CONTROLLER HANDBOOK

Scenario 4: "The Leak"

SSI Disclosure, Internal Investigation & Security Remediation
North Coast International Airport (NCIA)
FACILITATOR / INSTRUCTOR USE ONLY

FACILITATOR DOCUMENT — DO NOT DISTRIBUTE TO PLAYERS

1. EXERCISE OVERVIEW

Exercise Date: [Date]

Duration: 2 Hours

Scope: Discussion-based TTX. A local television station broadcasts details from NCIA's Airport Security Program, triggering an SSI disclosure crisis. Students must simultaneously investigate the source of the leak, change every compromised security measure, manage TSA's response, and handle media pressure — all while keeping the airport operational during the evening push.

Exercise Objectives

- **SSI Awareness:** Do students understand what SSI is, why it matters, and what happens when it's disclosed?
- **Dual-Track Response:** Can the team run an investigation AND a remediation effort simultaneously?
- **Media & Legal Judgment:** Can the PIO manage a hostile media environment without confirming sensitive details? Can Legal navigate the tension between the investigation and the wrongful termination complaint?
- **Operational Continuity:** Can Ops coordinate mass security changes (door codes, access groups) across airlines, vendors, and airport staff during active operations?
- **Systemic Thinking:** Does the team recognize that the leak was enabled by systemic failures — not just one bad actor — and develop long-term remediation?

2. HOW THIS SCENARIO WORKS

This exercise has two emotional peaks. The first is the broadcast itself — the gut-punch of seeing your security plan on television. The second is the TSA compliance review (I-10), where the team has to explain how the ASP was stored on a broadly accessible share with no print controls and no audit trail. That second peak is the real lesson: the problem isn't Ray Delgado. The problem is that it was this easy.

The investigation track is designed to build toward Delgado gradually — he's the obvious suspect, but the team shouldn't rush to accuse him. The attorney call (I-09) is the guardrail: it forces them to think about due process, retaliation risk, and the difference between suspicion and evidence.

The remediation track is designed to be overwhelming. Changing door codes sounds simple — until you realize that 143 people use Door S-3 and they all need to know the new code before it changes. This is where Ops

earns their paycheck.

3. ROOM SETUP

- **TV or Projector:** For the opening broadcast. If you have an AI-generated news video, play it. If not, read the script aloud with conviction. The visual impact of seeing your airport on the news matters.
- **Two Whiteboards:** Label one "INVESTIGATION" and the other "REMEDIATION." Teams should be tracking both throughout the exercise.
- **Team Seating:** Standard layout — Ops at the head, IT right, Security/Legal left, PIO rear.
- **Printed Materials:** SSI Reference Card is critical for this scenario. Every student should have one.

4. SIMCELL ROLE-PLAY GUIDANCE

TSA Federal Security Director (I-02)

Angry but professional. This is the FSD's worst nightmare. "I have to brief Washington by midnight. You have two hours." If the team hasn't started changing codes yet: "Why are we still talking? Every minute those codes are unchanged is a minute someone could walk through your doors." The FSD is an ally but an impatient one.

Jennifer Pratt, Channel 5 Reporter (I-03)

Confident, professional, and unintimidated. She's done nothing illegal — the First Amendment protects her. She will not reveal her source. She's calling to give the airport a chance to respond, which is actually a courtesy. If the PIO gets hostile: "I understand you're upset. But this information is now public, and I think your community deserves to know how their airport is secured. Would you like to comment or not?" She's fishing for reactions — especially to the "former employee" hint. Don't let the PIO confirm anything about the source.

Delgado's Attorney (I-09)

Sharp and direct. She's protecting her client and putting the airport on notice. "My client has a pending wrongful termination complaint. Anything you do that looks like retaliation — naming him publicly, contacting him without counsel, even implying he's a suspect in a press statement — will become part of our case. I'd suggest you let law enforcement handle this." If they push back: "Are you telling me you're conducting your own investigation into a federal SSI violation rather than referring it to the FBI or TSA? That's an interesting choice." She's right — the airport should refer this to law enforcement.

TSA Compliance Team (I-10)

This is the most important role-play in the scenario. The compliance officer is calm, methodical, and devastating. They're not there to yell. They're there to ask questions that the team can't answer well. "Show me the access permissions on the S:\Security share." (Too broad.) "Show me the print log controls." (None.) "Show me the authentication policy for SECWS-02." (Shared account.) "Show me your SSI distribution tracking log." (If they have one, good. If not — that's a finding.) Let the silence after each question do the work. The team should feel the gap between where they are and where they should be.

AP Reporter (I-07)

Friendly, matter-of-fact, and on deadline. The AP wire is the escalation — this takes the story national. "We're running this tonight. Every newsroom in the country will see it by morning. I need 100 words or less. Do you have a statement?" The clock pressure is real.

5. PACING GUIDE

Phase	Clock	Duration	Notes
0: Briefing	0:00 – 0:10	10 min	Distribute packets. Play the broadcast video or read the script. Let the room react. This scenario starts hot — no slow build.
1: Bomb Drops	0:10 – 0:35	25 min	Three rapid injects: broadcast, TSA call, reporter call. The team should feel overwhelmed. Watch whether they start on remediation (changing codes) or investigation first. The best teams do both simultaneously.
2: Investigation	0:35 – 1:10	35 min	Evidence builds toward Delgado. Remediation creates operational friction. The AP call escalates media pressure. Give 6-8 minutes between injects. Watch whether Legal is managing the Delgado situation carefully or jumping to conclusions.
3: Remediation & Reckoning	1:10 – 1:40	30 min	The attorney call complicates the investigation. TSA compliance review is the emotional climax — the team faces systemic failures they didn't know they had. Facilitator reveal, then forward-looking remediation planning.
4: Debrief	1:40 – 2:00	20 min	3-Up / 3-Down. Focus discussion on: SSI handling failures, off-boarding procedures, the tension between investigation and remediation, and media/legal constraints.

6. EVALUATION & GRADING RUBRIC

Metric	Assessment Criteria
Metric 1: SSI Awareness & Response (25 Points)	**Fail:** Team didn't recognize the ASP as SSI. Didn't notify TSA promptly. Discussed SSI details openly or confirmed them to media. **Pass:** Team recognized the SSI violation, notified TSA, and avoided confirming details to media. **Excellence:** Team cited 49 CFR Part 1520, initiated TSA notification within minutes, and PIO gave a statement that acknowledged the situation without confirming any SSI details.
Metric 2: Investigation Quality (25 Points)	**Fail:** Team jumped to accusing Delgado without evidence. Or ignored the investigation entirely. **Pass:** Team followed the evidence trail, identified Delgado as primary suspect, but handled the legal complications poorly. **Excellence:** Team built the case methodically, respected legal constraints (attorney, wrongful termination), and referred the matter to law enforcement rather than conducting their own confrontation.
Metric 3: Remediation Execution (25 Points)	**Fail:** Team talked about changing codes but never developed a plan for communicating changes to 143+ staff. Or changed codes without notifying airlines/vendors, causing operational disruption. **Pass:** Team developed a sequenced remediation plan and began coordinating with airlines/vendors. **Excellence:** Team prioritized remediation by exploitability (door codes first, camera positions later), created a communication plan for all affected staff, and addressed the armory lock as an urgent physical change.
Metric 4: Systemic Thinking (25 Points)	**Fail:** Team treated this as a "bad employee" problem. Never questioned how the ASP was stored or protected. **Pass:** Team recognized that the shared workstation and broad file access were contributing factors. **Excellence:** Team identified every systemic failure: unencrypted storage, no DLP, shared workstation, no print controls, no SSI access audit, inadequate off-boarding. Built a long-term remediation plan addressing all of them. Recognized that "it was only a matter of time" regardless of Delgado.

7. HOT WASH GUIDE

Key Discussion Questions

- **The Off-Boarding Problem:** "Delgado accessed the ASP on his last night. His account was active until the next morning. What should your off-boarding process look like for employees with SSI access? Should access be revoked the moment termination is decided — before the employee is told?"
- **The Storage Problem:** "Your most sensitive document was a PDF on a shared drive accessible to 40+ people. What does secure SSI storage look like? Encrypted vault? Physical-only copies? Access logging with alerts? Two-person access controls?"
- **The Media Problem:** "You can't stop the reporter from publishing. The First Amendment is clear. So what CAN you do? How do you minimize further damage while respecting press freedom?"
- **The Dual-Track Challenge:** "Did your investigation slow down your remediation, or vice versa? In a real event, you'd have limited personnel for both. How do you staff two simultaneous efforts?"
- **The Human Element:** "Delgado was angry. He felt wronged. He wanted revenge. Does your organization have processes for identifying and managing disgruntled employees before they become security risks? What about employee assistance programs?"

END OF CONTROLLER HANDBOOK