# Critical Infrastructure and Security Sensitive Information


**Presentation made by:**

**Allen Miller, Senior Manager, Commuter Rail**

**Michael Meader, Chief Safety Officer and AGM of Safety and Security**

**Robert Grado, Chief of Police**

**Linda Buss, Senior Manager, Information Governance**

**Marisela Sandoval, Assistant General Counsel**

# What is CSSI?

# PCII & SSI

- **Protected Critical Infrastructure Information (PCII) –** information that is not customarily in the public domain and is related to the security of critical infrastructure or protected systems

- **Security Sensitive Information (SSI) –** information that if released publically, would be detrimental to transportation security

# Why We All Need To Care

## September 10, 2001

# Why We All Need To Care

## September 11, 2001

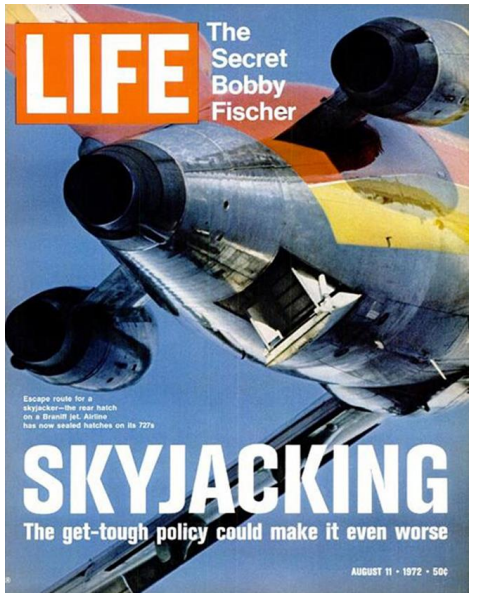
# Why We All Need To Care

- **September 11, 2001 and the collapse of the World Trade Towers was a direct result of architectural and engineering plans available to the general public**

- **With this information, terrorists pinpointed the vulnerability of the building's design and made targeting the weakness a possibility and ultimately a reality.**

# Historical Perspective

- SSI was developed as part of the *Air Transportation Security Act of 1974*
  - Required FAA to establish regulations for sharing SSI with airlines and airports
  - Direct response to the hijackings in the early 1970s




- SSI and PCII were applied to all modes of transportation after 9/11

# Based on Federal Law

## SSI

- Protected by Federal Regulations 49 C.F.R. Parts 15, 1520, 1580
- Protects security sensitive information related to transportation security
- Unauthorized SSI disclosure may result in civil penalty

## PCII

- The Protected Critical Information Act of 2002
- Protects private sector infrastructure information voluntarily shared with government
- PCII cannot be disclosed through a Freedom of Information Act (FOIA) request or in civil litigation

# Who decides what is protected?

## SSI

- Transportation security stakeholders determine what is SSI using regulations and guidelines
- Must mark as SSI

## PCII

- Submit to Department of Homeland Security
- Information is protected once validated and marked

# Who can access PCII?

## SSI

- "Covered persons": transportation officials and employees with a need to know, contractors, and stakeholders such as cities who have an identified need to know

## PCII

- "Covered persons": authorized and trained individuals with direct need to know, including transportation officials and employees and contractors

# Responsibilities of Those Covered

## SSI

- Must have appropriate understanding and awareness and have “need”
- Must safeguard SSI
  - Lock it up and ensure it is secure when not in use. This includes going to lunch, end of day, etc.

## PCII

- Must be authorized and trained in the proper handling and safeguarding
- Must have homeland security responsibility
- Must sign a non-disclosure agreement

# RTD Today

- **103.4 *million*** annual boardings
- **339,300** average weekday boardings
  - **1,634** rolling stock vehicles
  - **1,201** buses
  - **172** light rail vehicles
  - **66** commuter rail cars
  - **323** Access-a-Ride vehicles
- **137** scheduled routes
- **9,751** bus stops

- **48** light rail track miles
- **74** Park-n-Rides
- Over **2,734** employees
- FasTracks
  - **93.4** miles of commuter rail
  - **28.2** miles of light rail
  - **18** miles of bus rapid transit
  - **21,000** parking spaces
  - Denver Union Station
  - Denver International Airport Station
  - More than **$5 billion** in projects currently under construction

# Policy Impact on RTD

Departments affected by SSI and PCII Policy:

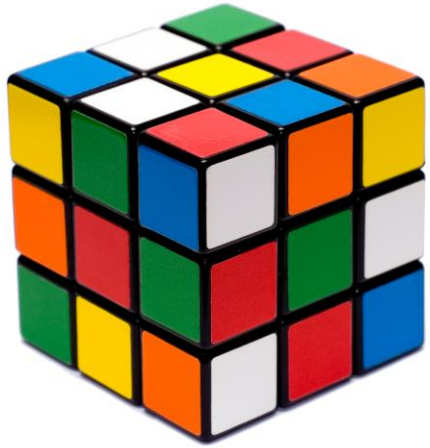
- Safety and Security
- Information Governance
- Legal
- Capital Programs/Engineering
- Operations and Maintenance
- Planning
- Communications
- ***ALL DEPARTMENTS!***

Others indirectly or directly affected by SSI and PCII Policy outside RTD:

- Contractors
- Stakeholders – Municipalities, Cities, County and State
- CDOT
- Chambers of Commerce
- Public Action Groups
- ***EVERYONE!***

# Key Challenges to Implementing An Effective CSSI Policy

- Identifying those responsible for developing and implementing the policy
- Identifying affected divisions, departments and 3rd parties
- Developing training and educated staff on the need and importance of protecting the information
- Implementing an broad policy that affects ALL of RTD



# Keys to a Successful Policy

- Identifying the keeper of the policy
- Developing a standing committee whose membership is from all departments led by safety and security with the authority to act, implement, and improve, enshrined within the policy
- Education through online training and handouts
- Getting buy-in and having staff take ownership

# Questions?