SCENARIO 4: "THE LEAK"

Security Information Disclosure & Crisis 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 6:15 PM on a Wednesday. You are in the Airport Operations Center watching the evening news. Channel 5's lead story stops you cold.

The anchor is standing outside the NCIA terminal. Behind her, the airport logo is clearly visible. She is reading details that should never be on television: specific door access codes for the Secured Area. The location of camera blind spots in Concourse B. The PIN override sequence for the ARFF station. The fact that the airport's armory is located in Room 114 of the Security office suite — and that it uses a standalone lock, not the PACS system.

She cites a "confidential source with direct knowledge of airport security operations." She holds up what appears to be a printed document. Even from the TV screen, you can see the header: **"AIRPORT SECURITY PROGRAM — SENSITIVE SECURITY INFORMATION."**

Your Airport Security Program is on the evening news. Someone gave it to a reporter. And now everyone — every passenger, every employee, every person with bad intentions — knows exactly how you secure this airport.

YOUR MISSION: Determine who leaked the ASP and how. Immediately change every compromised security measure. Manage TSA, the media, and your own workforce. Rebuild your security posture while keeping the airport open.

Item	Status
Airport Operations	Normal — evening push in progress. 12 departures in the next 2 hours.
Airport Security Program	COMPROMISED. Specific details broadcast on live television.
PACS / Door Codes	Current codes are now public knowledge. All must be assumed compromised.
Camera Coverage	Blind spots publicly identified. Attacker could navigate around cameras.
TSA Status	Not yet notified. Regional office closes at 5 PM — after-hours contact required.
Media	Channel 5 story is airing NOW. Other outlets will pick it up within the hour.
Source of Leak	Unknown.

2. WHAT THE BROADCAST REVEALED

Based on the Channel 5 report, the following specific security details are now public:

- **Secured Area Door Codes:** The 4-digit PIN codes for Doors S-1 through S-6 (main terminal access points between the non-sterile and sterile areas). These are the doors used by airline, vendor, and airport staff to bypass TSA screening.
- **Camera Blind Spots:** Two specific locations in Concourse B where CCTV coverage does not overlap — the corridor between Gates B-7 and B-8, and the stairwell to the ramp level near Gate B-12. The reporter described these as "surveillance gaps."
- **ARFF Station PIN Override:** The emergency override code for the Aircraft Rescue and Fire Fighting station, used when the electronic lock fails. This code provides direct access to firefighting vehicles and equipment.
- **Armory Location & Lock Type:** The airport's weapons storage room (Room 114) was identified by number, and the report noted it uses a standalone key lock rather than the PACS electronic system — meaning it cannot be remotely audited or disabled.
- **Response Time Standards:** The report cited NCIA's own response time benchmarks for security incidents — information that could help an adversary plan around your reaction speed.

3. TEAM ASSIGNMENTS & STANDING ORDERS

TEAM A: AIRPORT OPERATIONS (COMMAND)	
Role: The airport is still running. Passengers are still flying. But every security measure the reporter just described is now compromised. You have to keep the airport open while Security changes every lock, code, and procedure that was revealed. That means coordinating with airlines, vendors, and TSA — tonight.	**Standing Orders:** Continuity: The airport stays open. Period. Coordination: Every door code change affects airline and vendor staff. Communicate changes in real time. Decision Authority: You approve the sequence and timing of security changes.

TEAM B: IT & CYBERSECURITY	
Role: The ASP is a document. It lives on a server. Someone either printed it, emailed it, copied it to a USB drive, or accessed it digitally. Your job is to find out how it left the building. Pull file server access logs. Check print logs. Review email gateway records. Find the digital trail.	**Standing Orders:** Audit: Who accessed the ASP file in the last 90 days? Trace: Was it printed? Emailed? Copied to removable media? Preserve: Forensic images of any relevant systems before making changes.

TEAM C: PUBLIC INFORMATION (PIO)	
Role: The story is on the air right now. Other outlets are calling. Employees are texting each other. Passengers are posting on social media. You cannot make the story go away — the First Amendment protects the reporter. But you can control what comes next. Draft statements. Prepare for the press conference. Decide what to say and what NOT to say.	**Standing Orders:** Hold: Do not confirm or deny specific security details — even ones already broadcast. Prepare: Draft statements for media, employees, airlines, and passengers. Coordinate: Everything goes through PIO. No one else talks to media.

TEAM D: SECURITY, LEGAL & TSA LIAISON	
Role: The ASP is Sensitive Security Information under 49 CFR Part 1520. Unauthorized disclosure is a federal violation. TSA must be notified. But you also need to investigate internally — who had access, who had motive, and how do you conduct that investigation without creating a witch hunt? Meanwhile, every compromised security measure needs to be changed — tonight.	**Standing Orders:** Notify: TSA Regional Office — after-hours emergency contact. Change: Every door code, PIN, and procedure that was revealed. NOW. Investigate: Identify who had access to the ASP. Do not accuse — gather facts.

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.
- **Dual Track:** This exercise has two parallel tracks — the investigation (who leaked it?) and the remediation (change everything that was compromised). Both must happen simultaneously. Don't neglect one for the other.

• **First Amendment:** The reporter has the right to publish. You cannot demand she take the story down, delete the footage, or reveal her source. Your legal options are limited. Focus on what you CAN control.

• **Assume Hostile Viewing:** The broadcast went out to tens of thousands of viewers. Assume that anyone with bad intentions now has the information the reporter shared. Act accordingly.

5. INCIDENT BRIEFING FORM (ICS-201)

INVESTIGATION TRACKER
Who had access to the ASP? What does the digital trail show? Who had motive?

Security Measure	Compromised ?	New Measure	Implemented?	Communicated to Staff?
Door Codes S-1 through S-6	YES		■	■
Concourse B Camera Gaps	YES		■	■
ARFF Station Override PIN	YES		■	■
Armory (Room 114) Lock	YES		■	■
Response Time Standards	YES		■	■
Other (ASP not yet verified)	UNKNOWN		■	■

NOTIFICATION TRACKER
TSA: ■ Notified ■ Time: _____ ■ Contact: _____
FBI/Law Enforcement: ■ Notified ■ Time: _____
Airport Board: ■ Notified ■ Time: _____
Airlines: ■ Notified ■ Time: _____
Employees: ■ Notified ■ Time: _____

EXERCISE — EXERCISE — EXERCISE