FTA

FEDERAL TRANSIT ADMINISTRATION

Federal Oversight of Transit Security

Bonnie Graves, Attorney-Advisor
FTA Office of Chief Counsel
APTA Legal Affairs
February 26, 2018

U.S. Department of Transportation
Federal Transit Administration

Statutory Authority

- The Aviation and Transportation Security Act (2001) designated TSA as the primary federal agency responsible for securing all modes of transportation.
- The Implementing Recommendations of the 9/11 Commission Act of 2007.
- FTA appropriations acts beginning in FY 2005: *Provided further*, That none of the funds provided or limited in this Act may be used to create a permanent office of transit security under this heading

State Safety Oversight

- 49 CFR part 659
  - Requires system safety program plan
  - Requires separate system security plan
  - Sunsets April 15, 2019
- 49 CFR part 674
  - Removes system security plan requirement
  - Change "does not preclude RTAs from implementing measures securing their assets, [however] it is no longer the responsibility of the SSOAs to oversee those measures."

Memorandum of Understanding

- 2004: MOU between DOT and DHS – DHS has primary responsibility for transportation security, and DOT plays a supporting role.
- Parties will work cooperatively to develop an integrated system of regulations providing for a safe, efficient, and secure transportation system.
- Parties cooperate in sharing intelligence, security, law enforcement, and threat information affecting transportation.

MOU Transit Annex 2015

- 2015 Transit Annex: Supersedes 2005 Annex
- Supports information sharing to enhance public transportation security
- Parties will coordinate on program activities that support risk management
- TSA and FTA will consult with each other prior to disseminating security requirements (regulations, orders, directives) for transit agencies
- TSA and FTA will seek early and frequent coordination in the development of standards, regulations, guidelines, or directives.

TSA Activities

- Administers Transit Security Grant Program
- TSA conducts regulatory inspections for passenger rail systems
- TSA conducts non-regulatory security assessments and training in which transit agencies participate on a voluntary basis
  - Baseline Assessment for Security Enhancement
  - Risk Mitigation Activities for Surface Transportation

TSA Regulations - Transit

- 49 CFR part 1520 – Protection of Sensitive Security Information (SSI)
- 49 CFR part 1570 – General Rules
- 49 CFR part 1580 – Rail Transportation Security
  - Subpart C
    - 1580.201, Rail Security Coordinator
    - 1580.203, Reporting Significant Security Concerns

Part 1570 – General Provisions

- Each owner/operator must allow TSA, at any time or place, to make any inspections or tests to determine compliance with 49 CFR parts 1520 and 1580
- At the request of TSA, each owner/operator must provide evidence of compliance with parts 1520 and 1580, including copies of records.

Part 1580 – Rail Transit Security

- Applies to passenger railroad carriers operating on track that is part of the general RR system, including intercity and commuter rail service, as well as the host railroad.
- Applies to rail transit systems not operating on the general railroad, including heavy rail, light rail, automated guideway, cable car, inclined plane, funicular, and monorail systems.

Part 1580 – Rail Security Coordinator

- Each entity must designate an RSC and an alternate, both of whom must be appointed at the corporate level.
- Each entity must provide the RSC and alternate name, title, and contact information to TSA, and must notify TSA within 7 calendar days if this information changes
- The RSC:
  - is the primary contact for intelligence information and security-related communication with TSA.
  - Must be available 24/7
  - Coordinates security practices and procedures with appropriate law enforcement and emergency response agencies.

Part 1580 – Reporting Significant Security Concerns

- Each entity must immediately report to DHS potential threats and significant security concerns, to include:
  - Interference with the train or crew,
  - Bomb threats
  - Reports or discovery of suspicious items that result in the disruption of rail operations
  - Indications of tampering with passenger rail cars or rail transit vehicles

Part 1520 – Sensitive Security Information

- 49 CFR part 1520 issued as an interim final rule in 2004
- DOT issued identical regulatory standards at 49 CFR part 15 "in order to promote the efficiency and effectiveness of the regulation, as well as ease of compliance."
- Sensitive Security Information" (SSI) is defined by 49 CFR § 15.5 and 49 CFR § 1520.5 as sensitive but unclassified information obtained or developed in the conduct of security activities, including research and development, the unauthorized disclosure of which constitute an unwarranted invasion of privacy, reveal trade secrets or privileged or confidential information, or be detrimental to the security of transportation.

Types of SSI

- By regulation, SSI includes 16 types of records. See 49 CFR 1520.5 The types listed below apply to transit agencies:
  - Security programs and contingency plans issued, established, required, received, or approved by DOT or DHS,
  - Vulnerability assessments that are directed, created, held, funded, or approved by DOT or DHS, or that will be provided to either agency in support of a Federal security program, and
  - Threat information held by the Federal government concerning transportation, transportation systems, and cyber infrastructure, including sources and methods used to gather or develop the information.
- 49 CFR 15.3 and 49 CFR 1520.3 define a record as "any means by which information is preserved, irrespective of format, including a book, paper, drawing, map recording, tape, film, photograph, machine-readable material, and any information stored in an electronic format. The term record also includes any draft, proposed, or recommended change to any record."

Applicability of SSI Rules

- DOT's SSI rules, policy and apply to all DOT employees and to all DOT contractors, grantees, consultants, licensees, and regulated entities that have access to or receive SSI.
- Such employees, individuals, persons, entities, and organizations are subject to the safeguarding and non-disclosure restrictions of 49 CFR Part 15. They are referred to as "covered persons," and that term includes all persons employed by, contracted to, or acting for a covered person, as well as persons formerly in such positions.
- All DOT contracts, grants, and consulting agreements that will result in access to SSI must include provisions for handling and protecting SSI as specified in the policy and procedures, and be consistent with 49 CFR part 15.

Accessing SSI

NEED TO KNOW

- Perform official duties, for example, pursuant to a contract or grant.
- Requires access in order to
  - carry out transportation security activities, or when in training to carry out transportation security activities
  - Supervise or otherwise manage individuals carrying out transportation security activities

  When those activities are approved, accepted, funded, recommended, or direct by DHS or DOT
- When the person needs the information to provide technical or legal advice to a covered person regarding transportation security requirements of Federal law, or to represent a covered person in connection with a judicial or administrative proceeding regarding those requirements.

COVERED PERSON

- Persons who have access to SSI.
- Persons employed by, contracted to, or acting for a covered person, including a grantee of DHS or DOT, and persons formerly in such a position.
- Persons for whom a vulnerability assessment has been directed, created, held, funded, or approved by the DOT, DHS, or who have prepared a vulnerability assessment that will be provided to either agency in support of a Federal security program.
- Each industry trade association that represents covered persons and has entered into a non-disclosure agreement with the DHS or DOT.

Identifying and Designating SSI

Identification

- Does the public need to know this information?
- Is the same or similar information readily available from other sources?
- Could someone intent on causing harm misuse the information?

Designation

- Base designation of SSI on the regulatory definition and types of SSI listed in 49 CFR Parts 15 and 1520.
- Do not designate as SSI information relating to the environment, safety, or health unless security requirements significantly outweigh the public's need to know.
- Do not designate records as SSI out of convenience or a desire to keep them private.
- Do not designate records as SSI in order to conceal or delay the discovery of regulatory violations, errors, or inefficiencies; to avoid embarrassment; or to restrain competition.
- Ensure record-holders of records designated as SSI are notified of the categorization, and ensure the SSI can be uniformly protected. The individual or committee making the designation is responsible for notifying holders.

Marking SSI

- SSI records in both printed and electronic form must be marked as follows:

SENSITIVE SECURITY INFORMATION

- And must include the distribution limitation statement specified in the regulation:

Warning: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

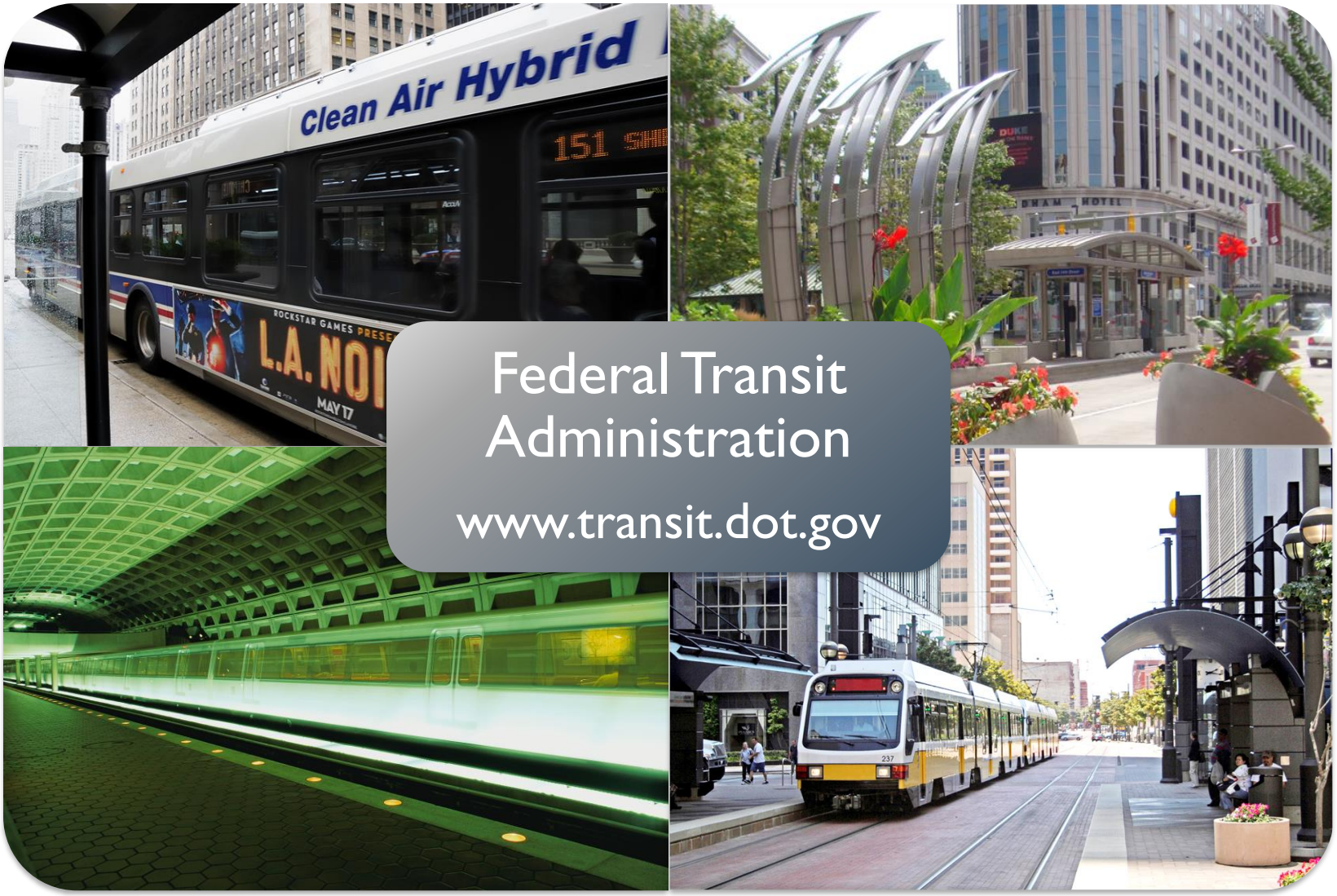
Controlling SSI

- Holders of SSI must take reasonable steps to safeguard SSI from unauthorized disclosure.
- This means controlling SSI during storage, use, reproduction, transmittal, and destruction.
- During use, SSI records should not be left out in the open.
- SSI records may be reproduced only to the extent necessary to carry out transit agency business.
- SSI can be sent to "known" persons, addresses, or locations on the basis of the receiver's "need to know."
- When a covered person becomes aware that SSI has been released to unauthorized persons, the covered person must promptly notify TSA or FTA.

Unauthorized Disclosure and Destruction of SSI

- Unauthorized Disclosure: Violation of part 1520 is grounds for a civil penalty and other enforcement or corrective action by DHS, and appropriate personnel actions for Federal employees. Corrective action may include issuance of an order requiring retrieval of SSI to remedy unauthorized disclosure or an order to cease future unauthorized disclosure.

- Destruction of SSI: 1520.19(b)(1): A covered person must destroy SSI completely to preclude recognition or reconstruction of the information when the covered person no longer needs the SSI to carry out transportation security measures.
- Exception. Paragraph (b)(1) of this section does not require a State or local government agency to destroy information that the agency is required to preserve under State or local law.



Federal Transit Administration

www.transit.dot.gov