MASTER INJECT DECK

Scenario 3: "Blackout Friday"

North Coast International Airport (NCIA)

Print and cut. Deliver at times indicated in the MSEL.

CONTROLLER DOCUMENT — NOT FOR PLAYER DISTRIBUTION (until delivered)

CONTROLLER DOCUMENT

INJECT I-01 Phase 1 — 0:10

THE PA WAS NOT AUTHORIZED

FROM: AOC Console Operator

TO: Operations / Security (Teams A & C)

DELIVERY: Phone Call — Facilitator uses a confused, alarmed tone

CONTENT (Read aloud or hand to players):

"This is the AOC. We need to tell you something. That PA message — the evacuation announcement — it did NOT come from us. Nobody in this room touched the PA console. Nobody authorized it. We checked every operator on shift. We checked the log on our physical console. Nothing. The PA system has a web admin interface — it's IP-based, installed about 18 months ago. Someone could have triggered the message through that web interface. But we don't have access to those logs from here. IT needs to check the PA controller. So to be clear: whatever that message was, it didn't come from airport operations. We do NOT have a confirmed security threat. We do NOT have any reason to believe there is an actual emergency. Someone sent that message without authorization. But we now have 4,000 people standing in the parking lot who think there's a bomb."

■ CONTROLLER NOTE (DO NOT READ TO PLAYERS):

This is the first critical clue: the evacuation was unauthorized. The team now knows there may be no real threat — but they can't assume that. The challenge: do you treat an unconfirmed threat as real or false? Until you KNOW it's fake, you have to assume it could be real. If the team immediately says 'false alarm, bring everyone back in' — push back: "You don't know that yet. All you know is the AOC didn't send it. Maybe someone else with access to the PA web interface sent it for a real reason."

INJECT I-02 Phase 1 — 0:15

TSA WANTS ANSWERS — NOW

FROM: TSA Federal Security Director

TO: Operations / Security (Teams A & C)

DELIVERY: Phone Call — Facilitator uses an urgent, command-level tone

CONTENT (Read aloud or hand to players):

"This is the FSD. My checkpoint is shut down. I've got counterflow — passengers trying to exit through the checkpoint while others are trying to enter. Two people fell. One has a possible broken wrist. I've pulled all my officers to crowd control. Here's my situation: five emergency exit doors were breached by passengers — A-6, A-8, A-12, B-3, and B-7. Those doors bypass screening. That means approximately 4,000 passengers left the sterile area through unscreened exits. Sterile area integrity is compromised. I need to know two things, and I need to know them fast: 1. Is there a REAL security threat? Because if there is, I'm calling for VIPR teams and a full ground stop. 2. If there ISN'T a real threat, I need to start the re-screening conversation. You understand what that means on the day before Thanksgiving."

■ **CONTROLLER NOTE (DO NOT READ TO PLAYERS):**

The FSD is asking for a binary answer: real threat or not? The team doesn't have that answer yet. The correct response right now is: 'Unconfirmed. We believe the PA message was unauthorized. We are investigating. Treat as a security event pending investigation.' Note the five specific doors: A-6, A-8, A-12, B-3, B-7. These become important later — CCTV at these doors can identify which specific passengers exited, enabling targeted (partial) re-screening.

INJECT I-03 Phase 1 — 0:22

SOCIAL MEDIA EXPLOSION

FROM: Social Media Monitor

TO: PIO (Team D)

DELIVERY: Printed report / read aloud

CONTENT (Read aloud or hand to players):

Social Media Monitoring Report — 3:10 PM:

• Passenger video of stampede near Gate B-7 posted to TikTok — **47,000 views** in 8 minutes and climbing
• #NCIAevacuation trending in local market, approaching national trend
• @NCIAirport account has 340+ DMs asking what's happening
• Passenger tweet (14K likes): "People are HURT at NCIA. A woman fell on the escalator. A kid was crying. NO ONE from the airport told us what was happening. Just a terrifying announcement and then NOTHING."
• Local TV (WNCI) has dispatched a crew — ETA 12 minutes
• CNN travel desk has called the airport media line
• One passenger: "My mom just called me crying. She saw the video. She thinks I'm in a terrorist attack. NCIA SAY SOMETHING."

■ **CONTROLLER NOTE (DO NOT READ TO PLAYERS):**

PIO must respond NOW. Every minute of silence makes it worse. The ideal statement at this point: 'NCIA is responding to a PA system malfunction that caused an unauthorized evacuation message. There is no confirmed security threat. Operations staff and TSA are working to restore normal operations. Passengers should follow instructions from airport and airline personnel.' 'Malfunction' is the right word — it's accurate (the PA was used in an unauthorized way) and it doesn't say 'cyberattack' prematurely.

INJECT I-04 Phase 1 — 0:28

THE AIRLINES ARE DONE WAITING

FROM: Airline Station Managers (Delta, United, American)

TO: Operations / PIO (Teams A & D)

DELIVERY: Three simultaneous phone calls — use multiple facilitators if available

CONTENT (Read aloud or hand to players):

Delta: "I have 3 departures in the next 2 hours. My passengers are in a parking lot. Do I board or not? If I don't get a decision in 10 minutes, I'm cancelling DL 1247 to Atlanta." **United:** "Same situation. 4 departures. My crew is timing out on UA 892 — if we don't board in 45 minutes, that flight is cancelled and there's no replacement crew. 350 passengers miss Thanksgiving. Your call." **American:** "I've already got passengers rebooking on their phones. Every minute we stand here costs me load factor. I need a timeline: when are we re-entering the terminal?"

■ **CONTROLLER NOTE (DO NOT READ TO PLAYERS):**

This forces the re-screening decision. If re-screening is ordered, the airlines can't board for 2-3 hours. Cancellations are inevitable. If no re-screening, they can start re-boarding in 15-20 minutes. Push the team: 'The airlines are making their own decisions in 10 minutes. If you don't give them a timeline, they'll cancel flights independently and blame you publicly.'

INJECT I-05 Phase 2 — 0:35

FIDS WAS MURDERED, NOT CRASHED

FROM: IT Analysis

TO: All Teams

DELIVERY: IT presents findings — urgent but technical

CONTENT (Read aloud or hand to players):

"We've been on the FIDS server. It didn't crash — someone killed it deliberately. The FIDS management console (web interface, port 8080) shows a session that logged in at 2:46 PM and executed two commands: service stop and display cache clear. One minute later, all 38 screens went black. Here's the key: the management console access log shows the session came from **IP address 10.1.50.10**. That's not an admin workstation. That's the PA controller — the Cisco UCM that runs our PA system. Someone accessed the FIDS management console FROM the PA controller. That means whoever hijacked the PA also killed the FIDS. These aren't two separate incidents. They're one coordinated attack, and the PA controller was the attacker's pivot point."

■ **CONTROLLER NOTE (DO NOT READ TO PLAYERS):**

Two revelations: (1) FIDS was deliberate, not a crash. (2) Both attacks came through the PA controller. The team should now focus on: how did the attacker reach the PA controller? That's the next domino. If IT jumps straight to 'check the PA controller logs' — reward that. If they're still processing, give them a moment.

INJECT I-06 Phase 2 — 0:42

THE GUEST WIFI + THE DEFAULT PASSWORD

FROM: IT Analysis

TO: All Teams

DELIVERY: IT presents — this is the AHA moment. Deliver with weight.

CONTENT (Read aloud or hand to players):

"We pulled the PA controller audit logs. Someone logged into the web admin interface at 2:44 PM. The source IP: **10.1.70.47**. That IP is on VLAN 70. Guest WiFi. Public passenger WiFi. A device on our GUEST WIFI accessed the PA system admin interface. We checked the firewall rules. Rule 49 — added 6 months ago during the WiFi upgrade — allows VLAN 70 to reach VLAN 50 on port 443. It was supposed to be a narrow rule for the captive portal authentication flow. But it's overly broad: it lets Guest WiFi reach ANYTHING on VLAN 50 over HTTPS. The PA controller's admin interface is on VLAN 50, port 443." (Pause.) "And the login credentials? We called Convergent AV Solutions — the vendor that installed it 18 months ago. The admin password is the vendor default: **admin / Converg3nt!**. It's in their publicly-available installation guide. PDF on their website. The password was never changed after deployment." (Long pause.) "So to summarize: someone sitting in our terminal on public WiFi logged into our PA system using a password they found in a Google search, broadcast a fake evacuation, and then used the same PA controller to kill our flight information displays. The entire attack cost them nothing."

■ **CONTROLLER NOTE (DO NOT READ TO PLAYERS):**

THIS IS THE ANSWER. Let it land. The attack chain: Guest WiFi → Rule 49 → PA controller (default creds) → pivot to FIDS (VLAN 50 → VLAN 10 permitted). Two failures: one firewall rule and one unchanged password. The room should be a mix of anger, disbelief, and dark humor. Someone will inevitably say 'you've got to be kidding me.' Let them react. Then ask: 'The attacker is still on your WiFi. What do you do NOW?'

INJECT I-07 Phase 2 — 0:50

THE ATTACKER IS STILL CONNECTED

FROM: IT / Facilitator

TO: All Teams

DELIVERY: Facilitator presents options

CONTENT (Read aloud or hand to players):

"The device at 10.1.70.47 is still connected to the Guest WiFi. The wireless controller shows it associated with AP-A-FC3 — that's the access point in the Concourse A food court. **Option A — Kill & Block:** Disconnect the WiFi session. Blackhole the MAC address. Attacker loses access immediately. But we lose the forensic trail and the attacker knows we found them. **Option B — Monitor & Isolate:** Redirect the session to a sandbox. The attacker thinks they're still connected, but they can't reach anything real. We capture any additional activity. **Option C — Physical Approach:** Use CCTV to identify the device owner. Coordinate with law enforcement for a physical approach in the food court. Takes 15-20 minutes." **Separate question:** Do you change the PA controller password RIGHT NOW to prevent a second PA broadcast? Or do you leave it to preserve the forensic state?

■ CONTROLLER NOTE (DO NOT READ TO PLAYERS):

PA password change is URGENT — if the attacker still has access, they could send another message. Change the password immediately. This is more important than forensic preservation. For the WiFi response: C is ideal but requires LEO coordination. In the meantime, Option B buys time. Option A is the panic button. Best combined answer: change PA password now, isolate WiFi session (B), initiate CCTV review for physical approach (C).

INJECT I-08 Phase 2 — 1:00

WE HAVE A FACE

FROM: CCTV / Security / Law Enforcement

TO: All Teams

DELIVERY: Printed CCTV capture / verbal description

CONTENT (Read aloud or hand to players):

CCTV review of the Concourse A food court, focused on the area served by AP-A-FC3: A male, mid-20s, seated at a high-top table near the west wall. He has a laptop open (silver, appears to be a MacBook). He's been seated since approximately 2:30 PM. At 2:44 PM (matching the PA controller login time), he's typing actively. At 2:55 PM (when the PA message plays), everyone around him stands up and starts moving. He closes his laptop. Puts it in a backpack. He does NOT appear alarmed. He picks up his coffee. He walks — not runs — toward Gate A-14. Gate A-14 is the 5:30 PM departure to Atlanta (DL 1247). He is currently sitting in the gate area. He appears calm. He has a boarding pass. Airport police and an FBI agent from the local field office are on site. They're ready to approach on your authority.

■ **CONTROLLER NOTE (DO NOT READ TO PLAYERS):**

The suspect is identified. Decision: approach now or observe? The team should approach — the laptop is critical evidence and delay risks the suspect boarding the flight or destroying evidence. The detail about his calm demeanor while everyone panics should feel damning. He triggered the panic and then walked to his gate with his coffee.

INJECT I-09 Phase 3 — 1:05

CHAOS COLLECTIVE CLAIMS CREDIT

FROM: Social Media

TO: PIO / All Teams

DELIVERY: Printed social media post

CONTENT (Read aloud or hand to players):

Posted simultaneously to X (Twitter) and Reddit by @ChaosCollective: *"We just evacuated @NCIAirport from the food court WiFi. One firewall rule. One default password. 6,000 people running. Your infrastructure is a joke. Fix it before someone with worse intentions finds the same holes we did. Proof attached: PA controller admin panel screenshot (timestamp: 2:44 PM). #BlackoutFriday #AirportSecurity #ChaosCollective"* The post includes a screenshot of the PA controller login page with the admin username visible and a timestamp. It has 200,000+ impressions and climbing. Major news outlets are picking it up. CNN, Fox News, and AP have all shared the post. The screenshot confirms the attack method. The hashtag is now national news.

■ CONTROLLER NOTE (DO NOT READ TO PLAYERS):

This changes everything: 1. It's now a confirmed cyberattack — PIO must update all communications. 2. It confirms there was NO real security threat — the evacuation was manufactured. 3. The hacktivists just broadcast the vulnerability to the ENTIRE WORLD. Other attackers now know Rule 49 exists and the PA uses default creds. 4. Does knowing there's no real threat change the re-screening decision? Push PIO: 'The word "malfunction" is no longer accurate. You need to acknowledge this was a cybersecurity incident. How do you frame it?'

INJECT I-10 Phase 3 — 1:15

THE RE-SCREENING DECISION

FROM: Facilitator

TO: All Teams

DELIVERY: Facilitator forces the call

CONTENT (Read aloud or hand to players):

"It's decision time. Here's where you stand: • The PA evacuation was fake — triggered by a hacktivist on your Guest WiFi. • There is no confirmed security threat. • BUT: 4,000 passengers exited through 5 emergency doors, bypassing screening. • Sterile area integrity is compromised. • TSA policy: compromised sterile area = re-screen. • It's the day before Thanksgiving. • Re-screening 4,000 people takes 2.5 hours. • 14 flights will be affected. Many will be cancelled. • You have CCTV at all 5 emergency exit doors. You can identify who exited. What do you do? **Full re-screen:** All 4,000+ passengers. 2.5 hours. Flights cancelled. Safe. **Targeted re-screen:** Use CCTV to ID passengers who exited the 5 doors. Re-screen only them. Enhanced random screening for everyone else. 45-60 minutes. **No re-screen:** Resume operations. Accept the risk. Fastest option. Make the call. Defend it."

■ **CONTROLLER NOTE (DO NOT READ TO PLAYERS):**

Let the room debate. This is the exercise's hardest moment. Push full-rescreeners: 'You're cancelling Thanksgiving for thousands because of a college student with a laptop.' Push no-rescreeners: 'Someone walks back in with a knife and you chose speed over safety.' Push targeted-rescreeners: 'Can CCTV really identify 4,000 faces? What's your error rate?' Targeted re-screening is the best answer — it's risk-based, defensible, and operationally feasible. But any answer that's articulated and defended earns credit.

INJECT I-11 Phase 3 — 1:25

ROOT CAUSE & REMEDIATION

FROM: Facilitator

TO: All Teams

DELIVERY: Facilitated Discussion

CONTENT (Read aloud or hand to players):

The failure chain:

1. **Firewall Rule 49** — Overly broad. Added 6 months ago during WiFi upgrade. Allowed Guest WiFi to reach the entire Passenger Ops VLAN on port 443. Should have been scoped to the captive portal server IP only.
2. **Default PA credentials** — admin/Converg3nt! for 18 months. Vendor installation guide is publicly available. Password was never changed.
3. **FIDS management on HTTP:8080** — Unencrypted, no authentication beyond IP-source. Reachable from VLAN 50.
4. **No PA controller login monitoring** — No alert when someone logs in. No anomaly detection. No audit review.
5. **No Guest WiFi traffic monitoring** — Nobody watching what Guest WiFi clients are connecting to on the internal network.
6. **No emergency PA authentication** — The 'Emergency All Zones' broadcast requires only a web login. No two-person authorization. No physical key.

Each team: what's your #1 remediation priority?

■ CONTROLLER NOTE (DO NOT READ TO PLAYERS):

Immediate actions: Delete Rule 49. Change PA password. Restrict FIDS management to VLAN 20 only. Systemic: credential audit on ALL OT systems. Firewall rule review (when was the last full audit?). PA system: add login alerting, consider physical-key requirement for emergency broadcasts. Guest WiFi: proper isolation — Guest WiFi should ONLY reach the internet. Period. Push: 'How many other default passwords are on your OT systems right now? BMS? CCTV NVR? Baggage handling? Do you know?'

END OF MASTER INJECT DECK