SCENARIO 3: "BLACKOUT FRIDAY"

Coordinated Systems Attack & Mass Panic Response

North Coast International Airport (NCIA)
Tabletop Exercise — Player Briefing Packet
Exercise Duration: 2 Hours
EXERCISE — FOR TRAINING USE ONLY

EXERCISE — EXERCISE — EXERCISE

1. SITUATION BRIEF

It is **2:47 PM on the Wednesday before Thanksgiving** — the single busiest travel day of the year at North Coast International Airport. The terminal is at **142% of normal capacity**. There are approximately **6,200 passengers** in the building right now, plus 1,400 airport and tenant employees. 14 departures are scheduled between now and 6:00 PM. The TSA checkpoint queue is 35 minutes deep. Every seat at every gate is taken. The food court is standing room only.

At 2:47 PM, every Flight Information Display System (FIDS) screen in the airport goes black. Simultaneously. All 38 displays — concourses, ticketing, baggage claim, the food court, curbside — **dead**. Passengers look up from their phones. Gate agents notice. The main departures board behind the ticket counters: blank.

The AOC receives the FIDS server alarm. IT is notified. Everyone assumes it's a system crash — annoying on the busiest day of the year, but manageable. Gate agents begin making verbal announcements. The AOC starts preparing manual flight boards.

Then, at 2:55 PM — eight minutes after the FIDS crash — the airport PA system broadcasts the following message:

```
"ATTENTION ALL PASSENGERS AND PERSONNEL. THIS IS AN EMERGENCY EVACUATION
NOTICE. A SECURITY THREAT HAS BEEN IDENTIFIED IN THE TERMINAL. ALL PERSONS
MUST EVACUATE THE BUILDING IMMEDIATELY THROUGH THE NEAREST EXIT. DO NOT
STOP TO COLLECT PERSONAL BELONGINGS. THIS IS NOT A DRILL. REPEAT — THIS IS
NOT A DRILL."
```

The message plays once. Then silence. No follow-up. No all-clear. No one in the AOC authorized it. No one at the TSA checkpoint triggered it. **No one knows where it came from.**

The result is immediate. 6,200 passengers — already stressed, already crowded, already on edge because it's the day before Thanksgiving — hear "SECURITY THREAT" and "EVACUATE" and they **move**. The food court empties in 90 seconds. Gate areas flood toward exits. Passengers in the sterile area push through emergency doors, triggering alarms. People inside the TSA checkpoint queue try to reverse direction — directly into the stream of passengers still entering. A mother drops a stroller on the escalator. Someone falls near Gate B-7. Three passengers have anxiety attacks.

Within four minutes, approximately **4,000 passengers have exited the sterile area** through emergency exits, bypassing security screening. The remaining 2,200 are in various states of confusion — some evacuating, some frozen in place, some ignoring the announcement because no follow-up came. **Sterile area integrity is compromised.**

YOUR MISSION: Determine if there is a real security threat. Manage the mass panic. Decide whether to re-screen thousands of passengers on the busiest travel day of the year. Find out who hijacked the PA system — and how. And figure out if the FIDS crash and the PA message are connected.

System	Status at 2:58 PM	Impact
FIDS (All 38 Displays)	DOWN — All screens black since 2:47 PM	No flight info anywhere in the terminal. Passengers have no gate/time data.
PA System	OPERATIONAL — but unauthorized message broadcast at 2:55 PM	Unauthorized evacuation announcement triggered mass panic.
Sterile Area Integrity	COMPROMISED — ~4,000 passengers exited through emergency doors	Passengers bypassed security. Re-screening may be required.
TSA Checkpoint	CHAOS — Counterflow of passengers entering/exiting. Two injuries reported.	Checkpoint effectively shut down. TSA requesting guidance.
Concessions / Retail	ABANDONED — Tenants evacuated with passengers	Cash registers open, merchandise unattended, some stores unsecured.
PACS / CCTV	NORMAL — All cameras recording, all doors responding	Emergency exit door alarms active (multiple doors tripped).
AODB / Email / Phones	NORMAL	Core ops systems unaffected.

2. TEAM ASSIGNMENTS

TEAM A: OPERATIONS & COMMAND (IC)	
Situation: You have 6,200 passengers in varying stages of panic. 4,000 have left the sterile area. 14 flights are waiting to board or depart. TSA checkpoint is non-functional. Gate agents are overwhelmed. You need to regain control of the terminal — NOW.	**Standing Orders:** Immediate: PA counter-message (if you trust the PA system). Establish crowd control. Decision: Do you continue the evacuation or issue a shelter-in-place? Decision: Re-screening — yes or no? (This is the hardest call in the exercise.)

TEAM B: IT & CYBERSECURITY	
Situation: Two systems failed within 8 minutes: FIDS and PA. Coincidence doesn't produce this pattern. You need to determine: Is this a cyberattack? If so, how did they get to both FIDS AND the PA system? What else can they reach? Is there a third phase coming?	**Standing Orders:** Investigate: FIDS server — crash or kill? Check logs, processes, management interface. Investigate: PA system — who sent that message? From where? What device? Assess: Are these attacks connected? Same source? Same vulnerability?

TEAM C: TSA & SECURITY	
Situation: Sterile area integrity is gone. 4,000 passengers exited unscreened doors. Any one of them could re-enter carrying a prohibited item. Federal regulations may require full re-screening before operations resume. On the day before Thanksgiving.	**Standing Orders:** Immediate: Secure emergency exits. Stop further unscreened egress. Assess: Is there an actual security threat? (Is the PA message real or fake?) Decision: Re-screening protocol — full, partial, or risk-acceptance?

TEAM D: PIO, LEGAL & AIRLINE OPS	
Situation: Social media is already on fire. Passengers are posting videos of the stampede. #NCIAevacuation is trending. Airlines want to know if they're boarding or not. National media will have this in 20 minutes.	**Standing Orders:** Draft: Immediate statement (what happened, what we're doing, are passengers safe). Coordinate: Airlines need a boarding/delay decision within 15 minutes. Prepare: If re-screening is ordered, that's a 2-3 hour delay for 4,000+ passengers. On Thanksgiving Eve. Communicate that.

3. THE RE-SCREENING QUESTION

This is the central decision of the exercise. Once sterile area integrity is lost, federal security regulations strongly indicate that all passengers must be re-screened before boarding. But consider the math:

Factor	Full Re-Screen	Partial / Risk-Based	No Re-Screen
Passengers Affected	~4,000 who exited + ~2,200 still in terminal = all	~4,000 who exited sterile area only	None. Resume operations.
Time Required	2.5 - 3 hours at full checkpoint throughput	1.5 - 2 hours (reduced population)	0 — immediate resumption

Flights Affected	All 14 remaining departures delayed or cancelled	6-8 departures delayed significantly	Minimal additional delay
Passenger Impact	Thousands miss Thanksgiving travel. Cascade to connecting flights nationwide.	Significant but contained delays	Minimal — but if something gets through...
Security Risk	LOW — full screening restores integrity	MODERATE — assumes those who stayed are clean	HIGH — sterile area was fully compromised
Legal Exposure	LOW — followed protocol	MODERATE — defensible if risk-based	EXTREME — if anything happens, you chose not to screen

There is no right answer. Full re-screening is the safest choice — and it will ruin Thanksgiving travel for thousands. No re-screening is the fastest — and it puts you one incident away from a career-ending investigation. Your job is to make a defensible decision and own it.

4. RULES OF ENGAGEMENT

- **"This is an Exercise":** Begin and end all simulated communications with this phrase.
- **Real-World Emergencies:** Use **"REAL WORLD — REAL WORLD"** to halt the exercise.
- **Two Simultaneous Crises:** You are managing a physical crisis (mass panic, re-screening) AND investigating a cyber incident (FIDS + PA) at the same time. Both require attention. Neither waits.
- **Time Pressure Is Real:** Every minute without a decision costs operations. Airlines are waiting. TSA is waiting. 6,200 passengers are waiting. Decide, communicate, act.
- **Is There a Third Attack?** FIDS was Phase 1. The PA was Phase 2. Is there a Phase 3? You don't know. You need to find out before it happens.

5. INVESTIGATION TRACKER

Question	Your Finding
1. Was the PA message authorized?	
2. Where did the PA message originate? (AOC console, IP endpoint, or other?)	
3. What caused the FIDS crash? (Hardware, software, or deliberate?)	
4. Are the FIDS crash and PA message connected?	
5. How did the attacker reach these systems?	
6. Is there a real security threat requiring evacuation?	
7. What other systems can the attacker reach?	
8. Who did this — and why?	

EXERCISE — EXERCISE — EXERCISE