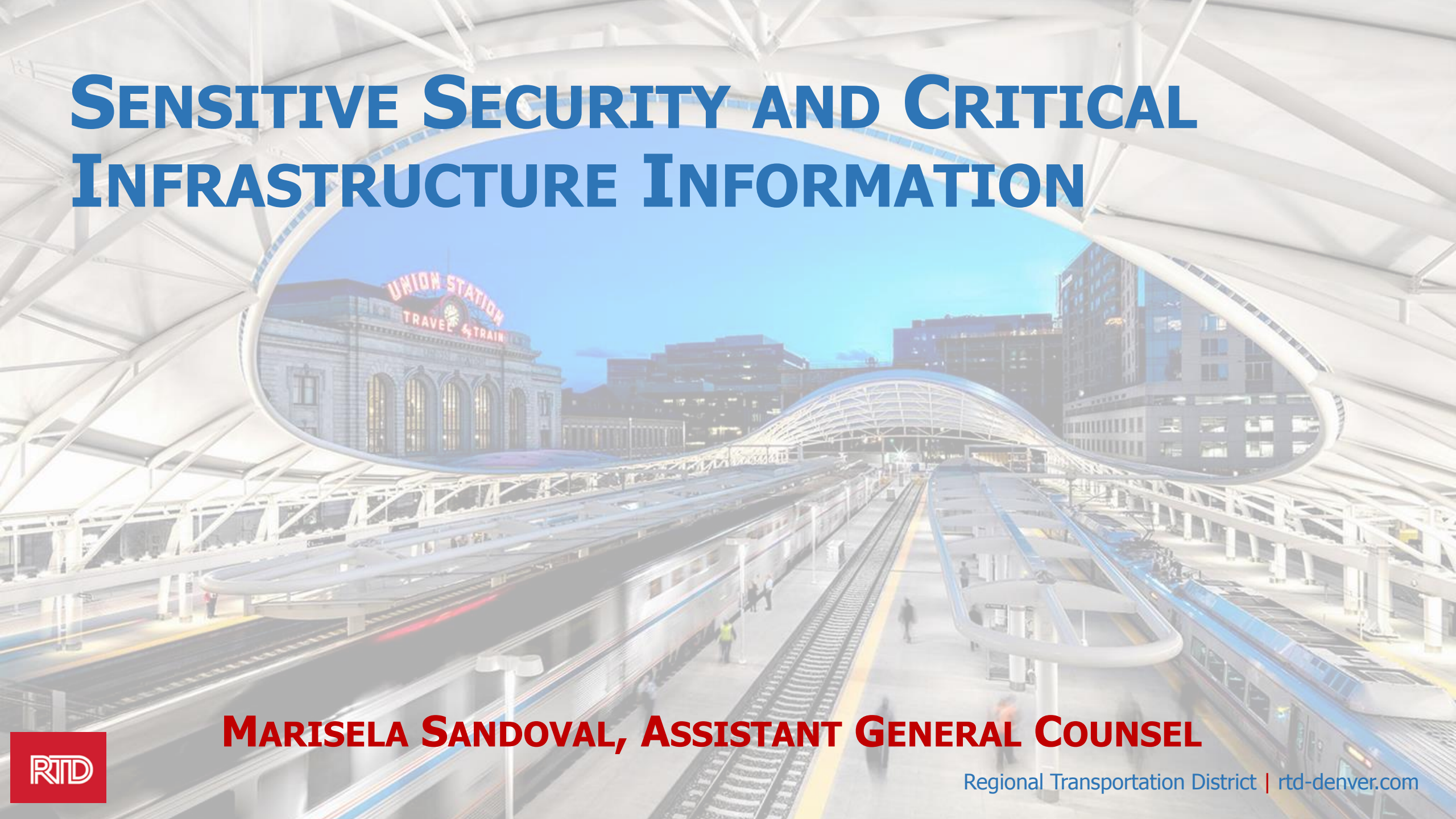
Sensitive Security and Critical Infrastructure Information



Marisela Sandoval, Assistant General Counsel

Regional Transportation District | rtd-denver.com

what is **SENSITIVE SECURITY INFORMATION?**

Sensitive Security Information (SSI)

- Information that, if released publicly, would be detrimental to transportation security
  - Transit system design configurations: architectural drawings and engineer schematics; critical assets; and network topology maps
  - Emergency procedures

what is **CRITICAL INFRASTRUCTURE INFORMATION?**

Critical Infrastructure Information (CII)

- Physical and cyber systems and assets that are so vital that their incapacity or destruction would be debilitating to physical or economic security or public health or safety

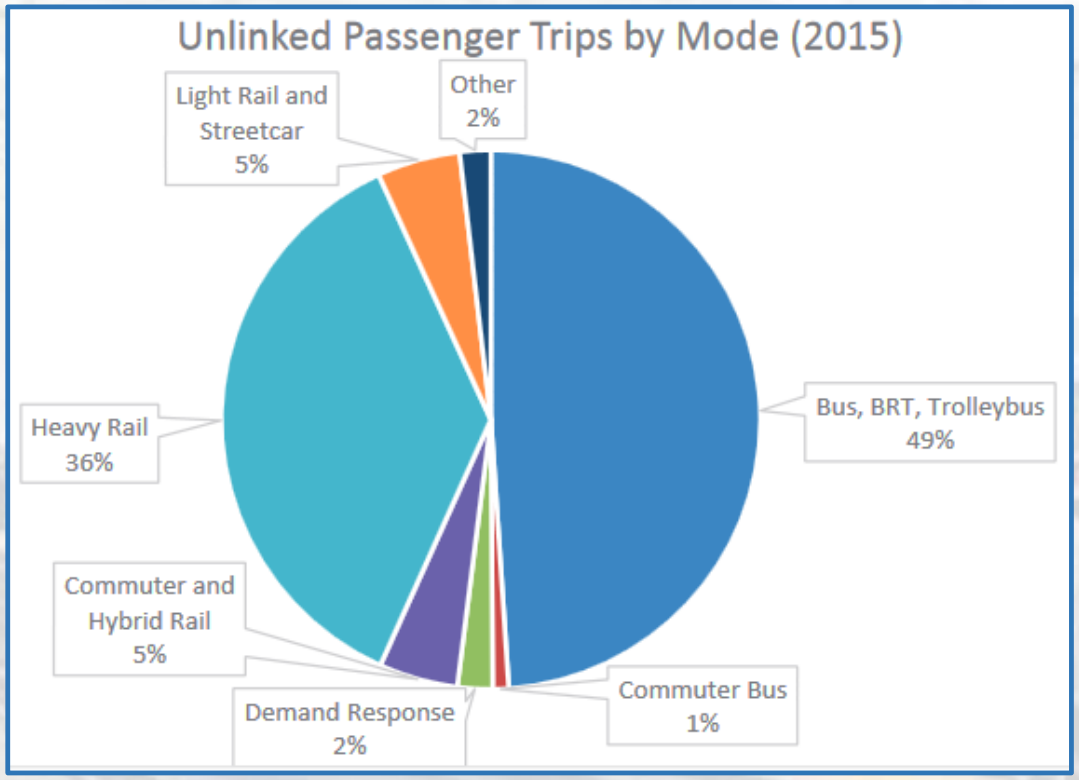
- Information that is not customarily in the public domain
  - Cybersecurity risks and incidents, vulnerability assessments of critical infrastructure, threat assessments of critical infrastructure or protected systems by physical or computer based attacks

- Once submitted to DHS, CII becomes PCII

why should we **CARE?**

Public Safety

- 10.59 billion unlinked total passenger trips
- 58.6 billion total passenger miles traveled
- 360.3 million hours of revenue service
- 6,700 organizations providing public transportation
- 147,186 railcars, buses, and vans operating in typical peak period



Source: APTA, 2017 Public Transportation Fact Book, 68 ed., March 2018

Runaway Boston Train Stokes Hacking Fears

December 10, 2015

"Massachusetts Governor Charlie Baker told reporters that it appeared that the controls had been manipulated and that the Department of Transportation and the MBTA are investigating the incident."

Barb Darrow, Fortune, http://fortune.com/2015/12/10/runaway-train-hacking-fears/

Ransomware attack hit San Francisco train system

November 28, 2016

"A ransomware attack took ticket machines for San Francisco's light rail transit system offline all day Saturday during one of the busiest shopping weekends of the year."

Ken Townsend, Security Week, https://www.securityweek.com/ransomware-attack-disrupts-san-francisco-rail-system

Iranian Hackers Claim Cyber Attack on New York Dam

December 25, 2015

"An Iranian hactivist group has claimed responsibility for a cyberattack that gave it access to the control system for a dam in the suburbs of New York."

Tracy Connor, *et al.*, NBC News, https://www.nbcnews.com/news/us-news/iranian-hackers-claim-cyber-attack-new-york-dam-n484611

Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say

July 6, 2017

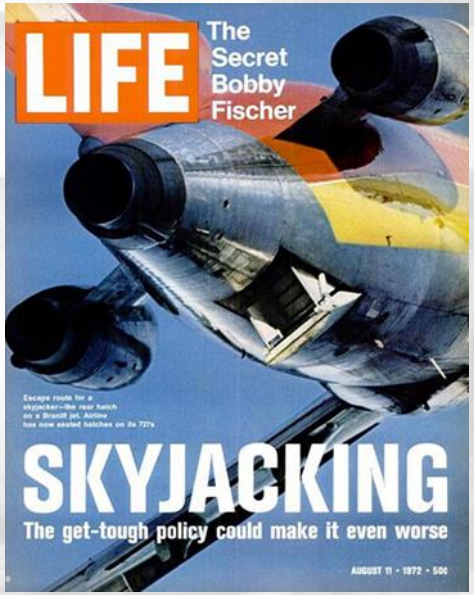
"Since May, hackers have been penetrating the computer networks of companies that operate nuclear power stations and other energy facilities, as well as manufacturing plants in the United States and other countries."

Nicole Perlroth, N.Y. Times, https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html

the history of **SSI and PCII**

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 applies to all modes of transportation after 9/11
- PCII was created in 2002 under CII Act



what are the protections for **SSI and PCII** based on?

Based on Federal Law

SSI

- Protected by Federal Regulations, 49 C.F.R. Parts 15, 1520, 1580
- Protects sensitive security information related to transportation security

PCII

- Protected by Federal Regulation, 6 C.F.R. Part 29
- Protects private sector infrastructure information voluntarily shared with government

Federal Law and State and Local Transportation Agencies, Organizations, and Districts

SSI

- Applies to Department of Transportation (DOT) and Department of Homeland Security (DHS) grantees
- Rail transit systems

PCII

- Voluntary submission of information to DHS
- Secure sharing of CII to promote protection of CI
- In exchange, information is protected

Who is responsible for protecting **SSI and PCII**?

Everyone is Responsible

- Everyone is responsible for properly marking, handling, protecting, storing, and destroying SSI and PCII

how should
SSI and PCII
be protected?

❶ Use Federal Regulations and Guidelines

- Requirements listed in SSI (49 C.F.R. Parts 15, 1520, 1580) and PCII (6 C.F.R. Part 29) Federal Regulations
- Guidelines
  - Best Practices Guides
  - Program Procedures Manual

❷ IDENTIFY SSI AND PCII

SSI

- Use the SSI Federal Regulations for guidance
- Consider:
  - Potential effect on transit operations and infrastructure
  - Safety requirements for transit operations
  - Federal and state regulatory requirements

PCII

- Consider:
  - How it relates to critical infrastructure
  - Whether or not information is in the public domain
- Submit CII to DHS to receive protection
- DHS will decide whether to mark information as PCII

❸ Limit Access to SSI and 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

❸ Limit Access to SSI and PCII

SSI

- Managers, employees, and contractors who need to access SSI in order to:
  - Perform official duties;
  - Carry out transportation security activities sanctioned by DHS or DOT;
  - Supervise individuals carrying out security activities sanctioned by DHS or DOT; or
  - Provide technical or legal advice about federal transportation security requirements.

PCII

- Managers, employees, and contractors who need know and:
  - Complete PCII Authorized User Training;
  - Have homeland security responsibilities; and
  - Sign a non-disclosure agreement.

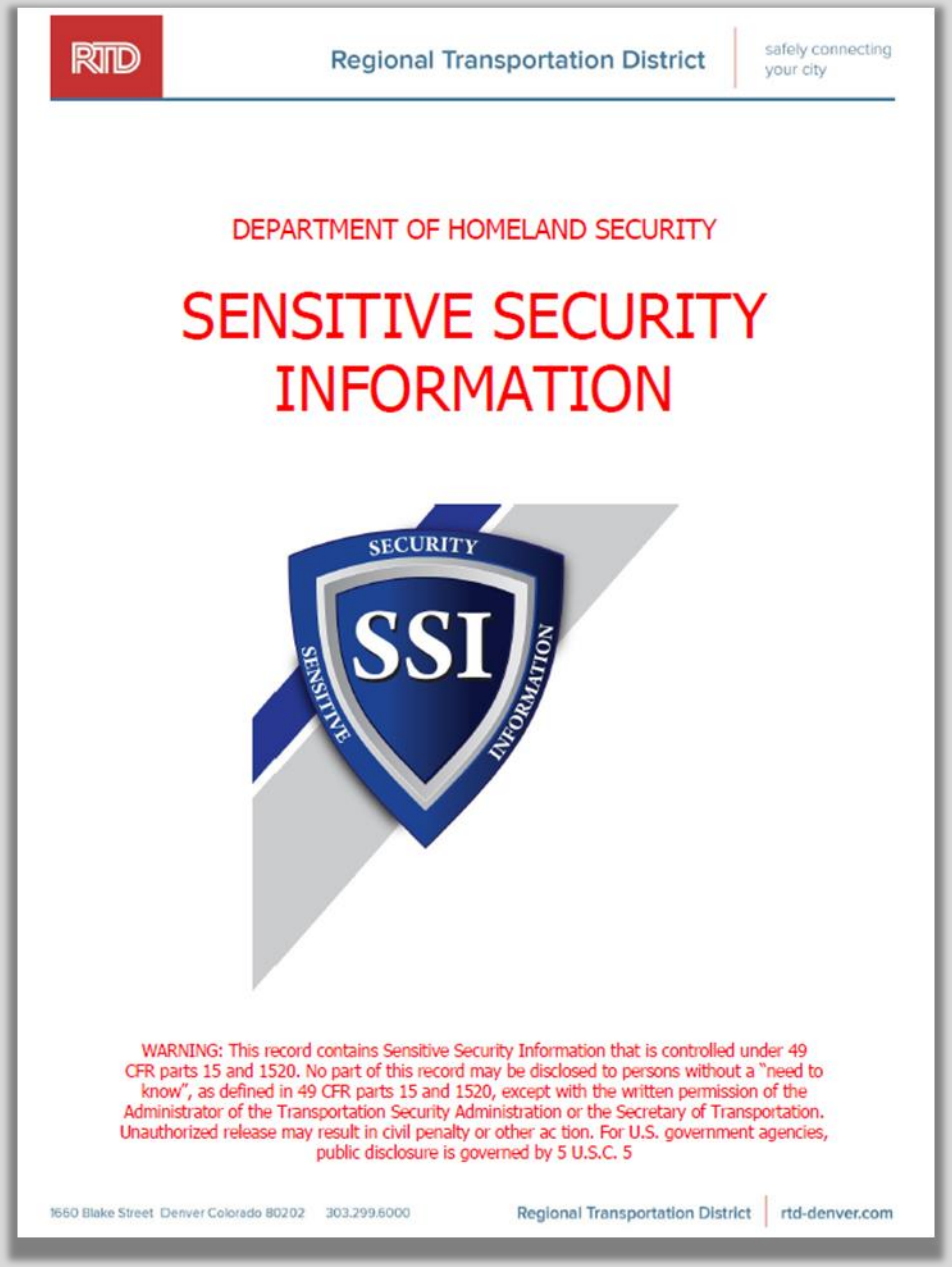
❹ Mark SSI and PCII

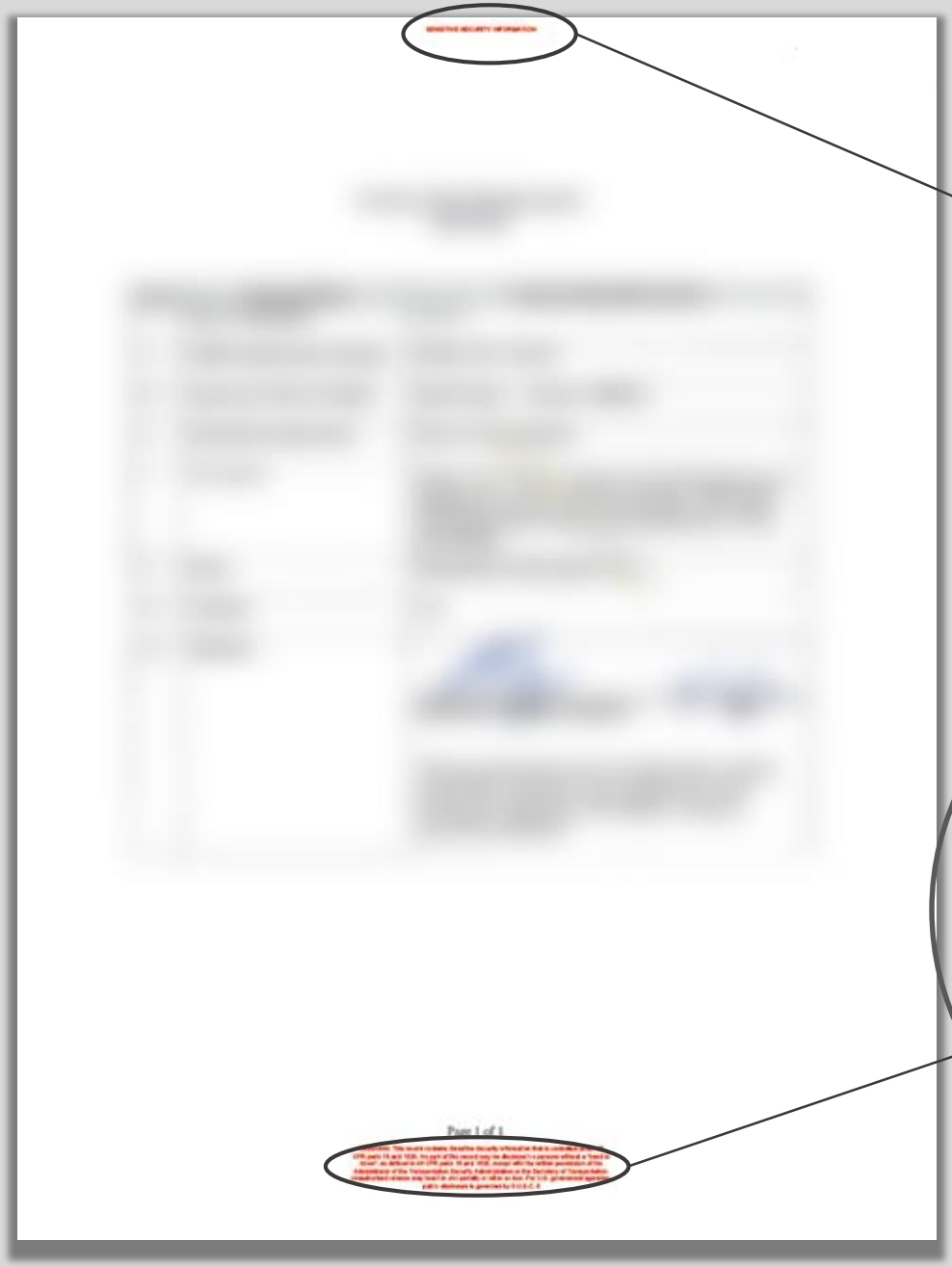
SSI

- Must be conspicuously marked after a determination is made
- "SSI" and distribution limitation statement must appear on all pages of document

PCII

- Only DHS may mark
- If information is not marked by DHS, it is not PCII.
- "PCII" and distribution limitation statement must appear on all pages of document


RTD
Regional Transportation District
safely connecting your city
DEPARTMENT OF HOMELAND SECURITY
SENSITIVE SECURITY INFORMATION
SECURITY
SSI
SENSITIVE
INFORMATION
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 ac tion. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 5
1660 Blake Street Denver Colorado 80202 303.299.6000
Regional Transportation District
rtd-denver.com



SENSITIVE SECURITY INFORMATION

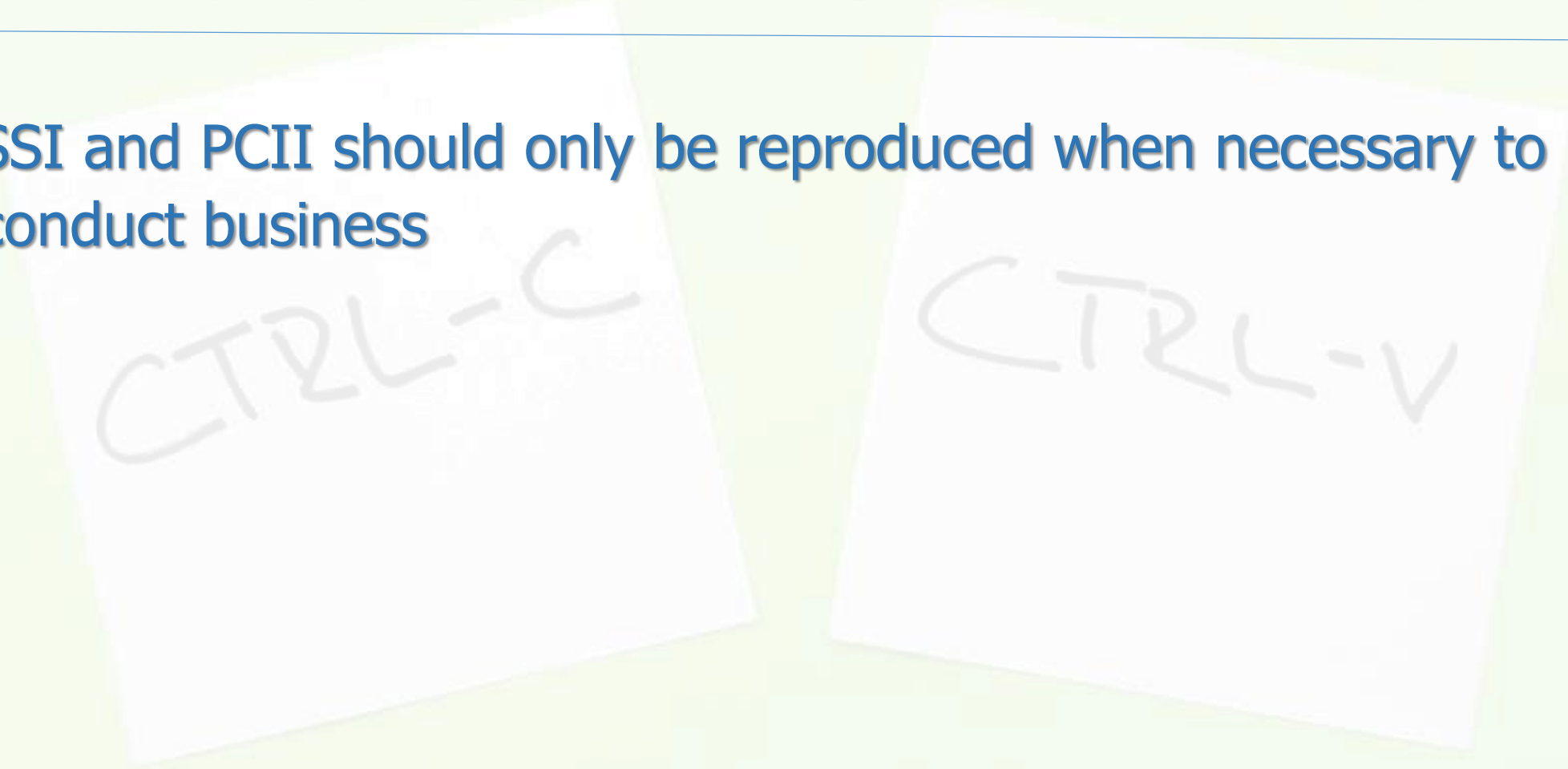
WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation 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.

❺ Handle and Use SSI and PCII with Care

- Ensure only persons with "need to know" handle and access
- Take any and all reasonable steps to prevent unauthorized disclosure
- Maintain vigilance when handling or discussing
- Use best judgment

❻ Reproduce SSI and PCII When Necessary

- SSI and PCII should only be reproduced when necessary to conduct business



7 Securely Transmit SSI and PCII

Email: SSI and PCII content should be placed in password-protected attachment to an email, password should be sent in a separate email

Mail: by U.S. First Class mail or traceable delivery service using opaque envelope

Interoffice mail: unmarked, opaque, sealed envelope

Fax: verify fax number, ensure intended recipient will promptly retrieve fax with SSI or PCII

❽ Disclose SSI and PCII Wisely

SSI

- Should generally not be available for public inspection or copying
- May redact "SSI" before disclosing per an open records act request

PCII

- Must not be available for public inspection or copying
- Must not disclose per an open records request
- Must not share with those who are not authorized PCII users
- Otherwise receive consent of DHS

❾ Disclose SSI and PCII Wisely

- Ensure SSI is protected when shared with third parties
  - Contractors, other government entities, etc.
- Use Non-Disclosure Agreements
- Collect SSI from third party when it is no longer needed or ensure third party destroys SSI

❽ Safely Store SSI and PCII

- Store in locked cabinets, rooms or receptacles
- Protect electronic SSI and PCII with passwords with that are known only by those with need to know
- Avoid removing SSI or PCII from workplace unless it is business necessary

⑩ Destroy SSI and PCII When Finished

- SSI and PCII should be destroyed using a method that prevents unauthorized retrieval
- Paper documents: shredding or incineration
- Electronic documents: any method precluding recognition or reconstruction

what are the consequences of failing to protect **SSI and PCII**?

Consequences of Unauthorized Disclosure

SSI

- Civil penalties (fines)
- Enforcement or corrective action by DOT/DHS
- Appropriate personnel actions for employees

PCII

- Fines up to $250,000
- Imprisonment for up to one year
- Termination
- Disqualification or removal from PCII program

ENDANGERING PUBLIC SAFETY


how are others protecting
SSI and PCII?

Steps to Protect SSI and PCII

- RTD recently adopted a procedure
- Developed by several departments
- Responsible department:

  Safety, Security & Asset Management
- Created a committee with representatives from the following departments:
  - Capital Programs
  - General Counsel
  - Finance
  - IT
  - Planning
  - Communications
  - Safety and Security
  - Bus Operations
  - Rail Operations

RTD Regional Transportation District — safely connecting your city

Procedure Name:	Sensitive Security Information and Protected Critical Infrastructure Information Procedure				
Procedure #:	RTD-SSA-PRC-0001	Adopted:	2018-04-16	Current Version	A
Revised:		Last review date			
Assistant General Manager Approval:	Michael S. Meader				
Division Manager Approval:					
Responsible Department:	Safety, Security & Asset Management				

1. PURPOSE AND SCOPE

1.1. This Sensitive Security Information and Protected Critical Infrastructure Information Procedure (the "Procedure") addresses the protection of Sensitive Security Information ("SSI," as further described in Section 2.1 below) and Protected Critical Infrastructure Information ("PCII," as further described in Section 2.2 below). Generally, SSI and PCII ("SSI/PCII") is information about the security, operations, facilities, critical infrastructure, and/or other assets or capital projects which disclosure would be detrimental to the security of RTD operations, infrastructure, employees, or customers. Federal law requires that RTD categorize and protect SSI/PCII. SSI/PCII is not subject to disclosure under the Freedom of Information Act ("FOIA") or the Colorado Open Records Act ("CORA"). SSI/PCII is also not available under discovery in litigation and is not required to be part of the record in federal rulemaking.

1.2. This Procedure is intended to assist RTD in identifying SSI/PCII to prevent its unauthorized disclosure, use, or dissemination while also preserving the public's right to know. This Procedure is based on guidance from the Transportation Security Administration ("TSA") and the U.S. Department of Transportation ("DOT"). As further described in Section 4, RTD will use the following factors to determine whether information constitutes SSI/PCII: (i) potential effect on RTD operations and infrastructure, (ii) safety requirements for RTD operations, and (iii) federal and state regulatory requirements.

1.3. This Procedure only governs the protection of SSI/PCII. There may be other reasons for restricting access to information unrelated to its status as SSI/PCII and RTD employees must comply with any other applicable RTD policies governing such information. (See, for example, Section 2.5 below.) RTD Employees with concerns about whether access

Keys to a Successful Policy or Procedure

- Education and awareness
- Communication among all departments
- Collaboration among all departments
- Creation of a committee to:
  - Develop and update policy or procedure
  - Make tough calls
  - Develop training
- Training

TAKEAWAYS

- Be aware of SSI and PCII
- Educate yourself on SSI and PCII
- Identify your organization's SSI and CII
- Protect it!

Thank you

Marisela Sandoval
Assistant General Counsel
Marisela.Sandoval@rtd-denver.com