# MASTER INJECT DECK

## Scenario 4: "The Leak"

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 BROADCAST

**FROM:** Channel 5 News (Jennifer Pratt, Reporter)

**TO:** All Teams (Played on screen or read aloud)

**DELIVERY:** VIDEO or Facilitator reads aloud with conviction — stand at the front of the room

**CONTENT (Read aloud or hand to players):**

"Good evening. Channel 5 has obtained documents that raise serious questions about security at North Coast International Airport. According to a confidential source with direct knowledge of airport security operations, the airport's security plan — a federally required document that governs how the facility protects against terrorism and unauthorized access — reveals troubling details. Among the findings: the four-digit PIN codes used to access secured areas of the terminal — the areas beyond TSA screening — are shared among more than one hundred airline, vendor, and airport employees. Some of these codes have not been changed in over a year. The documents also show that two areas of Concourse B have no camera coverage — what security professionals call 'blind spots' — including a corridor near Gate B-7 and a stairwell to the ramp level. Perhaps most concerning: the airport's weapons storage room, identified as Room 114, uses a standalone key lock that cannot be electronically monitored or remotely disabled. We reached out to NCIA for comment but have not yet received a response. The source, who asked to remain anonymous, told Channel 5: 'People need to know how this airport is really run.' We'll have more on this story at 11."

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

This is the opening. Play it big. If you have a video, use it. If not, stand at the front of the room, hold a piece of paper like a reporter, and read this like a live broadcast. The phrase "People need to know how this airport is really run" directly echoes Delgado's exit interview comment — but the students don't know that yet. It will click later when HR delivers the report. After the broadcast, give the room 2-3 minutes to react before delivering I-02. Watch who takes charge. Watch whether anyone says "change the codes NOW" immediately.

**INJECT I-02** Phase 1 — 0:17

## TSA DEMANDS ANSWERS

**FROM:** TSA Federal Security Director

**TO:** Security / Operations (Teams D & A)

**DELIVERY:** Phone Call — Facilitator uses a tense, urgent tone

**CONTENT (Read aloud or hand to players):**

"This is the Federal Security Director. I just watched Channel 5. Tell me that I did not just see your Airport Security Program details on live television." (Pause for response.) "Alright. Here's what I need. First: a written incident report documenting what was disclosed, when you became aware, and what immediate actions you're taking. I need that in two hours. Second: confirmation that every security measure that was broadcast has been changed — every door code, every PIN, every access configuration. Tonight. Not tomorrow. Third: I need to know who leaked this, because someone just committed a federal violation under 49 CFR 1520.17, and I intend to pursue it. I'm activating our Regional Compliance team. They'll be at your airport by 8 AM. I strongly suggest you have your house in order by then."

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

Play the FSD as angry but controlled. This is a career-threatening event for the FSD too — they're responsible for TSA's relationship with this airport. If the team hasn't started changing codes yet, push: "You're telling me the codes that were broadcast 20 minutes ago are still active? What are you waiting for?" The 2-hour written report deadline is aggressive but realistic for an SSI disclosure of this magnitude.

**INJECT I-03** Phase 1 — 0:24

## THE REPORTER CALLS

**FROM:** Jennifer Pratt — Channel 5 News

**TO:** PIO (Team C)

**DELIVERY:** Phone Call — Facilitator uses a confident, professional tone

**CONTENT (Read aloud or hand to players):**

"Hi, this is Jennifer Pratt from Channel 5. I aired a story about NCIA's security program tonight and I'm putting together a follow-up for the 11 o'clock broadcast. I want to give you the chance to respond. A few questions: Were airport officials aware of the security gaps described in the documents? What steps are being taken to address them? And — I have to ask — is it true that the source of these documents is a former airport employee who was recently terminated? I'm on deadline, so I'd appreciate a response in the next 30 minutes. If I don't hear back, I'll note in my story that NCIA declined to comment."

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

The "former employee" question is a trap. She's testing whether the airport will confirm her source. If the PIO reacts — even with surprise or denial — she learns something. Correct response: "We are aware of the broadcast and are taking immediate steps to address it. The security of this airport and the safety of the traveling public are our highest priorities. We are cooperating with federal authorities. We will not discuss specifics of our security program or any ongoing investigation." If the PIO says "no comment": that's their right, but the story will say "NCIA declined to comment," which reads as guilty. A holding statement is better than silence.

**INJECT I-04** Phase 2 — 0:35

## THE FILE SERVER AUDIT

**FROM:** IT Team Analysis

**TO:** All Teams

**DELIVERY:** In-Person Report (IT reports findings to the room)

**CONTENT (Read aloud or hand to players):**

"We pulled the access logs from the file server. The ASP is stored at S:\Security\ASP\NCIA_ASP_2025_Current.pdf. Access permissions on that directory are... broader than they should be. The entire 'Airport Staff' security group has read access. That's 43 accounts. In the last 90 days, five accounts actually opened the file. Three are expected: the Airport Security Coordinator, the Deputy ASC, and the Airport Director. Two are flagged. The IT Manager's service account accessed it 45 days ago — that's consistent with a routine backup scan, but we're verifying. And Ray Delgado's account accessed it 22 days ago at 10:31 PM. That was the night before his last day. His account wasn't disabled until 8:15 the next morning."

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

This inject introduces Delgado by name and puts him at the top of the suspect list. But notice: the IT Manager's service account is also flagged. Let the team wonder about that — it's a red herring (legitimate backup scan) but it keeps them from locking in on Delgado too early. The bigger finding is that 43 accounts had read access. That's the systemic failure. If a student catches that: excellent instinct.

**INJECT I-05** Phase 2 — 0:43

## THE DISGRUNTLED EMPLOYEE

**FROM:** HR Director

**TO:** Operations / Legal (Teams A & D)

**DELIVERY:** In-Person Report

**CONTENT (Read aloud or hand to players):**

"I need to flag something about Ray Delgado. He was terminated three weeks ago for cause — repeated policy violations. He left a secured door propped open on two occasions, he was insubordinate with the Airport Security Coordinator during a training session, and he was found sleeping in the ARFF station on a night shift. His exit was ugly. During his exit interview, he told the ASC — and I have this in my notes — "You'll regret this. People need to know how this place is really run." That's almost word-for-word what the Channel 5 source said. He also filed a wrongful termination complaint with the state labor board two days after he was let go. That complaint is still pending."

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

"People need to know how this place is really run" — the students should connect this to the broadcast. Motive, access, and now a direct linguistic match. But Legal should immediately flag the wrongful termination complaint. Any action against Delgado could be framed as retaliation. The correct path is: refer to law enforcement, do not contact Delgado directly, preserve all evidence, and let the FBI or TSA handle the interview.

**INJECT I-06** Phase 2 — 0:50

## THE OPERATIONAL NIGHTMARE

**FROM:** Security Officer

**TO:** Security / Operations (Teams D & A)

**DELIVERY:** In-Person Report (Security officer at the table, looking stressed)

**CONTENT (Read aloud or hand to players):**

"Status update on the code changes. I've changed S-1 and S-2 in the PACS console. New codes are active. But here's the problem: those doors are used by 87 airline employees from three carriers, 34 vendor staff, and 22 airport employees. I need to notify all of them of the new codes. Delta's station manager says he needs 30 minutes to brief his team. United wants it in writing. SkyLounge says their night shift doesn't start until 9 PM and they won't have staff to brief until then. And the catering company isn't answering their phone. If I activate the new codes before everyone has the new PIN, I'm going to have airline ramp workers locked out of the terminal at 7:30 PM during the departure push. That's a baggage handling disaster. Do I hold the old codes until everyone's briefed, or go live and deal with the lockouts?"

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

This is the operational crunch. The security imperative is: change the codes NOW. The operational reality is: if you change them before everyone knows the new ones, you're going to have airline workers locked out during the busiest hour of the evening. There's no clean answer. Best practice: change the codes now, post a security officer at each affected door to manually verify and admit authorized personnel until the new codes are fully distributed. It's resource-intensive but it solves both problems.

**INJECT I-07** Phase 2 — 0:58

## THE STORY GOES NATIONAL

**FROM:** Associated Press Reporter

**TO:** PIO (Team C)

**DELIVERY:** Phone Call — Facilitator uses a friendly, matter-of-fact tone

**CONTENT (Read aloud or hand to players):**

"Hi, this is David Chen with the Associated Press. We're picking up the Channel 5 report about a security document leak at North Coast International Airport. I'm filing for the national wire — this will go to every newsroom in the country by morning. My deadline is 9 PM. I need a statement — 100 words or less is fine. I'm going to include the details from the Channel 5 broadcast. I'd prefer to include your response alongside them. Is someone available to make a statement on the record?"

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

The escalation. This is no longer local news — it's going national. Every airline exec, every TSA official in Washington, every congressional office with transportation oversight will see this story by morning. The PIO should have a polished statement by now. If they're still drafting: "You've had 48 minutes. The AP is on deadline. What's your statement?" The pressure is the point.

**INJECT I-08** Phase 2 — 1:05

## THE PRINT LOG

**FROM:** IT Team Analysis

**TO:** Security / Legal (Teams D & A)

**DELIVERY:** In-Person Report

**CONTENT (Read aloud or hand to players):**

"Found something in the print server logs. The ASP was printed once in the last 90 days. It was printed 22 days ago at 10:47 PM from workstation SECWS-02 — that's the shared workstation in the Security office. Here's the problem: SECWS-02 uses a shared local account. It doesn't authenticate against Active Directory. There's no record of which individual was logged in. Anyone with physical access to the Security office could have walked up, logged in with the shared credentials, and printed the entire ASP. That said — the timing matches. Delgado accessed the file digitally at 10:31 PM. Sixteen minutes later, someone printed it from the Security office. Delgado was on shift that night. He had physical access to the office."

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

The evidence chain is now: Delgado accessed the file (10:31 PM), then someone printed it (10:47 PM) from a workstation in the Security office where Delgado was on duty. It's circumstantial but compelling. The systemic failure here is the shared workstation. If SECWS-02 required individual login, there would be a definitive log. Instead, there's a gap — and that gap benefits any future leaker too. If the team asks "can we check badge swipes to the Security office?" — great question. The answer: yes, but the Security office uses a standard key, not the PACS system. Another gap.

**INJECT I-09** Phase 3 — 1:10

## THE ATTORNEY CALLS

**FROM:** Sarah Kwan — Attorney for Ray Delgado

**TO:** Legal / Operations (Teams D & A)

**DELIVERY:** Phone Call — Facilitator uses a sharp, measured legal tone

**CONTENT (Read aloud or hand to players):**

"Good evening. This is Sarah Kwan, I'm counsel for Raymond Delgado. I'm calling because I understand from my client that he may be a person of interest in connection with a media report about your airport's security program. Let me be direct. Mr. Delgado has not been contacted by any law enforcement agency. He has not been charged with any offense. He has a pending wrongful termination complaint with the state labor board — a complaint that alleges he was fired without adequate cause. If NCIA publicly names Mr. Delgado as a suspect, takes any action that could be construed as retaliation for his labor complaint, or contacts him directly without going through my office, we will pursue every available legal remedy — including amending the labor complaint to include a retaliation claim. I'd suggest you refer any investigative concerns to the appropriate federal agency and let them handle it through proper channels. My number is 555-0194 if your legal team wants to discuss."

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

The attorney is right. Legally, the airport should not: (1) contact Delgado directly, (2) publicly name him as a suspect, or (3) take any action that looks retaliatory while the labor complaint is pending. The correct move: refer the matter to the FBI and/or TSA for investigation. Provide them with the file server logs, print logs, and HR records. Let law enforcement conduct the interview and build the case. If the team pushes back — "But we KNOW it was him!" — remind them: you have circumstantial evidence on a shared workstation. That's not "knowing." That's suspecting. There's a legal difference.

**INJECT I-10** Phase 3 — 1:18

## THE TSA COMPLIANCE REVIEW

**FROM:** TSA Regional Compliance Team

**TO:** Security / IT / Operations (Teams D, B & A)

**DELIVERY:** In-Person — Facilitator role-plays TSA compliance officer. Calm, methodical, devastating.

**CONTENT (Read aloud or hand to players):**

"TSA Compliance. Thank you for having us on short notice. I need to conduct an emergency SSI handling review. Let's start with your file systems. Where is the ASP stored digitally? Show me the access permissions on that directory." (After seeing the permissions:) "Forty-three accounts have read access to this file. How many of those individuals have a documented need to know under 49 CFR 1520.11?" "Show me your print controls. Is there an approval workflow for printing SSI documents? No? Alright. Show me the authentication policy on workstation SECWS-02. A shared local account. So anyone can sit down and print the Airport Security Program and you'd have no record of who did it." "Do you maintain an SSI distribution tracking log — a record of who has physical or digital copies and when access was last reviewed?" (Pause.) "Help me understand how a document this sensitive ended up on a general-access file share, printable from an unauthenticated workstation, with no access audit trail and no distribution log."

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

This is the emotional climax. Play the compliance officer as calm — not angry, just... thorough. Let each question land. Wait for the answer. Let the silence do the work. The team should realize: the leak wasn't just Delgado's fault. The system made it easy. The ASP was one click away from anyone on the 'Airport Staff' security group. No encryption, no DRM, no print restriction, no alert, no audit. This is the pivot from "find the leaker" to "fix the system." The best students will recognize that even if you fire Delgado and charge him, you've still got 42 other accounts that could do the same thing tomorrow.

**INJECT I-11** Phase 3 — 1:26

## THE REVEAL

**FROM:** Facilitator

**TO:** All Teams

**DELIVERY:** Facilitator addresses the room directly — out of character

**CONTENT (Read aloud or hand to players):**

"Here's what happened. Ray Delgado, on his last night of employment — 22 days ago — decided to take a copy of the Airport Security Program. At 10:31 PM, he accessed the ASP from his still-active domain account on his workstation. At 10:47 PM, he walked to the shared workstation in the Security office and printed the full 47-page document. He put it in his bag. He finished his shift. He turned in his badge the next morning. Nobody checked his bag on the way out. Three weeks later, he contacted Jennifer Pratt at Channel 5 — a reporter he'd met at a community event — and gave her the printed ASP. His motive was revenge. He felt he'd been fired unfairly. He wanted to embarrass the airport and prove that security was, in his words, 'a joke.'" "But here's the lesson. Delgado didn't hack anything. He didn't bypass any controls. He didn't social-engineer anyone. He used his own credentials to access a file that 43 accounts could access, printed it on a workstation that didn't log who was using it, put it in a bag that nobody searched, and walked out the door. He walked through open doors. Every single one."

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

Let this land. Give the room a moment. Then transition to I-12 — the forward-looking remediation discussion. The line "He walked through open doors" should be the takeaway they remember.

**INJECT I-12** Phase 3 — 1:32

## REMEDIATION PLANNING

**FROM:** Facilitator

**TO:** All Teams

**DELIVERY:** Facilitated Discussion — use the whiteboard

**CONTENT (Read aloud or hand to players):**

**The facilitator asks each team to address their area:**

**Security:** Beyond tonight's code changes — what permanent changes to physical security? Cameras in the B Concourse blind spots? New lock on the armory? Two-person access to SSI materials? Bag checks for departing employees with SSI access?

**IT:** How should the ASP be stored? Encrypted document vault? Access logging with real-time alerts? Print restrictions (watermarked, logged, approval-required)? Eliminate all shared workstations? DLP (Data Loss Prevention) tools?

**Legal:** Refer Delgado to FBI or TSA? What's the process? How do you protect the airport from the wrongful termination retaliation claim while pursuing the SSI violation? What's the timeline for mandatory ASP revision with TSA?

**PIO:** The 11 PM story is airing in hours. What's your final statement? Do you recommend a proactive press conference tomorrow morning to get ahead of the national coverage? What's the internal communication to employees?

**Ops:** When will all compromised security measures be fully replaced? What's the plan for running the airport during the TSA compliance review tomorrow?

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

This grounds the exercise in actionable planning. Push for specifics and timelines. The best outcomes include: - ASP moved to encrypted vault with individual access logging - Shared workstations eliminated or replaced with individual-auth terminals - Print controls requiring supervisor approval for SSI documents - SSI distribution log created and maintained - Off-boarding checklist updated: access revoked before notification, bag check policy - Camera repositioning to eliminate Concourse B blind spots - Armory lock upgraded to PACS-controlled electronic lock - PIO proactive press conference to demonstrate accountability and action

**END OF MASTER INJECT DECK**