
Reliability & Security Workshop
WECC
March 17–18, 2026
San Diego, California

ATC's Approach to Physical Security and Incident Response

PRESENTED BY:

Frank Berry, CPP

Physical Security Program Lead

Scott Quenneville

Manager, Enterprise Security Operations & Engineering

March 18, 2026

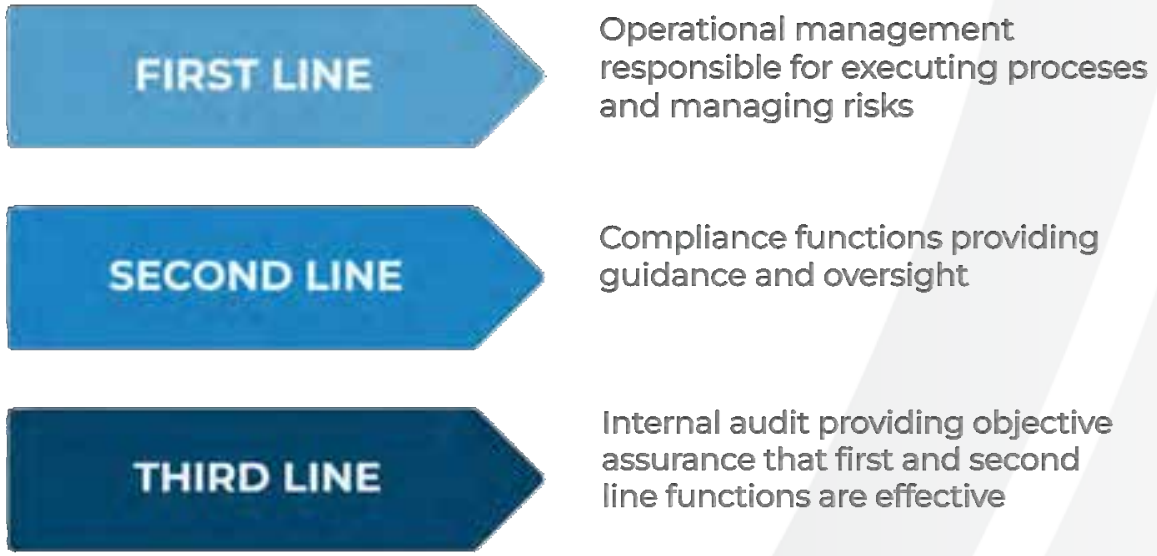
Agenda

- ATC's Approach to Oversight
- Physical Security Program Objective
- Threat and Vulnerability Assessment
- The Physical Security Plan
- Describe the Implementation Components
- Demonstration of Capabilities
- Incident Response Overview

ATC’s Approach to Oversight

- ATC has developed a comprehensive Reliability Standards Compliance program to ensure adherence to NERC standards.
- Documenting and Testing Internal Controls: Our RSIC (Reliability Standards Internal Controls) efforts focus on designing, implementing, and testing controls to prevent or detect risks.
- Periodic Reviews: Regular reviews are conducted to ensure ongoing compliance and continuous improvement.

ATC employs a structured approach to maintain independent oversight through multiple lines of defense.



ATC's Participation in the JMA

- 2025 ATC volunteered for the NERC-led Joint Monitoring Activity (JMA) Pilot
- JMA consisted of 12 regulators collectively across the ERO and FERC

Physical Security Program Objective

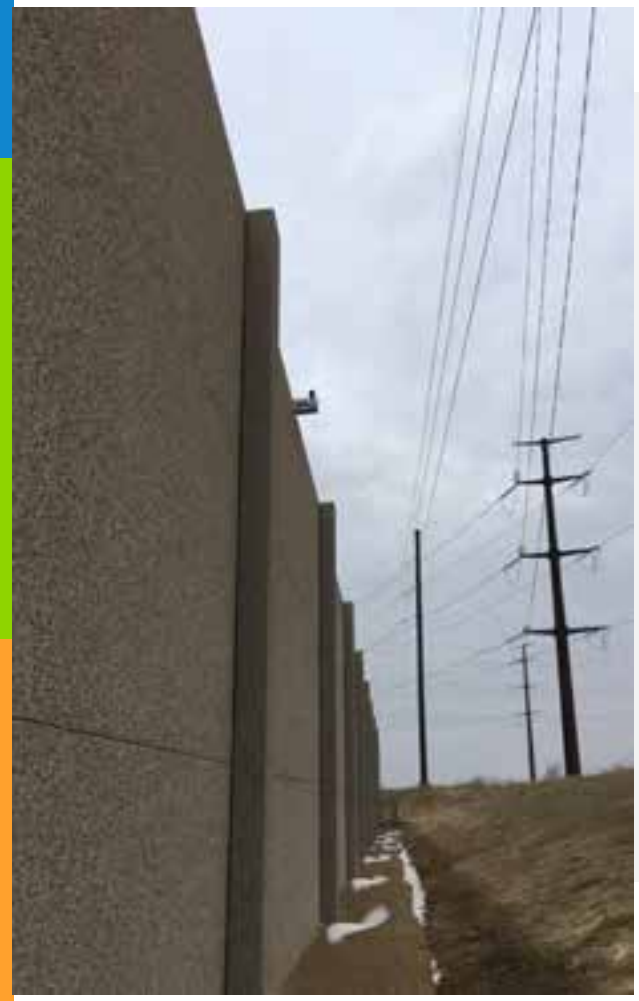
Program Objective

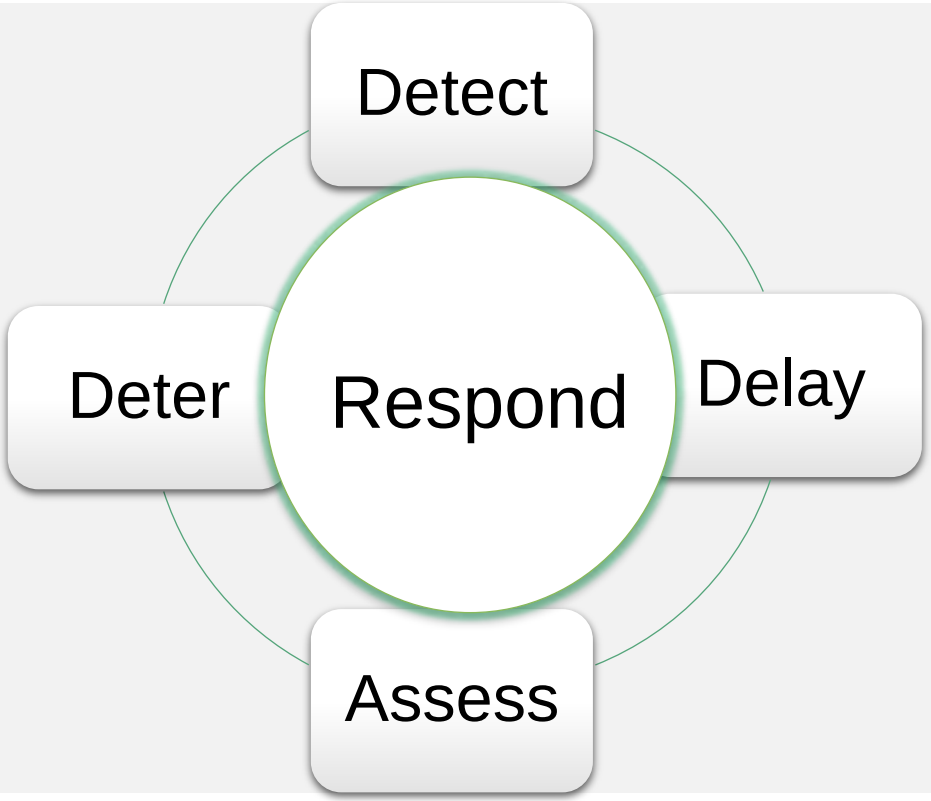
- To protect ATC personnel and assets from potential threats by mitigating identified vulnerabilities.
  - Proactive security management
  - Sound physical security principles

Proactive Security Management

- Internal Intelligence Gathering and Data Analytics
- Monitoring Activities within ATC Footprint
- Information Sharing with Utility Partners
- Subscriptions and Participation with Federal, State, and Local Law Enforcement (e.g., FBI and DHS)
- Participation with Industry Groups (e.g., EEI, NATF and ESAR) and Trade Groups (e.g., American Society for Industrial Security - ASIS)

Sound Physical Security Principles

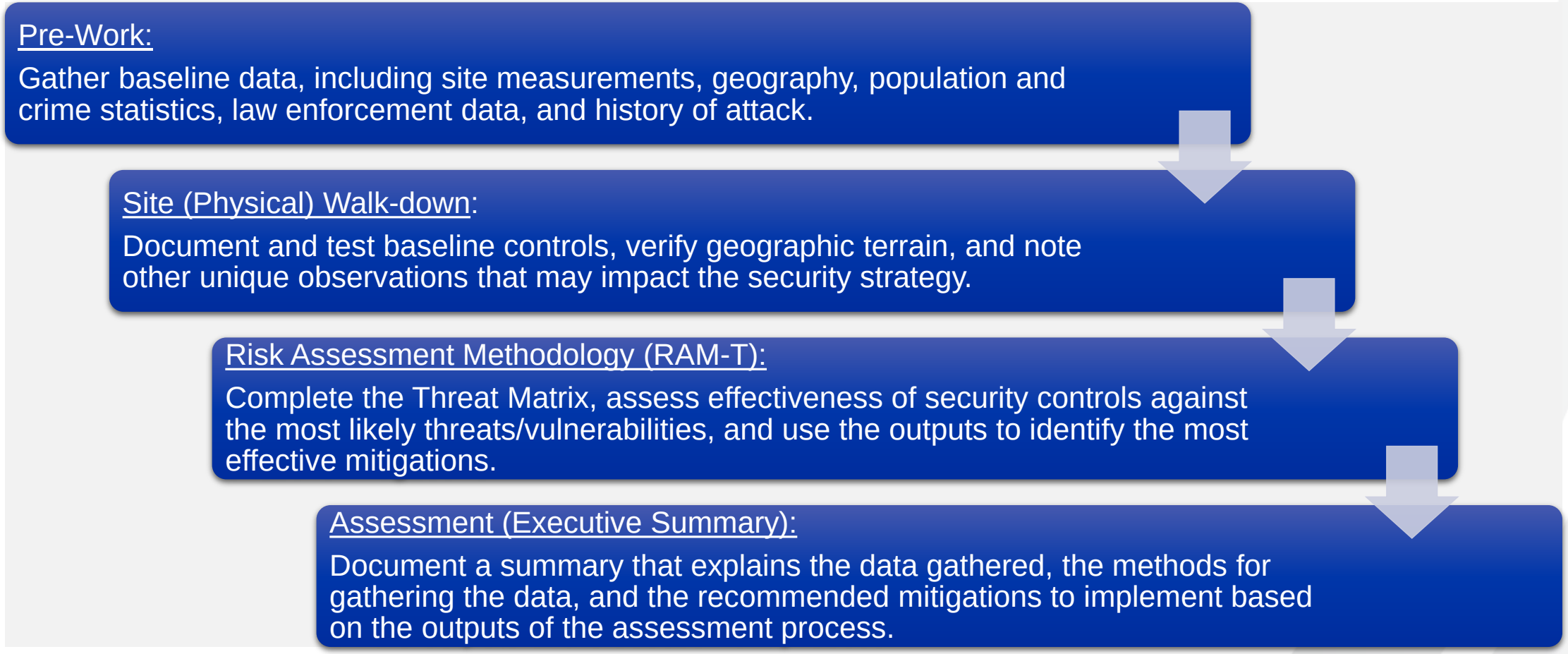




Threat and Vulnerability Assessment

CIP-014-3 R4

Security Assessment Process



Risk Assessment Methodology - Transmission (Ram-T)

Confidential (Red) — ATC Proprietary Information

THREAT ANALYSIS

Undesired Event vs. Likelihood of Attack (P_a) Worksheet Summary

Date: | Recorded by:

Facility Identifier:

Undesired Events	Likelihood of Attack (P_a) By Adversary					
	Domestic Terrorist/Activist	Criminal Activity	Rogue/Lone Wolf	Insider Threat	International Terrorist	
1. Loss of Mission: Damage to yard equipment due to explosion	H	VL	H	VL	L	
2. Loss of Mission - Loss of Control House due to fire in control house	H-	VL	H	VL+	H-	
3. Loss of Mission - Damage to yard equipment due to gunfire	H	L--	H	VL	L+	
4. Loss of Mission - Disruption of Service due to criminal damage (1. Theft, 2. Vandalism, 3. Sabotage)	H-	M-	H-	L--	L++	
5. Loss of Mission - Disruption of service due to insider sabotage	L++	VL	L++	L-	L	

PROTECTION SYSTEM EFFECTIVENESS ANALYSIS — VA-WS-F11.0

Worksheet

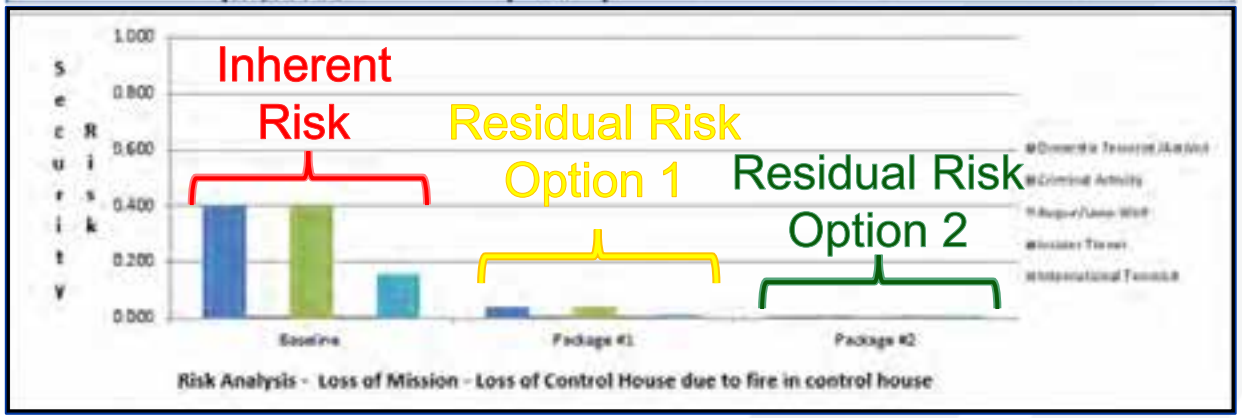
Date: | Recorded by:

Facility Identifier: | Assessment Stage: Security Option 2

Estimated protection system effectiveness, P_E

1. System Features	Offsite	Substation perimeter	Substation yard	Control House	Task	Substation yard	Substation perimeter	Offsite	0		
Detection Effectiveness	H	VH	VH	VH	VH	VH	VH	VH	0	vh	
Delay (s.)	25	45	35	2500	20	35	1300	25	0	3985	sec
Detection Areas Start Effectives (s.)	Detect	Assess / Respond	Monitor	Response	Monitor	Monitor	0	0	Detection	0	sec

A	Detection Effectiveness value (Maximum value)	vh
B	Response/mitigation Effectiveness value	VH
C	Sum of delays (including & after first H or second M for detection) in	3985
D	Response force time in seconds.	755
	Compare C to D	VH



Legend:
H = High
M = Medium
L = Low
V = Very
+ or ++ signify a level above H, M, or L
- or -- signify a level below H, M, or L

Physical Security Plan

CIP-014 R5

The Physical Security Plan

- Enterprise Security Expectations
- Resiliency Plan
- Threats
- Design Basis Threat Evaluation and Mitigation Measures to be Implemented
- Law Enforcement Contact and Coordination
- Implementation Timeline and Provisions for Plan Changes
- Provisions to Evaluate Evolving Physical Threats and Corresponding Mitigations
- Review and approval by responsible leadership

Third-Party Security Plan Review

- Security Plans drafted concurrently with third-party reviewer.
- Information sharing done throughout scoping process.
- Approved Security Plans shared using approved information sharing methods.
- Email communication to reviewer.
- Monitor activities for completion.

Implementation

CIP-014 R5

Implementation Process

- Project Status Meetings
- Monthly Physical Security Assessment Working Group Meetings
- Post Implementation Walk-down

Demonstration of Capabilities

Demonstration of Capabilities: Remote Lighting

Demonstration of Capabilities: One-way Communication

Demonstration of Capabilities: Perimeter Defender

Demonstration of Capabilities: Fusion/Radar Technology

Apparent Attempted Break-in *Why Details Matter*

Subject observed at an active construction site. At first glance, he appears as if he belongs, but what if we look closer?

- No keys.
  - Parked outside of right-of-way (ROW) gate.
  - Walked the entire right-of-way (approx. ¼ mile) up and back.
- No site check-in.
- Lack of proper PPE (FR clothing, Hardhat).
- Carrying a crowbar.
- Left immediately when challenged.

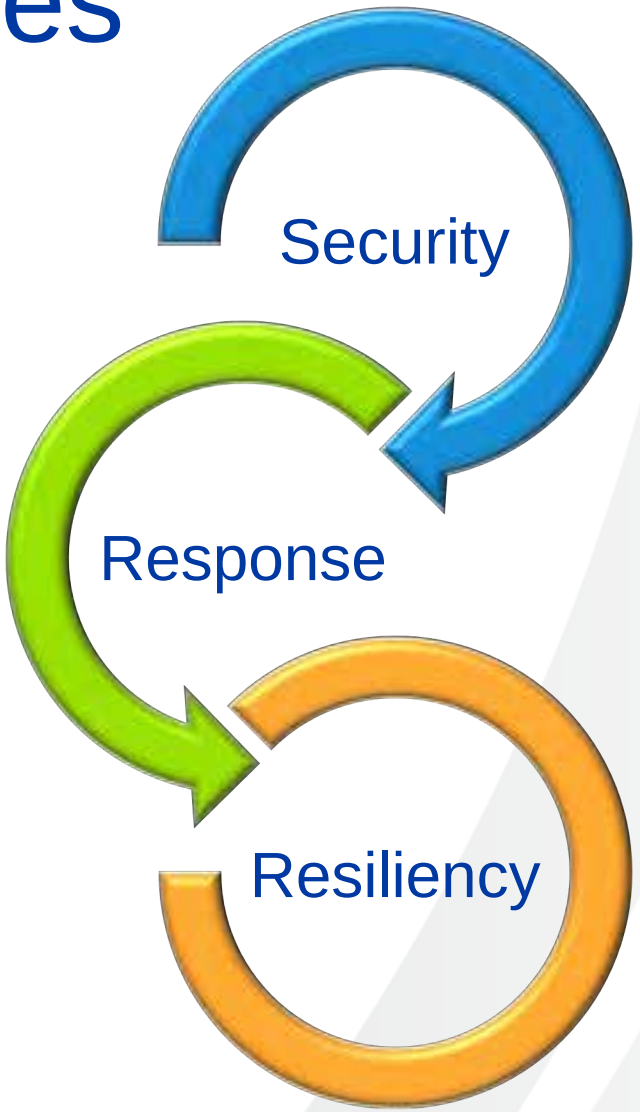
Sometimes things are not what they first appear to be. If something doesn't feel right, report it.

If you See Something, Say Something!

Incident Response Capabilities

Incident Response Capabilities

- Security and Response Culture, Mission, and Vision
- Design
- Capabilities
- Technologies
- Future Capabilities, Investment and Commitment
- Security Culture



Security and Response Culture, Mission and Vision

Culture

Partnering to advance risk transparency, to energize the culture and to execute security, response, and resumption capabilities with excellence.

Stakeholders

- Board of Directors / Owners
- Regulators
- Executive Management
- Functional Areas
- Partners (Internal / External)

Mission

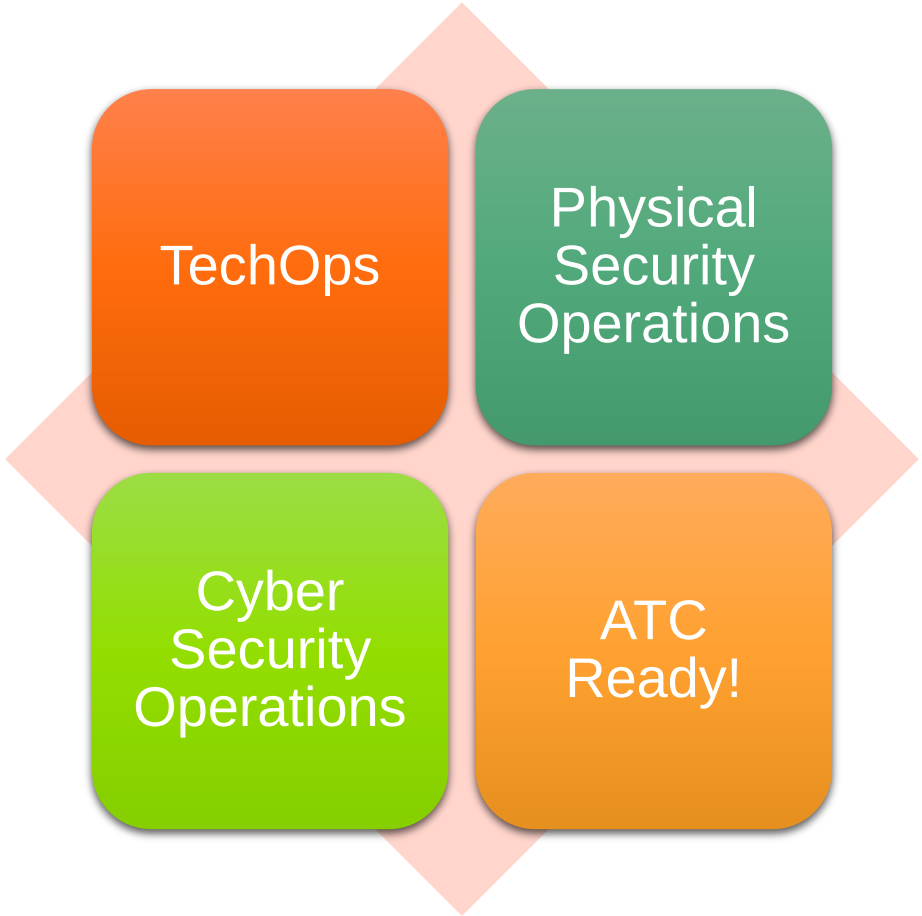
Protect reliable operations and ATC assets (people, information, facilities, and systems) through preparedness, and by mitigating vulnerabilities and threats.

Vision

Prepare ATC to be resilient to business disruption.

- Safeguard people, property, & process.
- Deliver Safe, Secure & Reliable Operations
- Ensure timely/sufficient response & resumption

Mission Assurance Center



- The MAC - Mission Assurance Center
  - Hub for technology reliability, situational awareness, and threat mitigation. The MAC is made up of the ISOC, TechOps and ER.
- The ISOC - Integrated Security Operations Center
  - Fusion of cyber and physical security operations, moving from silos to combined force.
- TechOps – Technology Operations
  - Focuses on monitoring underlying technology stacks (IT/OT) and coordinating responses to unplanned outages and deprecated services.
- ATC Ready! - Emergency Response
  - Ability to drive Incident Command and coordinate response major incidents.

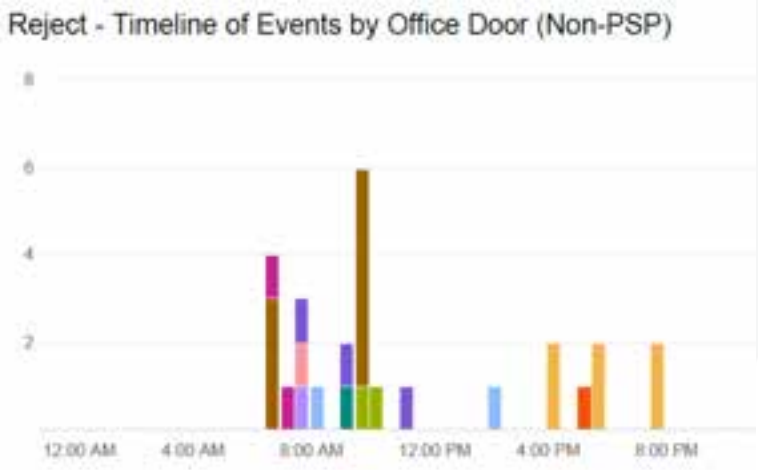
Physical Security Operations Center

- Role as part of the MAC
- ATC operates (2) two Physical Security Operations Centers (PSOC) with 24/7 coverage.

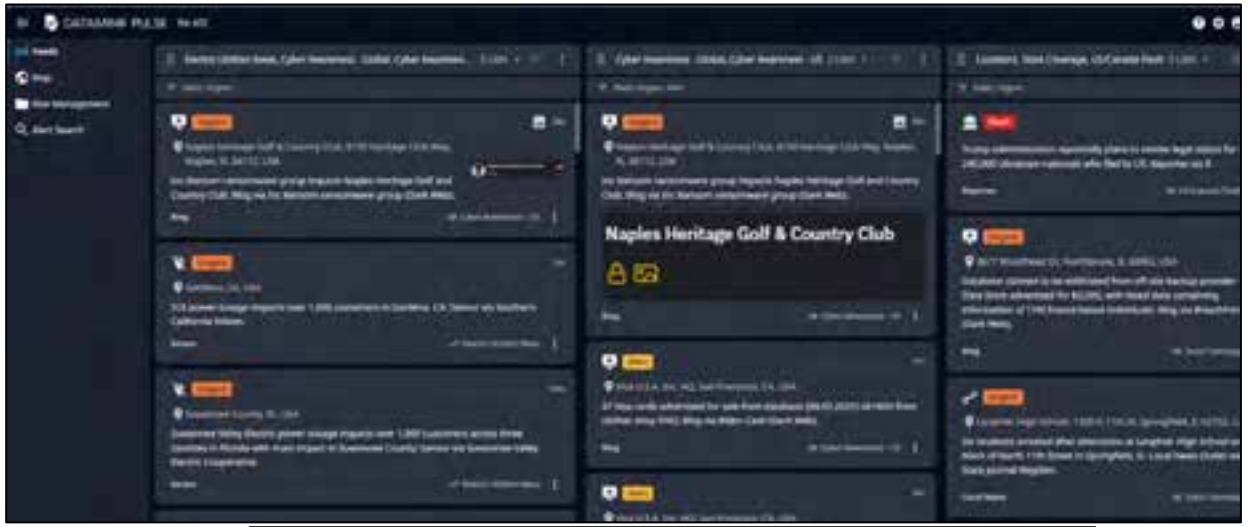
- Duties include:
  - Monitoring for physical security events
  - Incident response
  - Situational awareness
  - Mass notifications
  - Access management

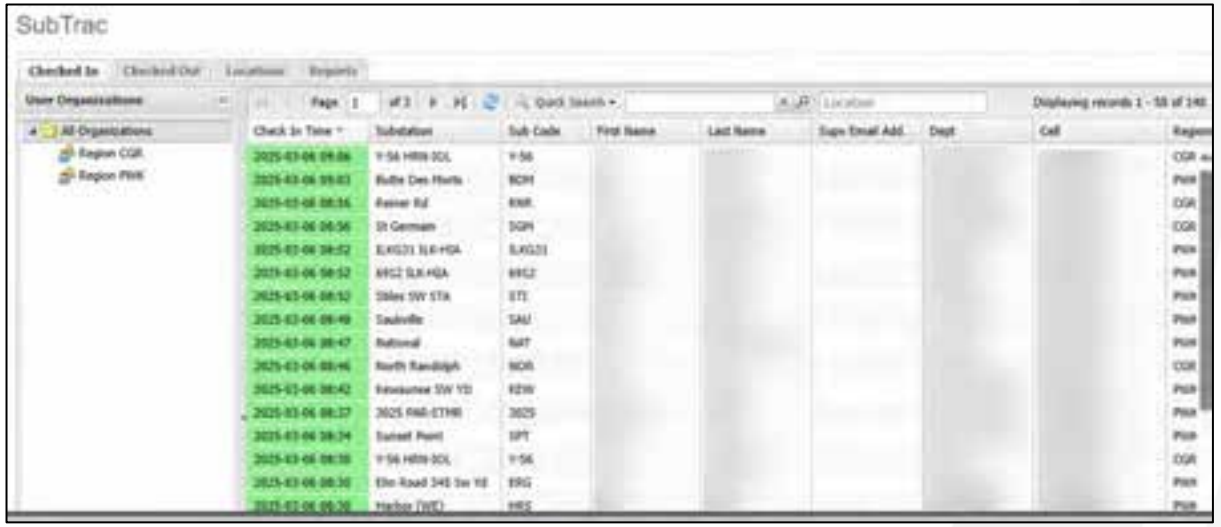
Capabilities

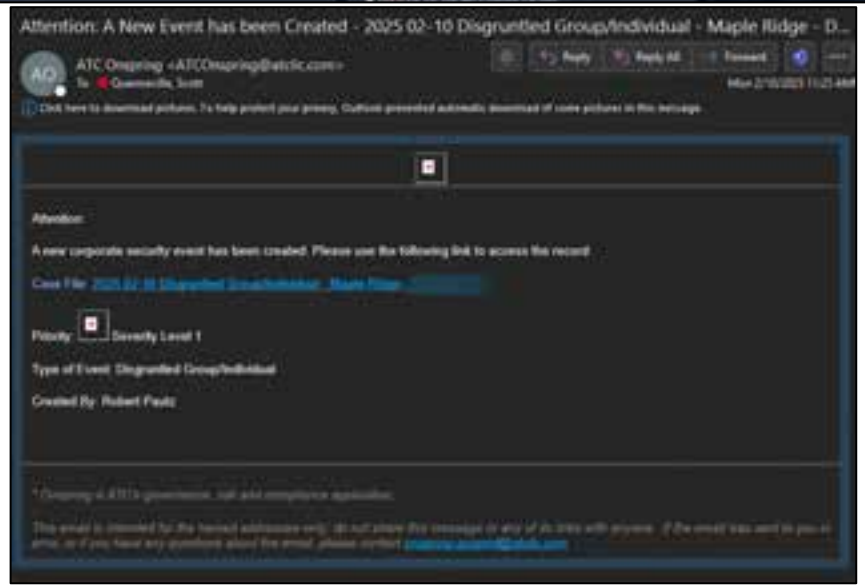
- Access to ~2,500 cameras with nearly 5,000 points of view
  - Fusion
  - Infrared
  - 360
  - Mobile Security Trailers
- Event Analysis Screens for geographic perspective for alerts
- Public Address System
- Mass Notification System
- Access to Substation Check-In Systems
- Direct line communications to state emergency management
- Open-Source Intelligence (OSINT) Monitoring
- Integration with Enterprise Security Information and Event Management (SIEM) System



Technologies

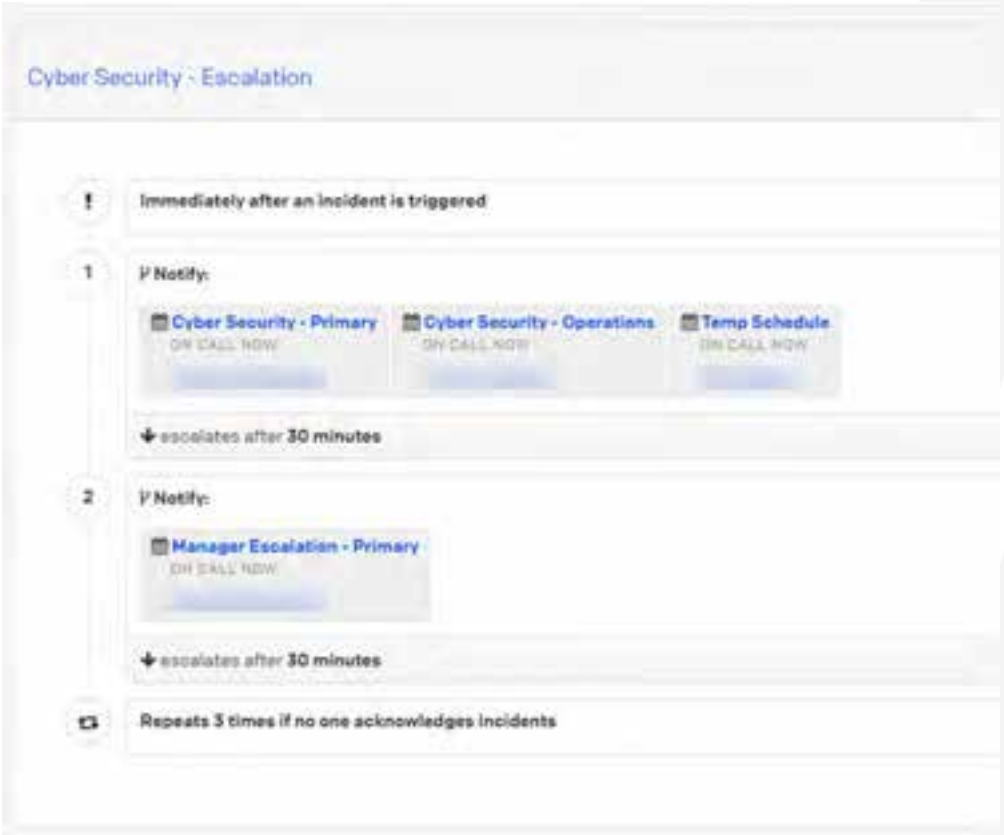






Future Capabilities, Investment, and Commitment

- Automation and fusion event capabilities
- Workflow optimization
- Unified Incident Response
- Common Operating Picture
- Capability Analytics



Security Culture