SSI HANDLING REFERENCE CARD

Scenario 4: "The Leak" — Supporting Material

What is SSI? Who can access it? What happens when it leaks?
FOR TRAINING USE ONLY

WHAT IS SENSITIVE SECURITY INFORMATION (SSI)?

Sensitive Security Information is a category of information protected under federal law (49 CFR Part 1520). SSI is not classified — it is not Secret or Top Secret. But it is restricted. SSI may only be accessed by persons with a "need to know" and may not be disclosed to the public.

At an airport, the most important SSI document is the **Airport Security Program (ASP)**. The ASP is the master document that describes how the airport complies with TSA security regulations. It contains details about access control, credentialing, law enforcement response, contingency procedures, and the airport's security infrastructure.

WHAT QUALIFIES AS SSI?

Category	Description
Airport Security Programs (ASP)	The entire document and any attachments, amendments, or appendices.
Security Directives & Emergency Amendments	TSA-issued directives that modify security requirements.
Vulnerability Assessments	Any assessment of the airport's security weaknesses.
Threat Information	Specific threat advisories received from TSA, FBI, or DHS/CISA.
Screening Procedures	Specifics of passenger and baggage screening operations.
Security Incident Details	Details about security breaches, investigations, and enforcement actions.
Contingency Plans	Security-related portions of emergency response plans.
PACS Data	Door codes, access levels, badge system configurations, camera placements.

WHO CAN ACCESS SSI?

Under 49 CFR § 1520.11, SSI may only be disclosed to persons who have a **need to know**. This includes:

- Airport employees whose job functions require access (security coordinators, certain operations staff)
- TSA personnel
- Law enforcement officers with a direct operational need
- FAA inspectors conducting Part 139 or security reviews
- Contractors working on security systems — **only** the portions relevant to their work

SSI may NOT be disclosed to: media, the general public, elected officials without clearance, airline employees (unless they have a specific need to know), or airport employees whose job functions do not require access to security details.

WHAT HAPPENS WHEN SSI IS DISCLOSED?

Unauthorized disclosure of SSI triggers several obligations:

- **TSA Notification:** The airport must immediately notify the TSA Federal Security Director (FSD) and the TSA Regional Office. TSA may require an emergency revision of the ASP and may impose additional security measures.
- **Law Enforcement Referral:** Unauthorized disclosure of SSI can result in civil penalties up to $25,000 per violation under 49 CFR § 1520.17. Criminal penalties may apply if the disclosure was intentional and connected to other offenses.
- **Security Remediation:** Every security measure described in the disclosed material must be assumed compromised and changed immediately — door codes, PINs, access configurations, camera positions, response procedures.
- **ASP Revision:** TSA may require the airport to submit a revised ASP within a compressed timeline. This is a major administrative and operational undertaking.

Important: The First Amendment generally protects the media's right to publish information, even SSI, once obtained. The airport's legal recourse is against the **source** of the leak, not the reporter. You cannot compel a journalist to reveal their source or take down a published story.

ASP ACCESS AT NCIA — WHO HAS IT?

Person / Role	Access Type	Notes
Airport Security Coordinator (ASC)	Full — digital & physical copy	Primary custodian. Office copy in locked safe.
Deputy ASC	Full — digital & physical copy	Backup custodian.
Airport Director	Full — digital only	Read access on file server (S:\Security\ASP).
Operations Director	Partial — operational sections	Security-relevant ops procedures only.
IT Manager	Full — digital (server admin)	Has server-level access to all files including ASP.
TSA Federal Security Director	Full — TSA's own copy	Maintained separately by TSA.
Security Officers (5)	Partial — procedures relevant to post	Receive extracts during training. Should not have full document.
Former Security Supervisor (Ray Delgado — terminated 3 weeks ago)	ACCESS REVOKED — but previously had full digital access	Terminated for policy violations. Departure was contentious. Badge deactivated. File server access removed on last day.