example of CIP 14 plan in action

Presenters

John Puccioni

- Over 15 years experience in physical, corporate security, and critical infrastructure
  - NV Energy
  - Sphere Las Vegas
- Workplace Violence and Active Shooter Response Instructor
- Designed and implemented numerous site-specific physical security plans
- Conducted several threat and vulnerability assessments with mitigation plans for high-value assets

Frank Gauthier CPP, PSP, PMP

- 40+ years military, law enforcement, foreign diplomatic security, and critical infrastructure protection experience
  - USAF
    - Crew Chief Nuclear B-52 Bombers
  - Sheriff's Department Sergeant
    - SWAT Team Leader
  - Department of State High Threat Protection (Contractor)
    - Protection Detail Leader, U.S. Ambassador to Iraq
    - Manager HTP U.S. Consulate Herat, Afghanistan
  - PG&E Critical Infrastructure Protection & Compliance
    - CIP-014 Lead
    - Manage multiple CIP-014 R4, R5, R6 iterations across multiple sites

Things to Consider

Considerations

- Site-specific threat and vulnerability assessments
  - Vulnerability cannot be assessed without direct correlation to known physical threats
- Understand that location of site will greatly impact response time
  - Law enforcement familiarity and understanding will greatly impact response time
- Importance of adversary sequencing

Adversarial Sequence Diagram

Task 1: x Time
Task 2: x Time
Task 3: x Time
Task 4: x Time
Task 5: x Time

Total Time: x Time

Tools to Improve Response

- Evolving security plan
  - Sites change and threats emerge
- Testing and training of security staff
  - Scheduled drills—don't over complicate
  - Penetration testing—don't over complicate
- Routine accuracy checks of contact information for response parties

Tools to Improve Response

- Security awareness and training of employees
  - Criticality awareness
  - Threat awareness
  - Compliance awareness
- Other actions
  - Notifications of employees arriving to site
  - Expectation of employees on site
  - Mass communication to affected employees?

DDDACR and Why It’s Important

DDDACR

- Deter
  - Prevent incident from occurring
    - Creating target shift is a great outcome
- Detect
  - Motion/gunshot
  - Fence cut or climb
  - Outside of perimeter
- Delay
  - Delay without detection is not delay
  - CPTED

DDDACR

- Assess
  - Combo of fixed/PTZ cams
    - Ensure all alarm zones can be assessed
- Communicate
  - Real-time information flow to comm systems
  - Notification to on-site personnel
- Respond
  - PA system
  - Auto vs. scripted vs. unscripted
  - External resources

External Response

- Partner with law enforcement
  - Networking and information sharing
  - Discuss system and impact of loss to public
  - Get their buy-in
- Other groups to consider
  - BLM
  - Fish and Wildlife
  - Local hunting/target shooting groups if rural

Post Incident

Post Incident

- Site walk
  - Check for damage, loss, and point of entry
  - Check exterior
    - Potential evidence
    - Avenue of approach
  - Notify cybersecurity to monitor for potential intrusion devices
  - Work with SMEs to assess damage and value of loss and replacement
    - True value of loss
    - Necessary for police report
  - Prepare documentation and video footage clips

Post Incident

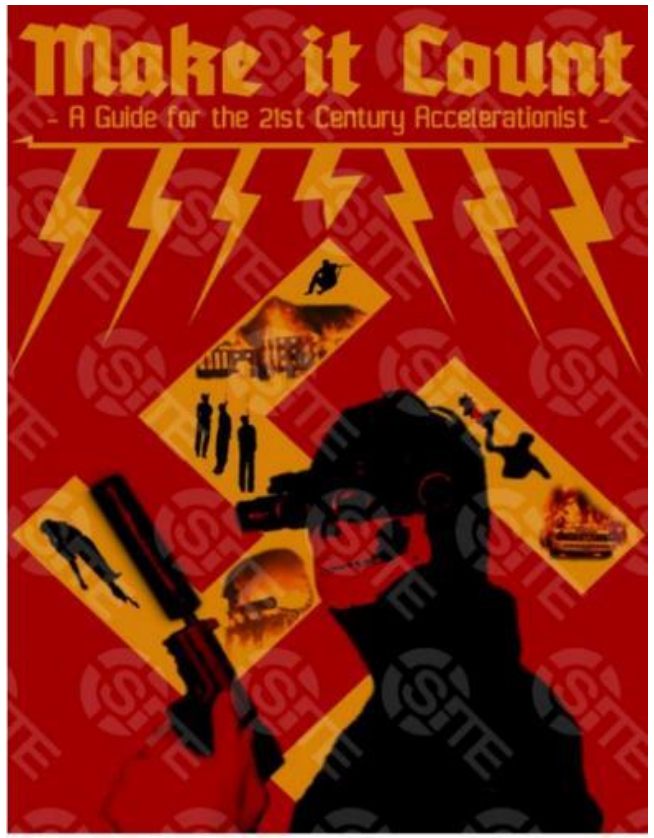
- External notifications
  - EOP-4 reporting
    - Check Attachment 1 for Reportable Events
    - Use reporting form on Attachment 2
  - DOE-OE-417
  - E-ISAC reporting
  - Partner with local law enforcement to convey importance
  - Be sure to include actionable items in report

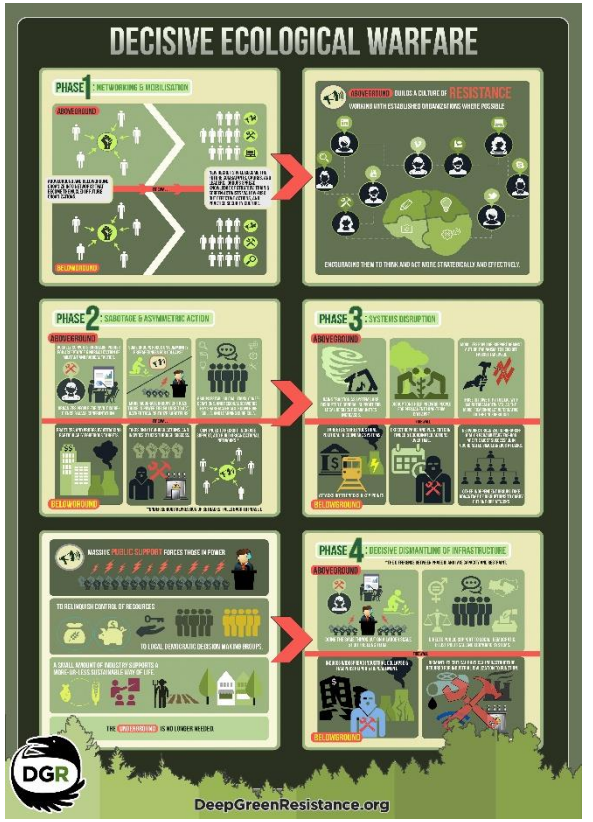
Final Thoughts

- Find what works for your program
- Keep in mind the impact to daily operations
- Questions?

Threat Detection Program

- **Cyber Threat Team**
- **Insider Threat Team**
- **External Threat Team**
  - Executive protection
  - Critical infrastructure





"Warrior Up" Announced Return After 5 Year Hiatus May 2025

LE Contact & Coordination Program

- POST certified training
- Criticality awareness
- Threat awareness
- Site visits / tour
- Maps & KMZ
- Reciprocity

Internal Training Program – Key Performance Indicator (KPI)

- **Web-based training (WBT) for NERC access**
  - All employees
  - All security officers

- **NERC 0900**
  - CIP-014 Critical Infrastructure Protection
  - Annual, in person, CSD instructor led
  - Employees commonly working at CIP-014
  - Security officers assigned to CIP-014
    - Completely changed the level of performance of the guards

Penetration Testing Program – Key Performance Indicator (KPI)

- **200+ sites per year**
- **Level-based**
  - Level One
  - Level Two
  - Level Three
    - Red Team
- **Communicate results**
  - Simple spreadsheet
    - Not long reports
- **Drives**
  - Policy change
  - Procedure change
  - Drives training

Current Technology

- **Precast concrete wall barriers**
  - Anti-cut / anti-climb
  - Ballistically resistant
- **100% detection & assessment**
  - Edge-based video analytics
  - 2D ground radar
  - 100% PTZ assessment
  - Gunshot detection

Future Technology

- **Anti-dig barrier**
- **Crash rated gates**
- **Sallyport access control point**
- **Elevated guard post with technology**
- **LRAD**
  - HD long range camera
  - High intensity spot and strobe light
  - High intensity alert tone
  - Laser dazzler
- **Security controlled lighting scheme**
- **Drone detection & assessment systems**
- **Ballistic protection of critical assets**

Thank you!

WECC

WWW.WECC.ORG | (801) 582-0353

155 N 400 W, Salt Lake City, UT 84103, USA