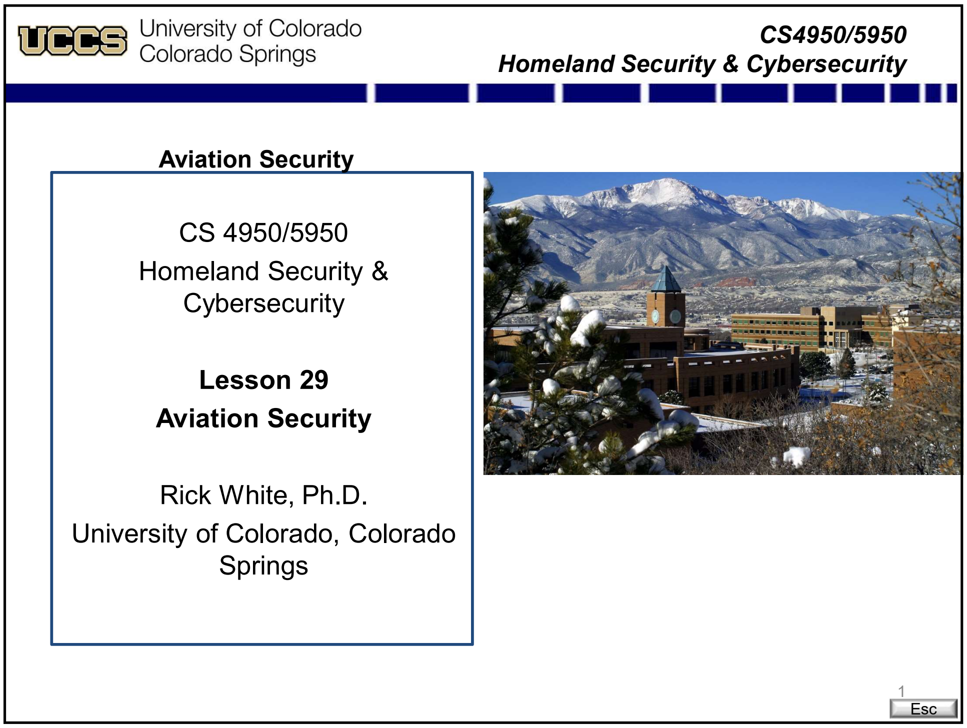


University of Colorado Colorado Springs

CS4950/5950 Homeland Security & Cybersecurity

Aviation Security

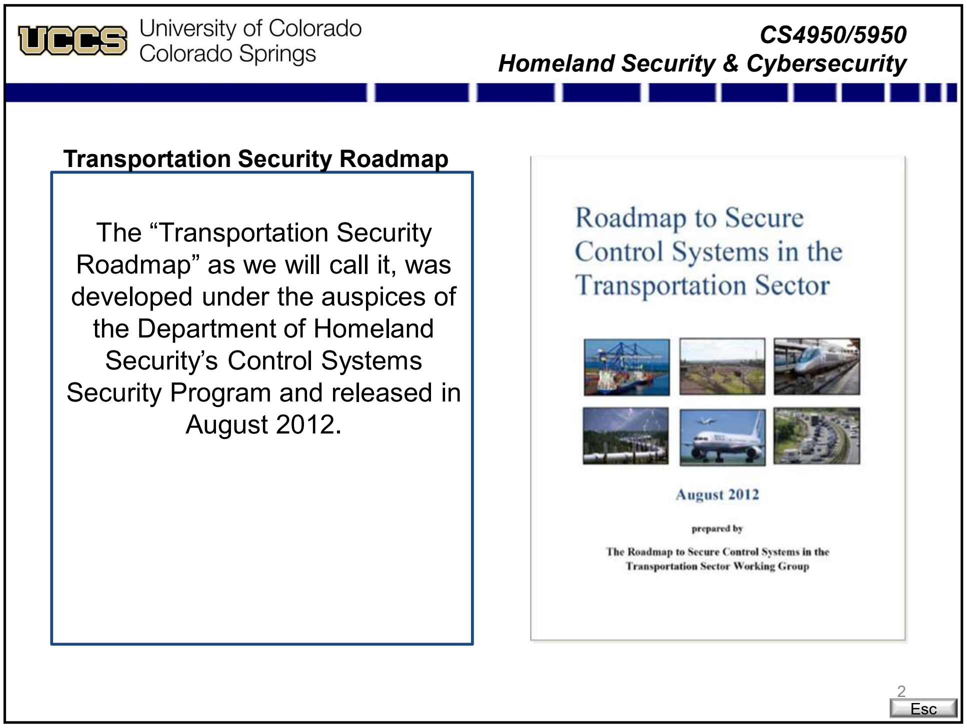
CS 4950/5950
Homeland Security & Cybersecurity

Lesson 29
Aviation Security

Rick White, Ph.D.
University of Colorado, Colorado Springs

1 Esc

1



University of Colorado Colorado Springs

CS4950/5950 Homeland Security & Cybersecurity

Transportation Security Roadmap

The "Transportation Security Roadmap" as we will call it, was developed under the auspices of the Department of Homeland Security's Control Systems Security Program and released in August 2012.

Roadmap to Secure Control Systems in the Transportation Sector

August 2012

prepared by

The Roadmap to Secure Control Systems in the Transportation Sector Working Group

2 Esc

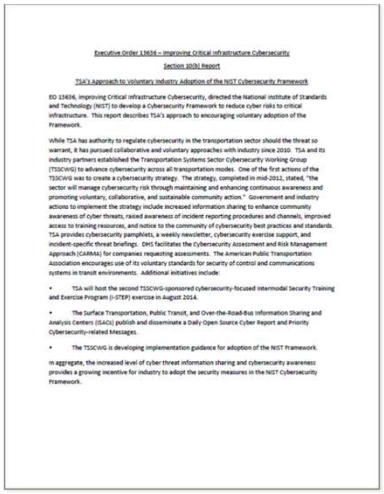
2

University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Transportation Security Roadmap

The Transportation Security Administration cited the Transportation Security Roadmap in its 2014 reply to **Executive Order 13636** saying it provided the basis for improving cybersecurity within the transportation sector in voluntary cooperation with industry.



Executive Order 13636 – Improving Critical Infrastructure Cybersecurity

Section 10(b) Report

TSA's Approach to Voluntary Industry Adoption of the NIST Cybersecurity Framework

EO 13636, Improving Critical Infrastructure Cybersecurity, directed the National Institute of Standards and Technology (NIST) to develop a Cybersecurity Framework to reduce cyber risks to critical infrastructure. This report describes TSA's approach to encouraging voluntary adoption of the Framework.

While TSA has authority to regulate cybersecurity in the transportation sector should the threat so warrant, it has pursued collaborative and voluntary approaches with industry since 2010. TSA and its industry partners established the Transportation Systems Sector Cybersecurity Working Group (TSSCWG) to advance cybersecurity across all transportation modes. One of the first actions of the TSSCWG was to create a cybersecurity strategy. The strategy, completed in mid-2012, stated, "the sector will manage cybersecurity risk through maintaining and enhancing continuous awareness and promoting voluntary, collaborative, and sustainable community action." Government and industry actions to implement the strategy include increased information sharing to enhance community awareness of cyber threats, raised awareness of incident reporting procedures and channels, improved access to training resources, and notice to the community of cybersecurity best practices and standards. TSA provides cybersecurity pamphlets, a weekly newsletter, cybersecurity exercise support, and incident-specific threat briefings. DHS facilitates the Cybersecurity Assessment and Risk Management Approach (CARMA) for companies requesting assessments. The American Public Transportation Association encourages use of its voluntary standards for security of control and communications systems in transit environments. Additional initiatives include:

- TSA will host the second TSSCWG-sponsored cybersecurity-focused Intermodal Security Training and Exercise Program (I-STEP) exercise in August 2014.
- The Surface Transportation, Public Transit, and Over-the-Road-Bus Information Sharing and Analysis Centers (ISACs) publish and disseminate a Daily Open Source Cyber Report and Priority Cybersecurity-related Messages.
- The TSSCWG is developing implementation guidance for adoption of the NIST Framework.

In aggregate, the increased level of cyber threat information sharing and cybersecurity awareness provides a growing incentive for industry to adopt the security measures in the NIST Cybersecurity Framework.

3

Esc

3

University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Transportation Security Roadmap

The Transportation Security Roadmap is broad based, **addressing all modes of transportation** including aviation, highway, maritime, pipeline, and rail.

4

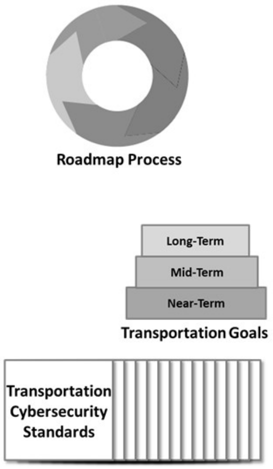
Esc

4

Transportation Security Roadmap

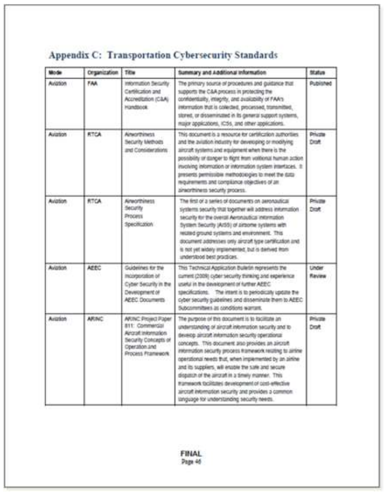
The Transportation Security Roadmap is roughly comprised of three parts:

1. Transportation Cybersecurity Standards
2. Transportation Goals
3. Roadmap Process.



Transportation Security Roadmap

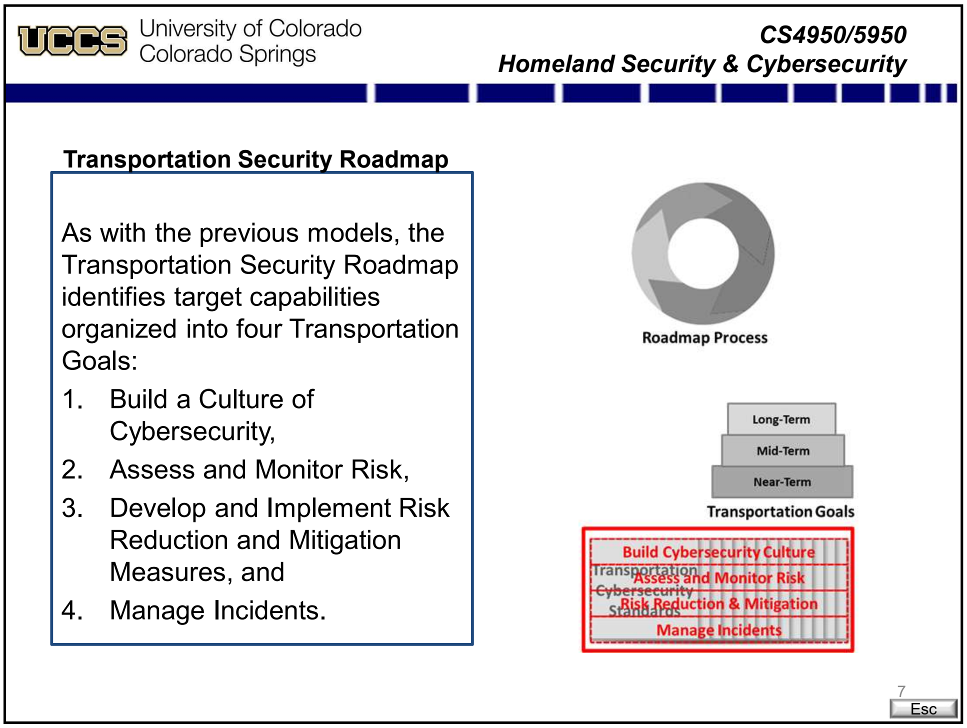
- The Transportation Cybersecurity Standards specific to each transportation mode are listed in Appendix C of the Transportation Security Roadmap.
- **Unfortunately, they are not freely available over the Internet.**



Appendix C: Transportation Cybersecurity Standards

Mode	Organization	Title	Summary and Additional Information	Status
Aviation	FAA	Information Security Certification and Accreditation (C&A) Handbook	The primary source of procedures and guidance that supports the C&A process in protecting the confidentiality, integrity, and availability of FAA's information that is collected, processed, transmitted, stored, or disseminated in its general support systems, major applications, ICSs, and other applications.	Published
Aviation	RTCA	Airworthiness Security Methods and Considerations	This document is a resource for certification authorities and the aviation industry for developing or modifying aircraft systems and equipment when there is the possibility of danger to flight from volitional human action involving information or information system interfaces. It presents permissible methodologies to meet the data requirements and compliance objectives of an airworthiness security process.	Private Draft
Aviation	RTCA	Airworthiness Security Process Specification	The first of a series of documents on aeronautical systems security that together will address information security for the overall Aeronautical Information System Security (AISS) of airborne systems with related ground systems and environment. This document addresses only aircraft type certification and is not yet widely implemented, but is derived from understood best practices.	Private Draft
Aviation	AEEC	Guidelines for the Incorporation of Cyber Security in the Development of AEEC Documents	This Technical Application Bulletin represents the current (2009) cyber security thinking and experience useful in the development of further AEEC specifications. The intent is to periodically update the cyber security guidelines and disseminate them to AEEC Subcommittees as conditions warrant.	Under Review
Aviation	ARINC	ARINC Project Paper 811: Commercial Aircraft Information Security Concepts of Operation and Process Framework	The purpose of this document is to facilitate an understanding of aircraft information security and to develop aircraft information security operational concepts. This document also provides an aircraft information security process framework relating to airline operational needs that, when implemented by an airline and its suppliers, will enable the safe and secure dispatch of the aircraft in a timely manner. This framework facilitates development of cost-effective aircraft information security and provides a common language for understanding security needs.	Private Draft

FINAL
Page 46



UCCS University of Colorado Colorado Springs

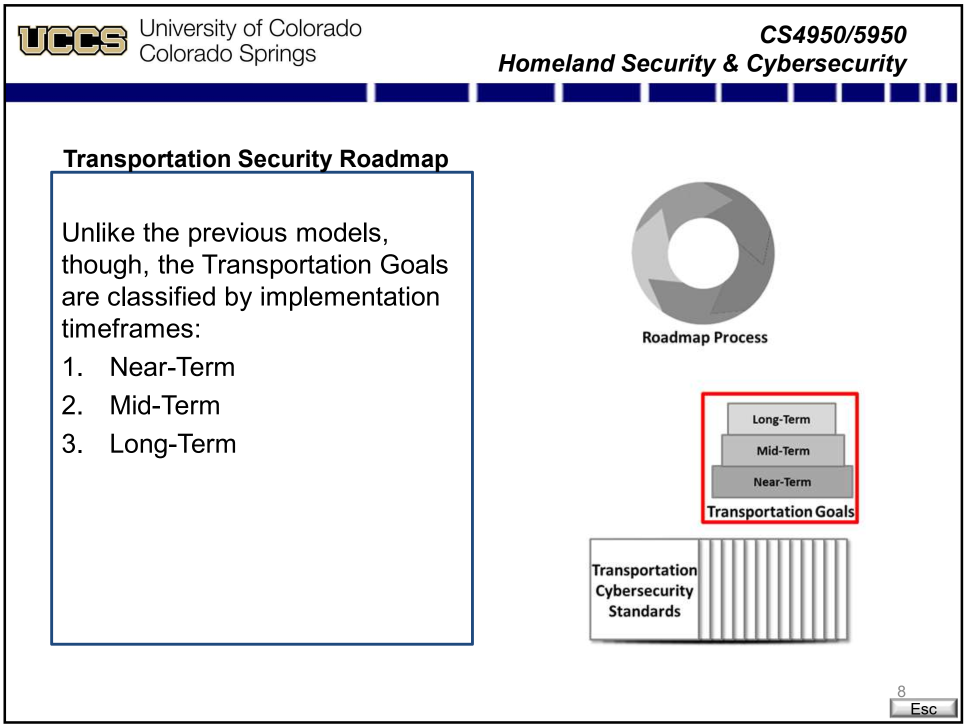
CS4950/5950
Homeland Security & Cybersecurity

Transportation Security Roadmap

As with the previous models, the Transportation Security Roadmap identifies target capabilities organized into four Transportation Goals:

1. Build a Culture of Cybersecurity,
2. Assess and Monitor Risk,
3. Develop and Implement Risk Reduction and Mitigation Measures, and
4. Manage Incidents.

7



UCCS University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Transportation Security Roadmap

Unlike the previous models, though, the Transportation Goals are classified by implementation timeframes:

1. Near-Term
2. Mid-Term
3. Long-Term

Roadmap Process
Long-Term
Mid-Term
Near-Term
Transportation Goals
Transportation Cybersecurity Standards
8
Esc

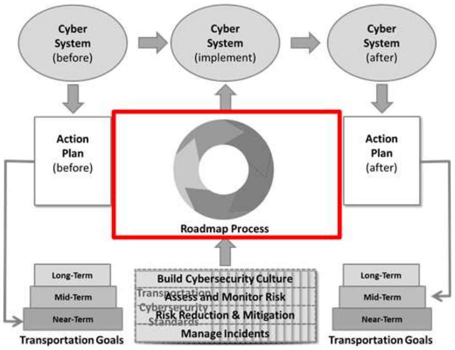
8

University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Transportation Security Roadmap

the Roadmap Process is also similar to the previous models in that it engages all stakeholders inside and outside the organization in a continuous improvement program.



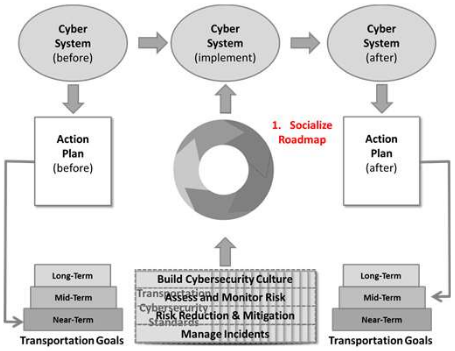
9
Esc

University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Transportation Security Roadmap

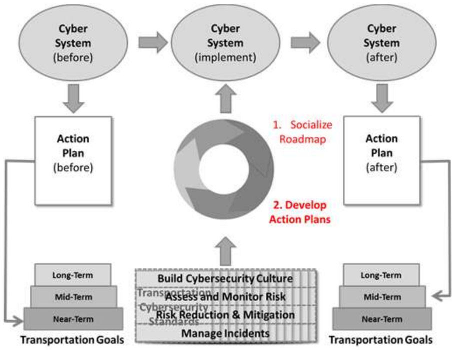
Step 1: Socialize Roadmap and Gain Buy-In.



10
Esc

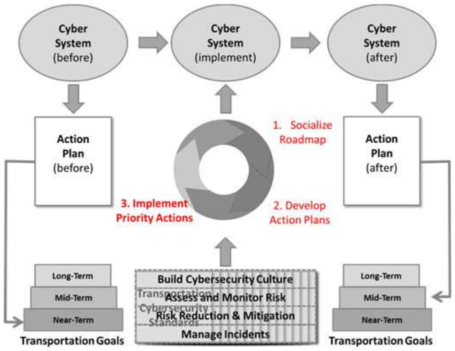
Transportation Security Roadmap

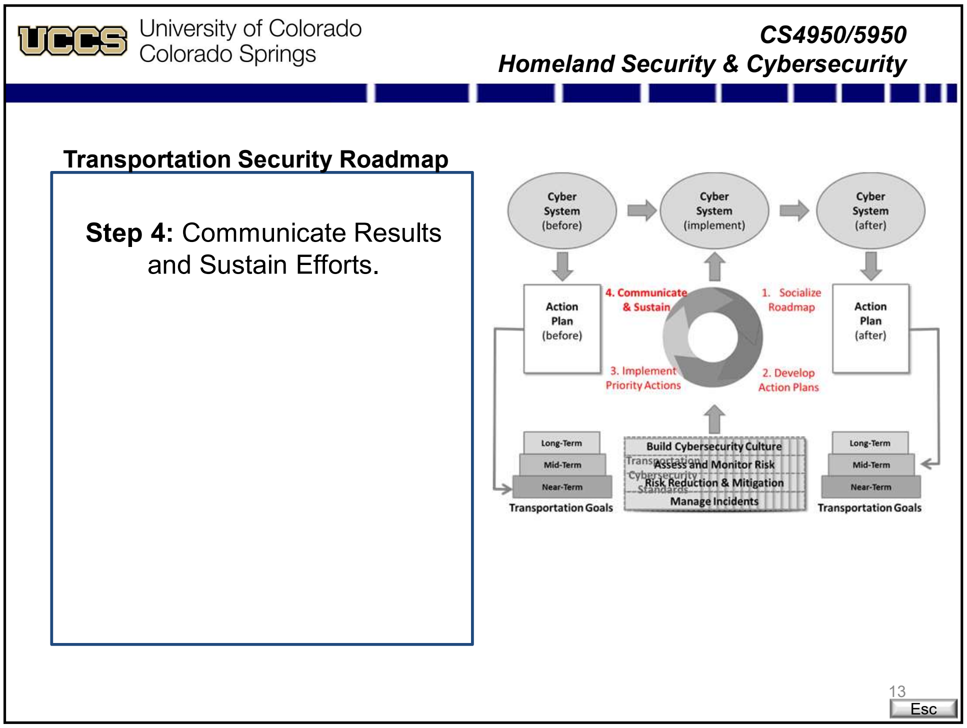
Step 2: Develop Action Plans.



Transportation Security Roadmap

Step 3: Implement Priority Actions.





University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

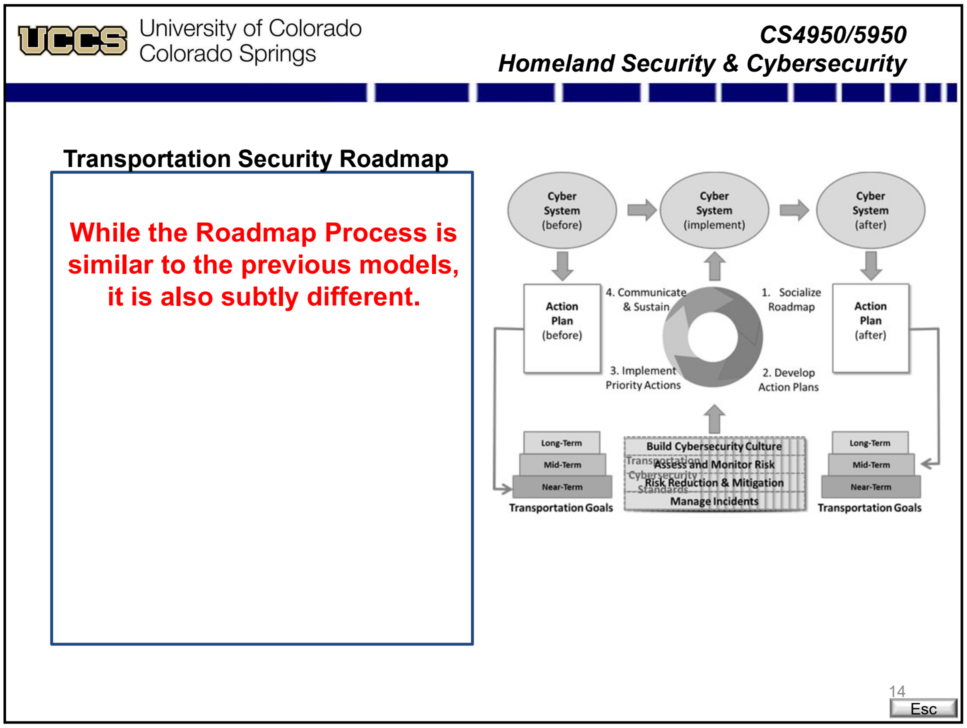
Transportation Security Roadmap

Step 4: Communicate Results and Sustain Efforts.

13

Esc

13



University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

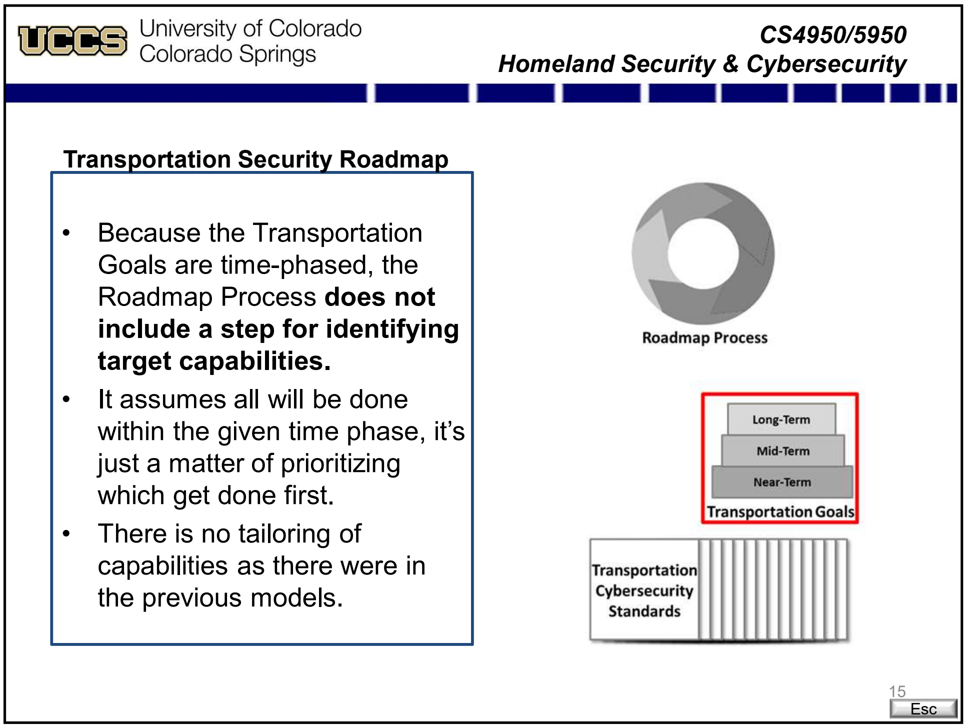
Transportation Security Roadmap

While the Roadmap Process is similar to the previous models, it is also subtly different.

14

Esc

14



University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Transportation Security Roadmap

- Because the Transportation Goals are time-phased, the Roadmap Process **does not include a step for identifying target capabilities.**
- It assumes all will be done within the given time phase, it's just a matter of prioritizing which get done first.
- There is no tailoring of capabilities as there were in the previous models.

Roadmap Process

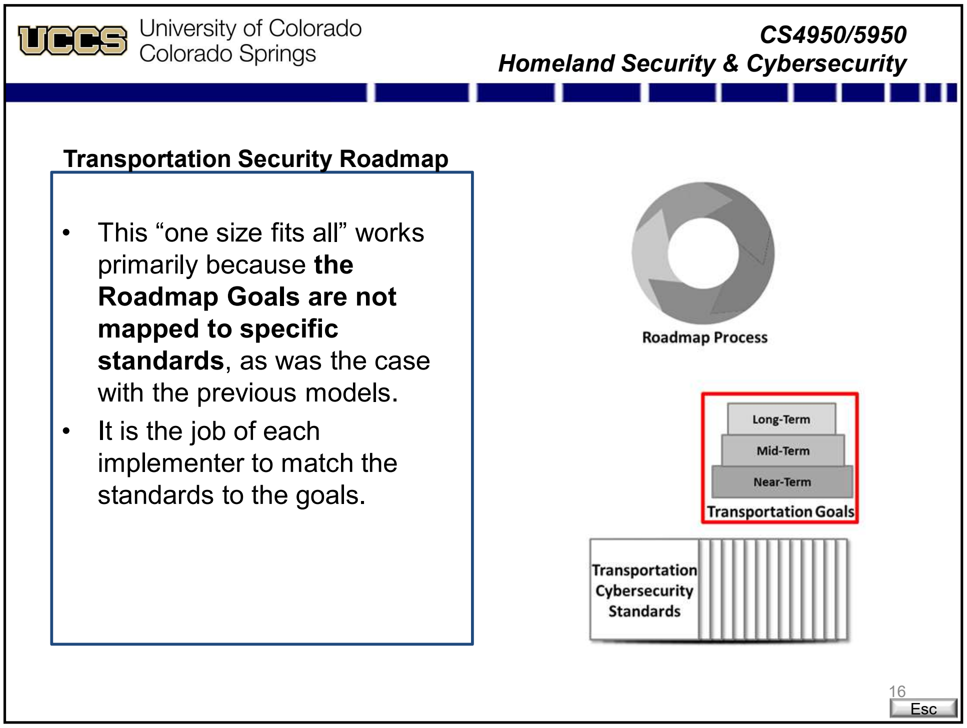
Long-Term
Mid-Term
Near-Term
Transportation Goals

Transportation Cybersecurity Standards

15

Esc

15



University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Transportation Security Roadmap

- This "one size fits all" works primarily because **the Roadmap Goals are not mapped to specific standards**, as was the case with the previous models.
- It is the job of each implementer to match the standards to the goals.

Roadmap Process

Long-Term
Mid-Term
Near-Term
Transportation Goals

Transportation Cybersecurity Standards

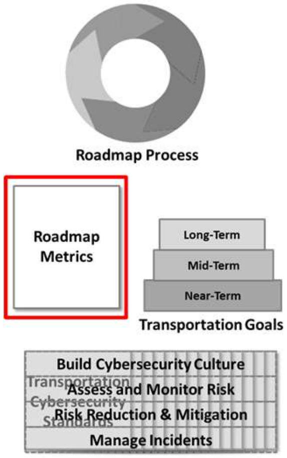
16

Esc

16

Transportation Security Roadmap

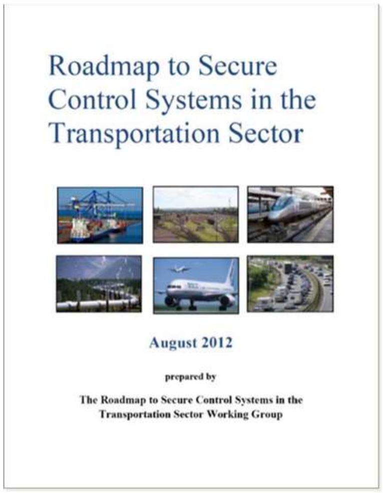
- Finally, the Transportation Security Roadmap does include one thing not found in the NIST Cybersecurity Framework or ES-C2M2.
- For each Transportation Goal, **the Roadmap also identifies corresponding "metrics"** indicating when the goal has been achieved.



Esc

Transportation Security Roadmap

The Transportation Security Roadmap thus provides a means for aviation officials to gauge their progress towards uniform objectives.



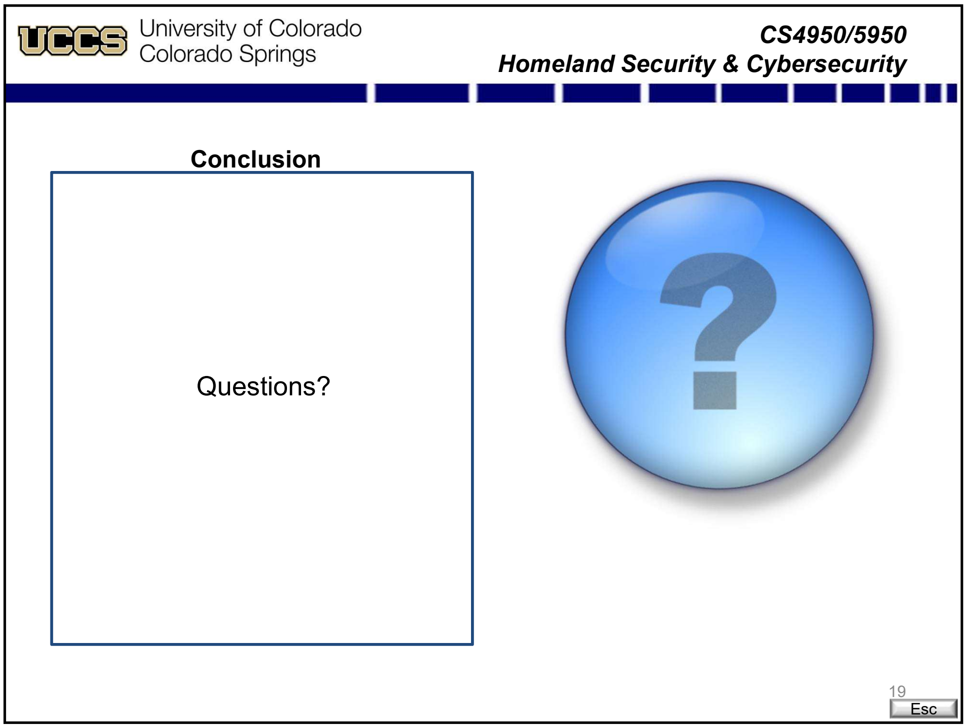
Roadmap to Secure Control Systems in the Transportation Sector

August 2012

prepared by

The Roadmap to Secure Control Systems in the Transportation Sector Working Group

Esc



University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Conclusion

Questions?

19

Esc

19