MASTER SCENARIO EVENTS LIST (MSEL)

Scenario 4: "The Leak" — SSI Disclosure & Internal Investigation

North Coast International Airport (NCIA)
Duration: 2 Hours | Target: All Teams
CONTROLLER DOCUMENT — NOT FOR PLAYER DISTRIBUTION

CONTROLLER DOCUMENT — DO NOT DISTRIBUTE TO PLAYERS

SCENARIO OVERVIEW

Theme: What happens when your security plan becomes public knowledge. SSI handling, internal investigation, media/legal tension, and the massive operational burden of changing every compromised security measure at once.

The Trigger: A local TV reporter broadcasts specific details from NCIA's Airport Security Program on the evening news, citing a "confidential source." The ASP is SSI — this is a federal violation by the source. The airport must simultaneously investigate the leak, notify TSA, change all compromised measures, and manage the media firestorm.

The Twist: Multiple plausible sources emerge during the investigation. A recently terminated security supervisor with a grudge. A file server with overly broad access permissions. A print log that points to a specific workstation. The real answer — revealed in Phase 3 — is that the terminated officer (Ray Delgado) printed the ASP on his last night and took a physical copy. But the deeper lesson is that the ASP was inadequately protected: stored on an unencrypted shared drive accessible to 40+ employees, printable without approval, and never audited. Even without Delgado, it was a matter of time.

Key Design Principle: This scenario runs on two parallel tracks that compete for attention. Track 1 is the investigation — the whodunit. Track 2 is the remediation — changing every compromised security measure while the airport is still operating. Teams that focus on one and neglect the other will struggle. The best teams work both tracks simultaneously.

PHASE 0: BRIEFING 0:00 — 0:10

Time	ID	From	To	Event / Message	Expected Action
0:00	START	Facilitator	All	STARTEX. Distribute Player Briefing Packet and SSI Reference Card. Set the scene: it's 6:15 PM, you're watching the news, and your ASP is being read on live television. If you have a video prepared (AI-generated news broadcast), play it now.	Players review materials. Teams organize. The energy should be urgent from the start — this scenario doesn't have a slow burn. It starts hot.

PHASE 1: THE BOMB DROPS 0:10 — 0:35

Goal: Immediate crisis response. TSA notification, initial security changes, media pressure. Everything hits at once.

Time	ID	From	To	Event / Message	Expected Action
0:10	I-01	Facilitator (Channel 5)	All	The broadcast. Facilitator reads the news script aloud (or plays video if available). "Channel 5 has obtained documents revealing critical security vulnerabilities at North Coast International Airport. According to a confidential source, the airport's security plan — which governs how the facility protects against terrorism and unauthorized access — contains details that raise serious concerns..." (Read specific details about door codes, camera gaps, armory location, ARFF override.)	Immediate reaction. Who takes command? First question should be: "Is this real?" (Answer: yes — the details are accurate.) Second question: "Who do we call first?" (TSA.) Third: "What do we change first?" (Door codes — they're the most immediately exploitable.)
0:17	I-02	Phone Call	Security / Ops	TSA Federal Security Director calls (after-hours emergency line): "I just saw Channel 5. Tell me this isn't real. Tell me your ASP is not on television right now." (Pause.) "It is? Alright. I need three things from you in the next two hours: a written incident report, a list of every security measure that was compromised, and confirmation that you've changed every code and PIN that was broadcast. I'm activating our Regional Compliance team. Expect them on-site by 8 AM tomorrow. And I need to know who leaked this — because someone committed a federal violation."	Security/Legal must own the TSA relationship. Start the incident report. Begin cataloging every compromised measure. The 2-hour deadline is aggressive but realistic. Do they have the capacity to change all door codes AND investigate AND manage media simultaneously?
0:24	I-03	Channel 5 Reporter	PIO	Phone call: "Hi, this is Jennifer Pratt from Channel 5. I'm the reporter who aired the security story tonight. I want to give NCIA the chance to respond. We're running a follow-up at 11 PM. Are airport officials aware of these vulnerabilities? What are you doing to fix them? And is it true that a former employee provided us with this information?" (She's fishing — she won't confirm her source, but she's hinting it's a former employee to see if you react.)	PIO must decide: comment or no comment? If they comment, what do they say? Key trap: if they react to "former employee," they've confirmed a line of investigation. Correct approach: "We are aware of the broadcast and are taking immediate steps to address it. We take the security of this airport extremely seriously. We will not discuss specifics of our security program." Do NOT engage with the source question.

PHASE 2: THE INVESTIGATION 0:35 — 1:10

Goal: The parallel tracks intensify. The investigation produces multiple leads. The remediation creates operational friction. External pressure mounts.

Time	ID	From	To	Event / Message	Expected Action
0:35	I-04	IT Team	All	IT reports on the file server audit: "The ASP is stored as a PDF on the S:\Security share. Access logs show that 5 accounts accessed this file in the last 90 days. Three are expected — the ASC, the Deputy ASC, and the Airport Director. Two are not: the IT Manager's service account (routine backup scan — probably benign) and... Ray Delgado's account. He accessed the file 22 days ago — the night before his last day. His access wasn't revoked until the next morning."	Delgado is now the primary suspect. But caution: the IT Manager's access is also unexplained (and it IS benign, but they don't know that yet). Do they jump to a conclusion or keep investigating? Legal should remind them: accusation without proof is a lawsuit waiting to happen.
0:43	I-05	HR Dept	Ops / Legal	HR Director reports: "Ray Delgado was terminated three weeks ago for repeated policy violations — failure to follow patrol procedures, insubordination with the ASC, and an incident where he left a secured door propped open. He did not go quietly. He told the ASC during his exit interview, and I'm paraphrasing: 'You'll regret this. People need to know how this place is really run.' He filed a wrongful termination complaint with the state labor board two days later."	Motive established. But Legal should flag: a wrongful termination complaint means anything the airport does regarding Delgado could look like retaliation. They need to be very careful about how they handle this. Do they contact Delgado directly? Through counsel? Through law enforcement?
0:50	I-06	Security Officer	Security / Ops	An on-duty security officer reports: "I'm trying to change the door codes on S-3 and S-4, but every code change has to be pushed through the PACS admin console, and then every badged employee who uses those doors needs to be notified of the new code. That's 87 airline employees, 34 vendor staff, and 22 airport employees for S-3 alone. I can change the code in the system in two minutes. Getting 143 people to stop using the old code and start using the new one? That's going to take all night. And half of them are mid-shift right now."	This is the operational reality of remediation. Changing a code is easy. Communicating the change to 143 people across multiple employers while flights are actively operating is hard. Ops needs to coordinate with airlines and vendor managers. Do they change all codes at once (maximum disruption) or sequentially (slower but more manageable)?
0:58	I-07	Phone Call	PIO	A second reporter calls — this time from the Associated Press wire service: "We're picking up the Channel 5 story about the airport security breach. This is going to go national. Our deadline is 9 PM. Do you have a statement?"	The story is escalating. It's no longer a local news item — it's going national. PIO should have a statement ready by now. If they don't, they're behind. The AP wire means every newspaper, TV station, and website in the country will see this by morning. Does the PIO upgrade their response? Call a press conference?
1:05	I-08	IT Team	Security / Legal	IT reports on the print log analysis: "I pulled the print server logs. The ASP was printed once in the last 90 days — 22 days ago, at 10:47 PM, from the shared workstation in the Security office (SECWS-02). That's after normal business hours. There's no record of who was logged in because that workstation uses a shared local account — it doesn't authenticate against Active Directory. Anyone with physical access to the Security office could have printed it. But given the timing... it was Delgado's last night on shift."	The evidence is circumstantial but strong: Delgado accessed the file digitally AND someone printed it from the Security office on his last night. But it's a shared workstation — no definitive proof. Legal question: is this enough to refer to law enforcement? IT question: why is there a shared workstation that doesn't log individual users?

PHASE 3: REMEDIATION & RECKONING 1:10 — 1:40

Goal: The investigation reaches its conclusion. But the bigger lesson emerges: the leak was enabled by systemic failures in SSI handling. The team must plan long-term remediation.

Time	ID	From	To	Event / Message	Expected Action
1:10	I-09	Phone Call	Legal / Ops	Delgado's attorney calls: "This is Sarah Kwan, counsel for Ray Delgado. I'm calling because I understand the airport may be considering accusations against my client in connection with a media report. I want to be clear: Mr. Delgado has not been contacted by law enforcement and has not been charged with anything. If NCIA publicly names him as a suspect or takes any action that could be construed as retaliation for his wrongful termination complaint, we will pursue all available legal remedies. I'd encourage your legal team to tread very carefully."	Legal must handle this. The attorney is right — they can't publicly accuse Delgado without proof, and the wrongful termination complaint complicates everything. The correct move is to refer the matter to law enforcement (FBI or TSA) and let them conduct the interview. The airport should not contact Delgado directly.
1:18	I-10	TSA Compliance Team	Security / Ops	TSA compliance team arrives (facilitator role-plays): "TSA Compliance. We're here for the emergency SSI review. I need to see three things immediately: your SSI distribution log — who has copies and who has access. Your file server access controls — show me the permissions on the ASP directory. And your workstation authentication policy — I understand you have a shared local account on a security office workstation?" (Long pause.) "Walk me through how a document this sensitive was stored on a general-access file share, printable from an unauthenticated workstation, with no access audit trail."	This is the reckoning. TSA is asking the real question: not just who leaked it, but how was it possible to leak it this easily? The systemic failures: (1) ASP on a broadly accessible share. (2) No DLP or print controls. (3) Shared workstation with no individual authentication. (4) No SSI access audit log. The team should start building a remediation plan that goes beyond changing door codes.
1:26	I-11	Facilitator	All	FACILITATOR REVEAL: "Here's what happened. Ray Delgado, on his last night of employment, accessed the ASP from his still-active account, walked to the shared workstation in the Security office, printed the full document, and walked out of the building with it. Three weeks later, he gave it to Jennifer Pratt at Channel 5." "But that's only half the story. The reason Delgado could do this so easily is because the ASP had no meaningful access controls. It was a PDF on a shared drive. Any of 40+ employees could have accessed it. There was no digital rights management. No print restriction. No access alert. The shared workstation didn't even log who was sitting at it. Delgado didn't hack anything. He didn't bypass any controls. He walked through open doors."	Let the team absorb this. Then pivot to the forward-looking discussion (I-12).

Time	ID	From	To	Event / Message	Expected Action
1:32	I-12	Facilitator	All	REMEDIATION PLANNING. The facilitator asks each team to address: — Security: What physical and procedural changes are needed beyond the immediate code changes? Camera repositioning? New lock on the armory? Response procedure revisions? — IT: How should the ASP be stored going forward? Encryption? Access logging? DRM? What about the shared workstation problem? — Legal: What's the process for referring Delgado to law enforcement? How do you handle the wrongful termination complaint alongside a federal SSI violation? — PIO: The 11 PM follow-up story is airing tonight. What's your statement? What about a proactive press conference tomorrow morning? — Ops: How long until all compromised measures are fully replaced? What's the plan for the TSA ASP revision requirement?	Teams build a comprehensive remediation plan. This should be concrete and specific. The facilitator should push for timelines: "When will the new door codes be fully operational? When will the ASP revision be submitted to TSA? When will the shared workstation be replaced?"

PHASE 4: DEBRIEF / HOT WASH 1:40 — 2:00

Time	ID	From	To	Event / Message	Expected Action
1:40	END	Facilitator	All	ENDEX. 3-Up / 3-Down, followed by key discussion questions: 1. When you saw the broadcast, what was your first instinct? Fight the media? Find the leaker? Change the codes? 2. How did you balance the investigation and the remediation? Did one suffer? 3. Could you have prevented this? What SSI controls would have stopped Delgado? 4. The reporter has First Amendment protection. How does that change your options? 5. What does your organization's off-boarding process look like? Would a departing employee have time and access to do what Delgado did?	Team reflects. Facilitator captures lessons learned. Exercise complete.

END OF MSEL