CONTROLLER HANDBOOK

Scenario 3: "Blackout Friday"

Coordinated Systems Attack — FIDS + PA Hijack + Mass Panic
North Coast International Airport (NCIA)
FACILITATOR / INSTRUCTOR USE ONLY

FACILITATOR DOCUMENT — DO NOT DISTRIBUTE TO PLAYERS

1. EXERCISE OVERVIEW

Duration: 2 Hours

Scope: A coordinated cyberattack on the busiest travel day of the year. A hacktivist exploits an overly-broad firewall rule and a default password to kill FIDS and inject a fake evacuation message through the PA system. Mass panic follows. The exercise tests cyber investigation, crisis management, crowd control, the re-screening dilemma, and communications under extreme pressure.

Exercise Objectives

- **Dual-Crisis Management:** Can the team handle a physical crisis (stampede, injuries, re-screening) AND a cyber investigation simultaneously?
- **Network Segmentation:** Can IT trace the attack from Guest WiFi → PA controller → FIDS server? Do they find Rule 49 and the default credentials?
- **The Re-Screening Decision:** The exercise's hardest call. No right answer — but the team must make a defensible choice and own the consequences.
- **Crisis Communications:** Can PIO manage the narrative when passenger video is going viral, the hacktivists are posting proof, and CNN is calling?
- **OT Security:** The PA system is operational technology that was treated like IT infrastructure. Default vendor credentials, no monitoring, no alerting. Does the team recognize this as systemic?

2. THE PUZZLE — SOLUTION MAP

#	Clue	What It Reveals	Source
1	PA message was not authorized by AOC	Someone injected the message externally. There may be no real threat.	I-01
2	FIDS was killed via management console, not crashed	Deliberate attack, not hardware failure. Attacker had network access to FIDS.	I-05
3	FIDS console was accessed from 10.1.50.10 (PA controller)	Attacks are connected. PA controller was the pivot point.	I-05
4	PA controller was accessed from 10.1.70.47 (Guest WiFi)	Attacker is on public WiFi. Inside the terminal.	I-06
5	Firewall Rule 49: VLAN 70 → VLAN 50:443 = ALLOW	Guest WiFi can reach the PA controller. The network isn't isolated.	I-06 / Ref Card
6	PA controller password is the vendor default	No authentication barrier. Anyone who finds the interface can log in.	I-06

7	CCTV shows suspect in food court with laptop	Physical identification. Suspect is at Gate A-14.	I-08
8	Chaos Collective claims credit on social media	Hacktivist motivation confirmed. No real security threat. Attack was for exposure.	I-09

3. FACILITATOR NOTES

Managing the Physical Crisis

The first 20 minutes should feel chaotic. TSA is yelling for answers. Airlines are threatening cancellations. Social media is exploding. Passengers are hurt. Do NOT let the IT investigation overshadow the physical response — if Ops ignores the crowd management while IT chases network logs, push back: "There are 6,200 passengers outside your terminal on the busiest travel day of the year. What are you doing about THEM?"

The Re-Screening Debate

This is the exercise's emotional core. Some students will insist on full re-screening (safety first). Others will argue that re-screening 4,000 passengers will cancel Thanksgiving for thousands. Both sides have merit. Push BOTH: "So you'd cancel 14 flights and ruin Thanksgiving for 4,000 families because a college student played a prank?" AND "So you'd skip re-screening on the busiest travel day and bet your career that nobody slipped something through those 5 open emergency doors?"

The best answer is partial re-screening: use CCTV to identify passengers who exited through the 5 specific emergency doors, re-screen them individually, and implement enhanced random screening for all passengers re-entering the sterile area. This balances security with operational reality.

The 8-Minute Window

FIDS died at 2:47. PA fired at 2:55. That's 8 minutes. During those 8 minutes, did anyone consider that the FIDS crash might be deliberate? If they had, could they have locked down the PA system before the evacuation message? This is a powerful post-exercise discussion point about cascading attacks and response speed.

4. EVALUATION RUBRIC

Metric	Criteria
Metric 1: Crisis Management (30 pts)	**Fail:** Team focused on investigation while ignoring passengers, injuries, and airlines. **Pass:** Ops managed crowd control and airline communication while IT investigated. **Excellence:** Immediate PA counter-message, crowd control at emergency exits, injury response, airline liaison within 10 minutes, shelter-in-place decision.
Metric 2: Cyber Investigation (25 pts)	**Fail:** IT never traced the attack chain. Never found Rule 49 or the default password. **Pass:** IT traced FIDS to PA controller. Found the Guest WiFi connection. **Excellence:** IT mapped the full chain (WiFi → Rule 49 → PA default creds → pivot to FIDS), identified the suspect via CCTV, and immediately changed the PA password to prevent Phase 3.
Metric 3: Re-Screening Decision (25 pts)	**Fail:** Team never made a decision. Or made a decision they couldn't defend. **Pass:** Team made a clear decision (full, partial, or waive) and could articulate why. **Excellence:** Team developed a risk-based partial re-screening plan using CCTV to identify specific passengers, communicated the plan to TSA, airlines, and passengers, and documented the rationale for the record.

Metric 4: Communications & Remediation (20 pts)	**Fail:** PIO said "cyberattack" too early, gave "no comment," or was absent. **Pass:** PIO issued a holding statement and updated as facts emerged. **Excellence:** PIO controlled the narrative, provided accurate updates, managed the hacktivist claim proactively, and the team produced a remediation plan covering Rule 49 deletion, credential rotation, FIDS hardening, and PA system monitoring.

5. HOT WASH GUIDE

• **The $9 Attack:** "A latte and public WiFi. That's what it cost to evacuate your airport. What's the ROI on changing one default password?"

• **Rule 49:** "A firewall rule added 6 months ago during a WiFi upgrade. Did anyone review it? Did anyone test Guest WiFi isolation after the change? How many other rules are sitting in your firewall right now that you've never audited?"

• **OT vs. IT:** "The PA system is operational technology. Who owns it? IT? Facilities? The AV vendor? If nobody owns it, nobody patches it, nobody changes the password, and nobody monitors it."

• **The PA Trust Problem:** "Now that the PA system has been used as a weapon, will passengers trust it? If there's a REAL emergency tomorrow, will people evacuate when the PA tells them to — or will they assume it's another hack?"

• **The 8-Minute Window:** "Could you have prevented the PA attack if you'd recognized the FIDS crash as deliberate within those 8 minutes? What would that response look like?"

• **Re-Screening:** "What did you decide? What would the headline be? 'Airport Cancels Thanksgiving for Thousands Over Prank' vs. 'Airport Skips Security Screening After Cyberattack.' Which do you prefer?"

END OF CONTROLLER HANDBOOK