SCENARIO 5: "CARBON COPY"

Access Control Compromise & Digital Forensics

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 7:42 AM on a Thursday. The morning departure push is underway. The Airport Operations Center receives an automated alert from the PACS system — the Physical Access Control System that manages every badge reader on every secured door in the terminal.

The alert reads:

> **PACS ALERT — DUPLICATE CREDENTIAL EVENT**
>
> ```
> BADGE #: NCIA-2847
> ASSIGNED TO: Carlos Mendez (SkyWay Catering – Vendor)
> EVENT 1: Door S-4 (Concourse A Sterile/Non-Sterile) – 07:38:12 – ACCESS GRANTED
> EVENT 2: Door R-7 (Ramp Level – Baggage Makeup) – 07:39:41 – ACCESS GRANTED
>
> ALERT: Two access events on the same credential at physically non-adjacent readers
> within 89 seconds. Minimum transit time between S-4 and R-7 is approximately 4
> minutes on foot.
> ```

The same badge was used at two different doors, 89 seconds apart, in locations that are at least 4 minutes apart on foot. That is physically impossible.

Either the PACS system has a glitch — or someone has cloned an airport security badge.

YOUR MISSION: Determine whether this is a system error or a cloned badge. If cloned, identify the clone holder, trace every door they accessed, determine what they were after, and secure the airport — all before whoever is using the clone finishes what they came to do.

Item	Status
Airport Operations	Normal. Morning departure push. 14 flights in the next 90 minutes.
PACS System	Online. Alert triggered. No other anomalies detected — yet.
Badge NCIA-2847	Assigned to Carlos Mendez, SkyWay Catering vendor employee. 2-year tenure. No prior incidents.
Door S-4	Concourse A sterile/non-sterile boundary. High-traffic. Leads to gate area.

Door R-7	Ramp level access — baggage makeup area. Connects to active aircraft ramp.
CCTV Status	Cameras at both doors are operational. Footage available for review.

2. KEY CONCEPT: HOW BADGE CLONING WORKS

Most airport access badges use RFID (Radio Frequency Identification) or proximity card technology. When you hold your badge near a reader, the badge transmits a stored credential number wirelessly. The reader sends that number to the PACS controller, which checks it against a database of authorized credentials.

The vulnerability: many legacy proximity card systems — particularly those using 125 kHz technology (such as HID ProxCard II) — transmit the credential number **unencrypted**. The number is static — it never changes. Anyone with a $25 RFID reader/writer device (available online) can stand close to a badge holder, capture the credential number in seconds, and write it to a blank card. The clone is functionally identical to the original.

More modern systems use 13.56 MHz smart cards (iCLASS, SEOS, DESFire) with encrypted, mutually authenticated communication. These are significantly harder to clone — but not impossible, especially if the PACS controller is still configured to read legacy formats for backwards compatibility.

NCIA's Current Badge Technology

Component	Specification	Security Implication
Card Type	HID iCLASS SE (13.56 MHz)	Modern encrypted card. Resistant to casual cloning.
Legacy Support	HID ProxCard II (125 kHz) — legacy mode ENABLED on 12 readers	VULNERABILITY: 12 readers still accept unencrypted 125 kHz credentials for backwards compatibility with older vendor badges.
PACS Software	Lenel OnGuard 8.1	Supports anti-passback and duplicate credential alerts.
Anti-Passback	Enabled on exterior doors. NOT enabled on interior doors.	VULNERABILITY: Once past an exterior door, movement between interior doors is not tracked for passback violations.
Duplicate Alert	Enabled — triggers on same badge at 2+ readers within configurable time window	This is how the alert was generated. Working as designed.

3. TEAM ASSIGNMENTS & STANDING ORDERS

TEAM A: AIRPORT OPERATIONS (COMMAND)	
Role: Someone may be moving through your secured areas right now with a cloned badge. That means an unauthorized person is potentially on the ramp, near aircraft, near baggage. You have a morning departure push underway. You need to decide: do you lock down? Increase screening? Post officers at doors? And you have to coordinate with the airlines — their ramp workers use these same doors.	**Standing Orders:** Assess: Is this a system error or a real threat? Decide your posture. Contain: Consider posting officers at S-4 and R-7 immediately. Coordinate: Airlines need to know if ramp access is being restricted.

TEAM B: IT & CYBERSECURITY (LEAD — THIS IS YOUR SCENARIO)	
Role: This is a digital forensics puzzle. You need to pull PACS logs, correlate them with CCTV timestamps, analyze badge reader communication protocols, and determine whether this credential was cloned — and if so, how. Was it a 125 kHz legacy exploit? Was the PACS database breached? Was the card physically captured and duplicated? The technical trail will tell you what happened. You are the lead team for this exercise.	**Standing Orders:** PACS Forensics: Pull the full event log for NCIA-2847 — last 30 days. Protocol Analysis: Determine which readers accepted the credential and at what frequency. Correlate: Match PACS events to CCTV footage. Two people, two doors, same time = clone confirmed. Trace: Map every door the clone accessed. Build the movement timeline.

TEAM C: PUBLIC INFORMATION (PIO)	
Role: If word gets out that airport badges can be cloned, it's a devastating headline: "Anyone can walk into the secured area." That's not true — but it's what people will think. Your job is to prepare for that narrative while the investigation runs. Draft holding statements. Monitor social media. Be ready.	**Standing Orders:** Prepare: Draft statements for multiple scenarios (system error vs. confirmed clone). Monitor: Watch social media for any passenger reports of unusual activity. Hold: Do NOT confirm a badge cloning incident until IT has verified it.

TEAM D: SECURITY & LAW ENFORCEMENT	
Role: If this is a cloned badge, someone walked through a secured door with a forged credential. That's a federal violation — 49 USC § 46314 (entering an airport area in violation of security requirements). You need to identify the clone holder, find them if they're still in the building, and secure any area they accessed as a potential crime scene. You also need to figure out: was this targeted, or a test for something bigger?	**Standing Orders:** Identify: Work with IT to match CCTV to the clone events. Get a face. Locate: Is the clone holder still in the building? Check current PACS data. Secure: Any area the clone accessed should be treated as potentially compromised. Notify: TSA must be informed of an access control breach.

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.

• **This Is a Puzzle:** There is a specific answer. The clues are in the PACS logs, CCTV footage, badge reader data, and witness reports. You have to assemble them. Pay attention to timestamps, locations, and details.

• **The Clock Is Real:** If the clone holder is still in the building, every minute you spend debating is a minute they could be accessing restricted areas. Move with urgency.

• **IT Leads:** Team B is the lead investigative team for this scenario. Other teams support and make operational decisions based on IT's findings.

5. INCIDENT BRIEFING & INVESTIGATION WORKSHEET

CLONE MOVEMENT MAP

As IT identifies doors accessed by the clone, plot them here to build a movement timeline:

Time	Door	Location	Real Mendez or Clone?	CCTV Con firmed?	Notes
07:38:12	S-4	Concourse A boundary	?	■	
07:39:41	R-7	Ramp — baggage makeup	?	■	

KEY QUESTIONS TO ANSWER

1. Is this a system glitch or a confirmed clone? _____
2. Which frequency was the clone read at? (125 kHz legacy or 13.56 MHz?) _____
3. Where was the original badge likely captured/copied? _____
4. Who is the clone holder? (Physical description from CCTV) _____
5. What areas did the clone access? _____
6. What was the clone holder after? _____
7. Is the clone holder still in the building? _____
8. How many other badges could be at risk from the same cloning method? _____

EXERCISE — EXERCISE — EXERCISE