TR Exercise 3

CS 4950/5950

Homeland Security & Cybersecurity

Lesson 30

Aviation Security

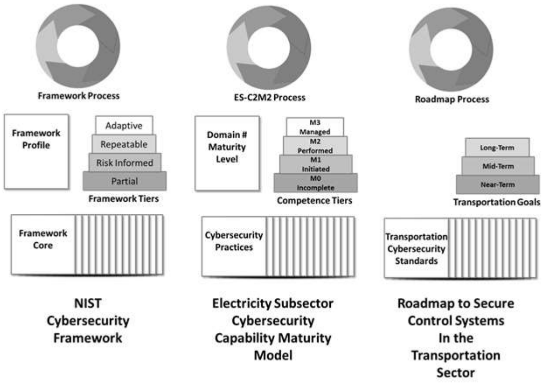
Exercise 3

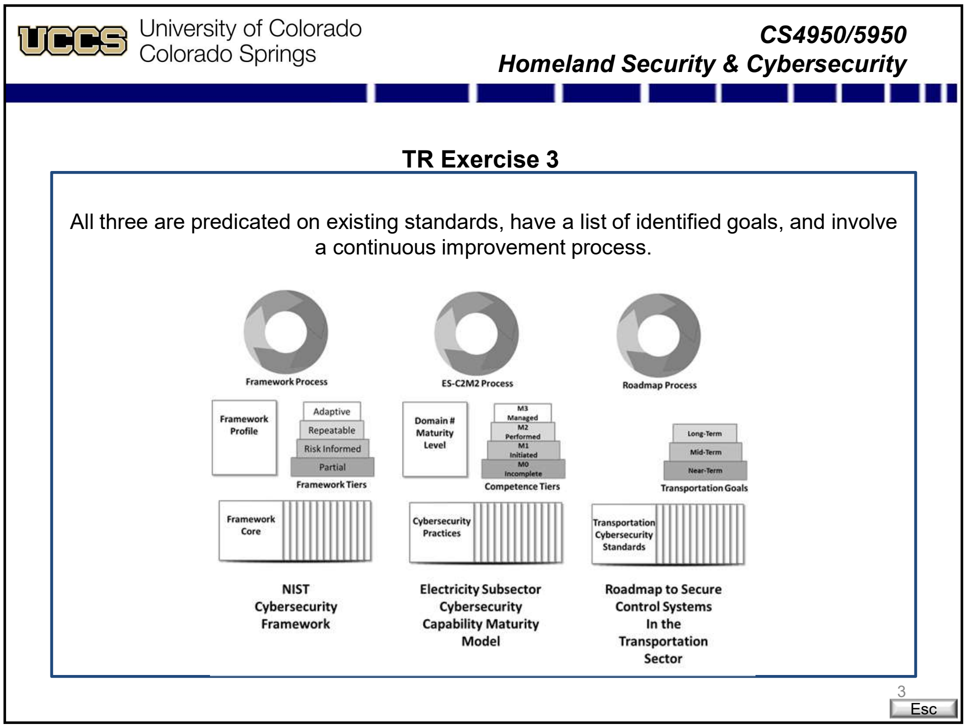
Rick White, Ph.D.

University of Colorado, Colorado Springs

TR Exercise 3

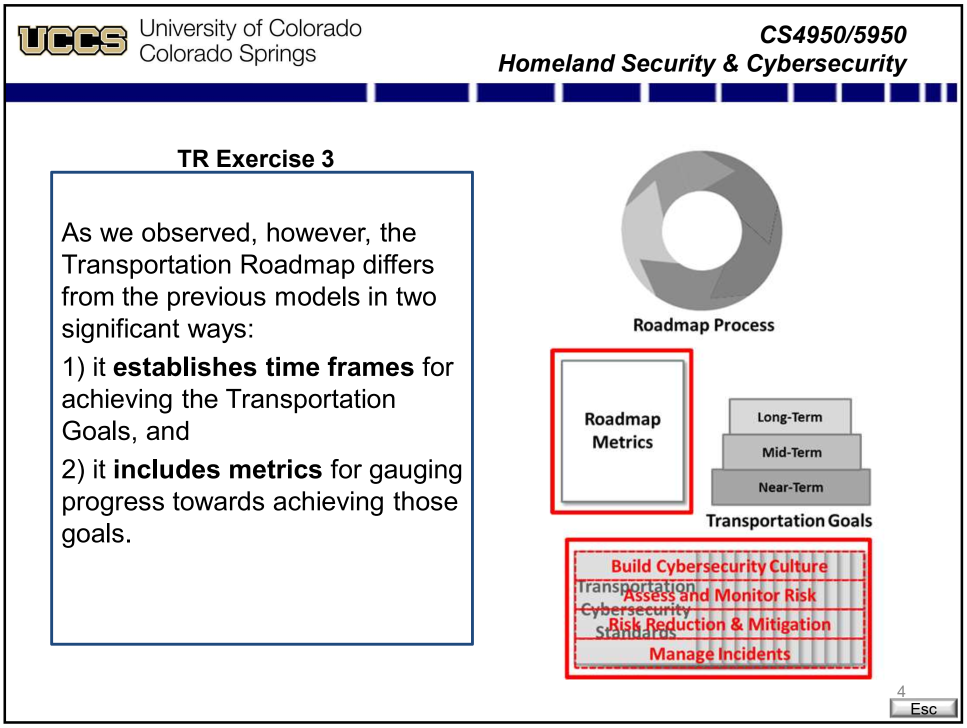
Structurally, the Transportation Roadmap is very similar to the NIST Cybersecurity Framework and Electricity Subsector Cybersecurity Capability Maturity Model.





TR Exercise 3

All three are predicated on existing standards, have a list of identified goals, and involve a continuous improvement process.

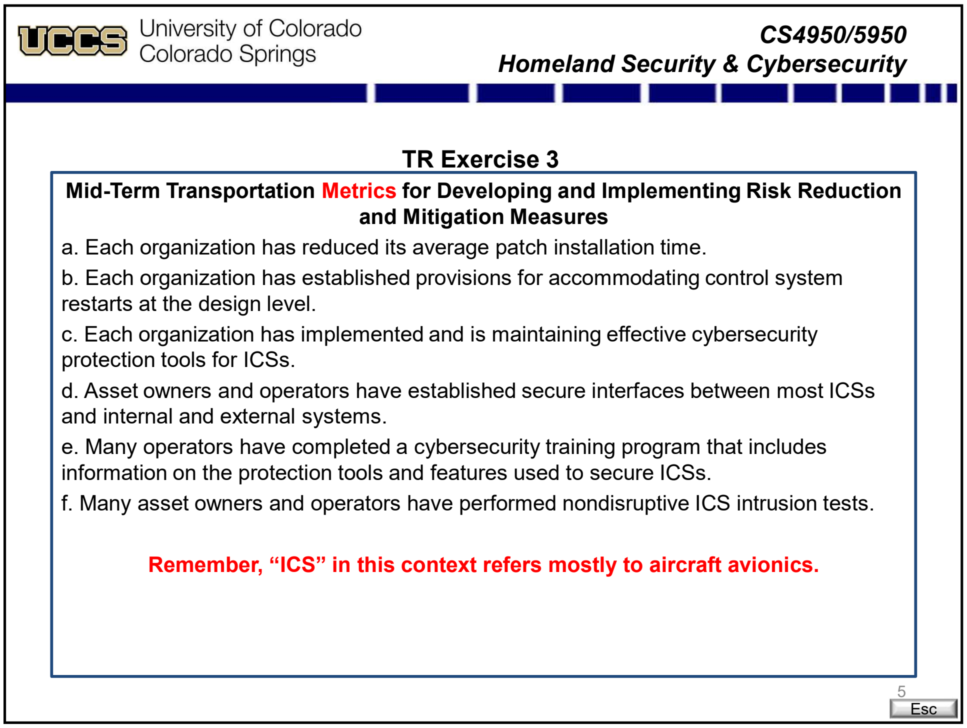


TR Exercise 3

As we observed, however, the Transportation Roadmap differs from the previous models in two significant ways:

1) it **establishes time frames** for achieving the Transportation Goals, and

2) it **includes metrics** for gauging progress towards achieving those goals.



University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

TR Exercise 3

Mid-Term Transportation Metrics for Developing and Implementing Risk Reduction and Mitigation Measures

a. Each organization has reduced its average patch installation time.

b. Each organization has established provisions for accommodating control system restarts at the design level.

c. Each organization has implemented and is maintaining effective cybersecurity protection tools for ICSs.

d. Asset owners and operators have established secure interfaces between most ICSs and internal and external systems.

e. Many operators have completed a cybersecurity training program that includes information on the protection tools and features used to secure ICSs.

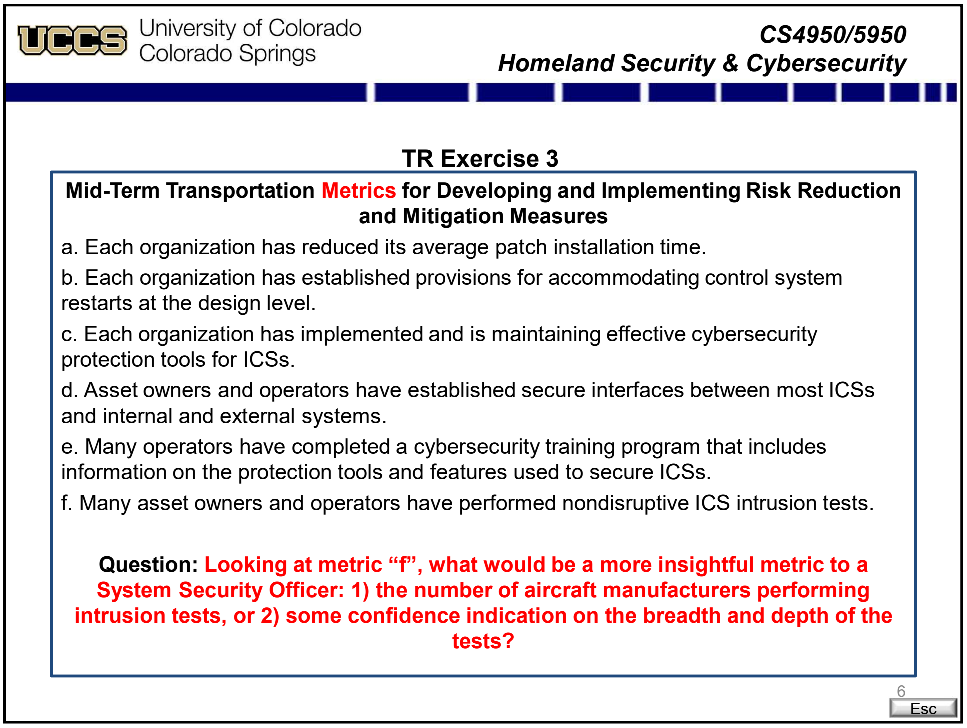
f. Many asset owners and operators have performed nondisruptive ICS intrusion tests.

Remember, “ICS” in this context refers mostly to aircraft avionics.

5

Esc

5



University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

TR Exercise 3

Mid-Term Transportation Metrics for Developing and Implementing Risk Reduction and Mitigation Measures

a. Each organization has reduced its average patch installation time.

b. Each organization has established provisions for accommodating control system restarts at the design level.

c. Each organization has implemented and is maintaining effective cybersecurity protection tools for ICSs.

d. Asset owners and operators have established secure interfaces between most ICSs and internal and external systems.

e. Many operators have completed a cybersecurity training program that includes information on the protection tools and features used to secure ICSs.

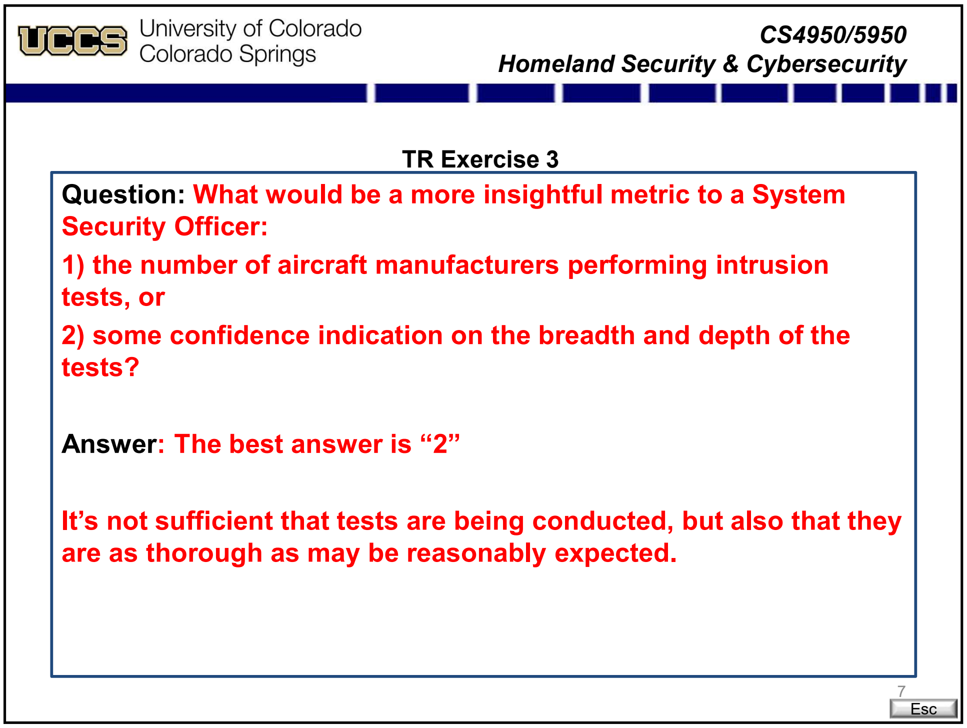
f. Many asset owners and operators have performed nondisruptive ICS intrusion tests.

Question: Looking at metric “f”, what would be a more insightful metric to a System Security Officer: 1) the number of aircraft manufacturers performing intrusion tests, or 2) some confidence indication on the breadth and depth of the tests?

6

Esc

6



University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

TR Exercise 3

Question: What would be a more insightful metric to a System Security Officer:

1) the number of aircraft manufacturers performing intrusion tests, or

2) some confidence indication on the breadth and depth of the tests?

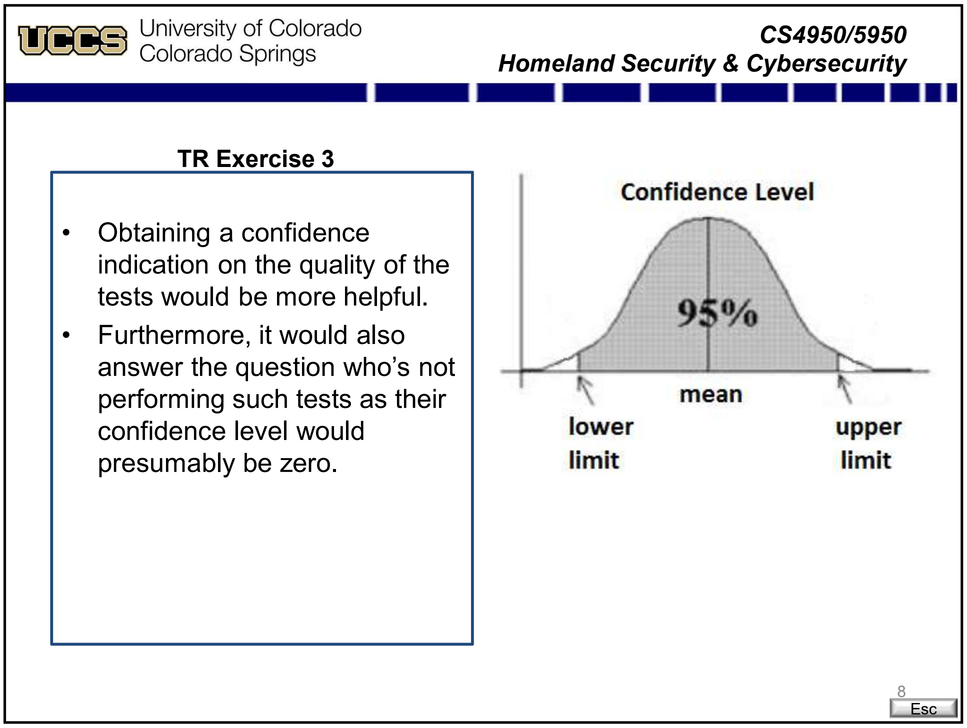
Answer: The best answer is “2”

It’s not sufficient that tests are being conducted, but also that they are as thorough as may be reasonably expected.

7

Esc

7



University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

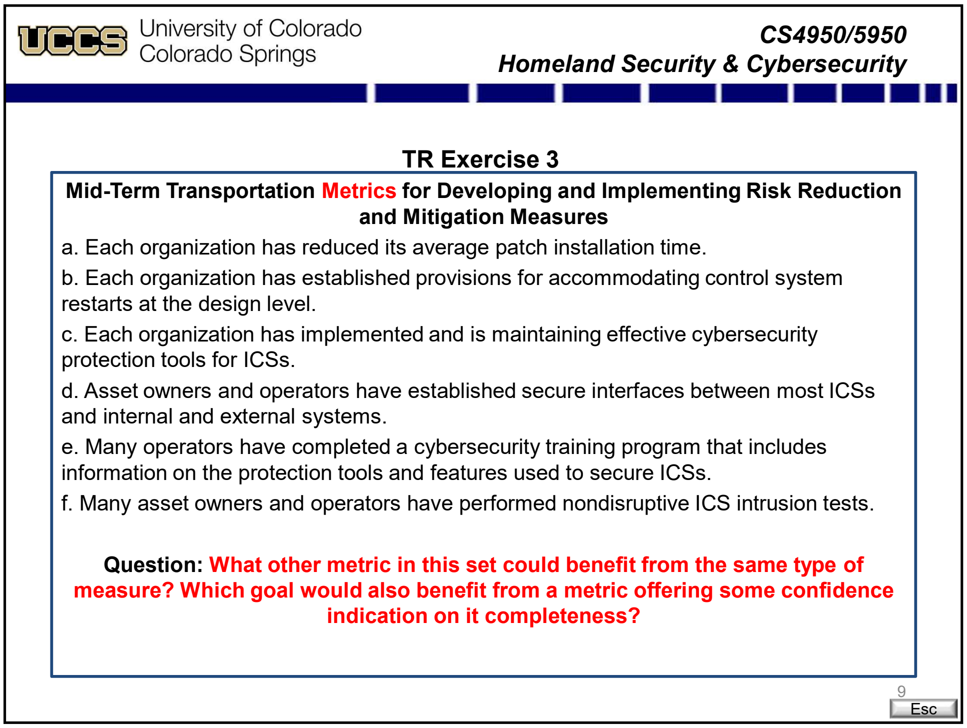
TR Exercise 3

- Obtaining a confidence indication on the quality of the tests would be more helpful.
- Furthermore, it would also answer the question who’s not performing such tests as their confidence level would presumably be zero.

8

Esc

8



TR Exercise 3

Mid-Term Transportation Metrics for Developing and Implementing Risk Reduction and Mitigation Measures

a. Each organization has reduced its average patch installation time.

b. Each organization has established provisions for accommodating control system restarts at the design level.

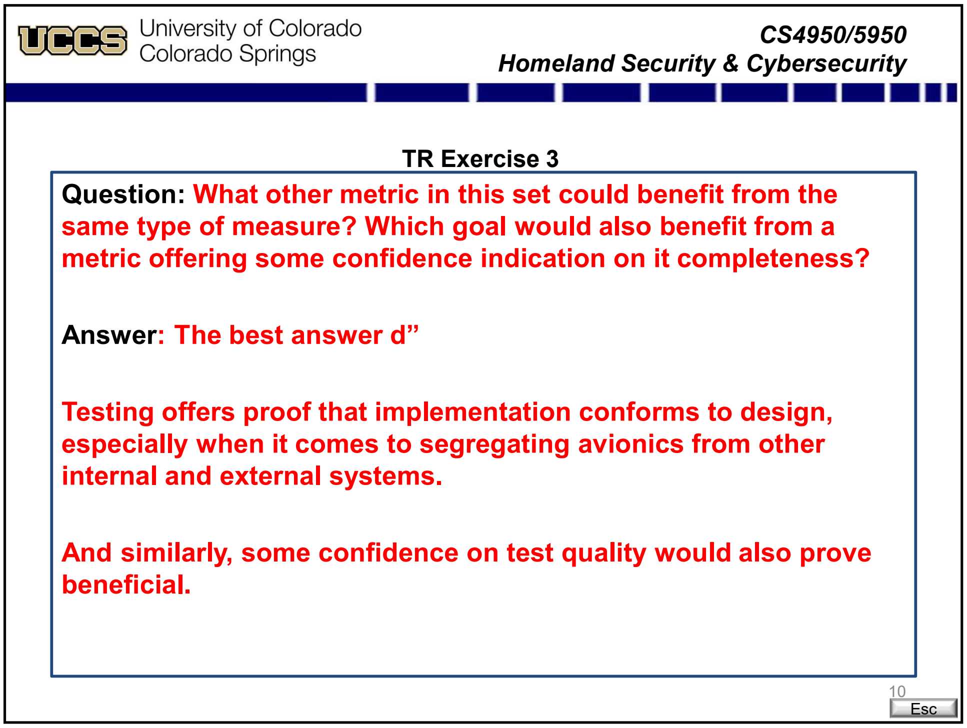
c. Each organization has implemented and is maintaining effective cybersecurity protection tools for ICSs.

d. Asset owners and operators have established secure interfaces between most ICSs and internal and external systems.

e. Many operators have completed a cybersecurity training program that includes information on the protection tools and features used to secure ICSs.

f. Many asset owners and operators have performed nondisruptive ICS intrusion tests.

Question: What other metric in this set could benefit from the same type of measure? Which goal would also benefit from a metric offering some confidence indication on it completeness?



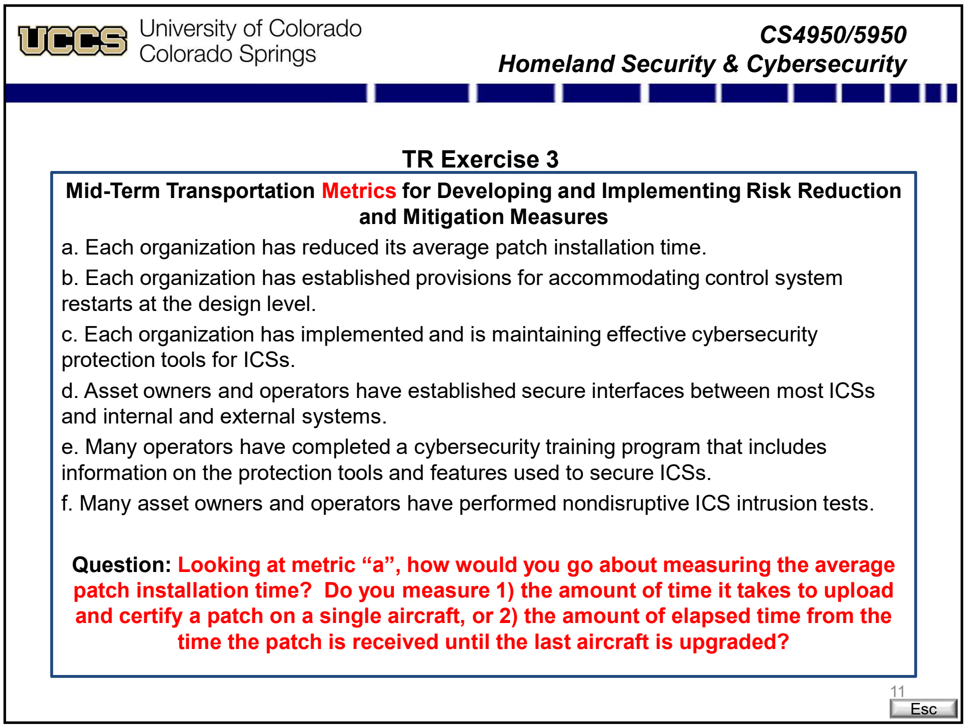
TR Exercise 3

Question: What other metric in this set could benefit from the same type of measure? Which goal would also benefit from a metric offering some confidence indication on it completeness?

Answer: The best answer d”

Testing offers proof that implementation conforms to design, especially when it comes to segregating avionics from other internal and external systems.

And similarly, some confidence on test quality would also prove beneficial.



TR Exercise 3

Mid-Term Transportation Metrics for Developing and Implementing Risk Reduction and Mitigation Measures

a. Each organization has reduced its average patch installation time.

b. Each organization has established provisions for accommodating control system restarts at the design level.

c. Each organization has implemented and is maintaining effective cybersecurity protection tools for ICSs.

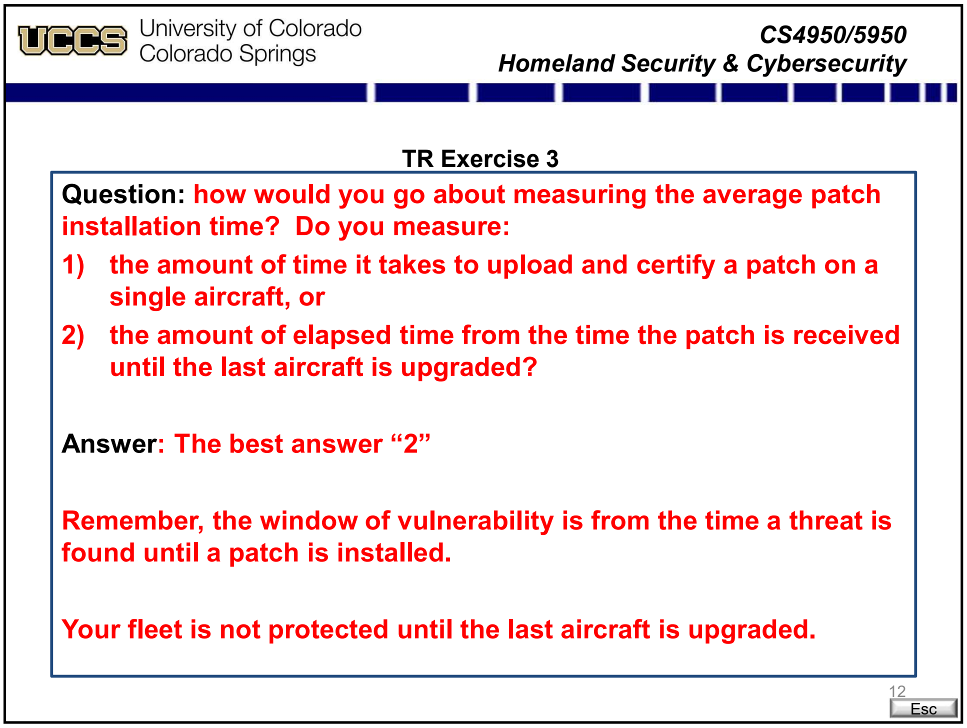
d. Asset owners and operators have established secure interfaces between most ICSs and internal and external systems.

e. Many operators have completed a cybersecurity training program that includes information on the protection tools and features used to secure ICSs.

f. Many asset owners and operators have performed nondisruptive ICS intrusion tests.

Question: Looking at metric "a", how would you go about measuring the average patch installation time? Do you measure 1) the amount of time it takes to upload and certify a patch on a single aircraft, or 2) the amount of elapsed time from the time the patch is received until the last aircraft is upgraded?

Esc



TR Exercise 3

Question: how would you go about measuring the average patch installation time? Do you measure:

1) **the amount of time it takes to upload and certify a patch on a single aircraft, or**
2) **the amount of elapsed time from the time the patch is received until the last aircraft is upgraded?**

Answer: The best answer "2"

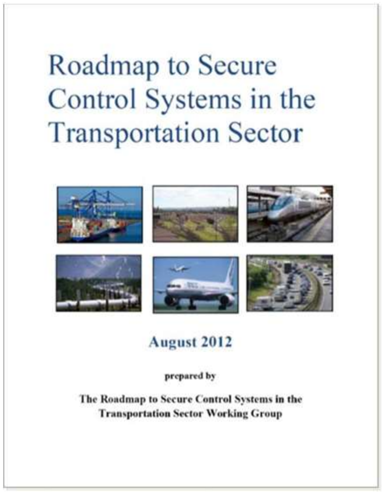
Remember, the window of vulnerability is from the time a threat is found until a patch is installed.

Your fleet is not protected until the last aircraft is upgraded.

Esc

TR Exercise 3

This concludes our look at cybersecurity policy for the aviation subsector.



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

Conclusion

Questions?