TR Exercise 2

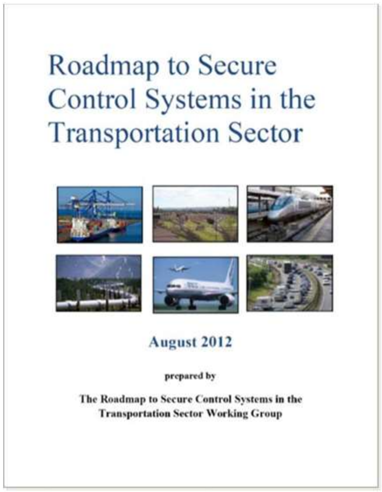
CS 4950/5950
Homeland Security & Cybersecurity

Lesson 30
Aviation Security
Exercise 2

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

TR Exercise 2

Let us take us see how we might apply Transportation Roadmap for cybersecurity.



Roadmap to Secure Control Systems in the Transportation Sector

August 2012

prepared by

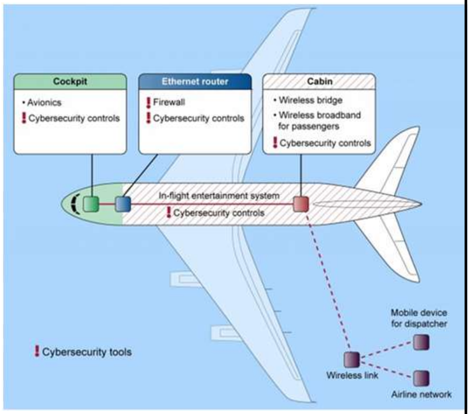
The Roadmap to Secure Control Systems in the Transportation Sector Working Group

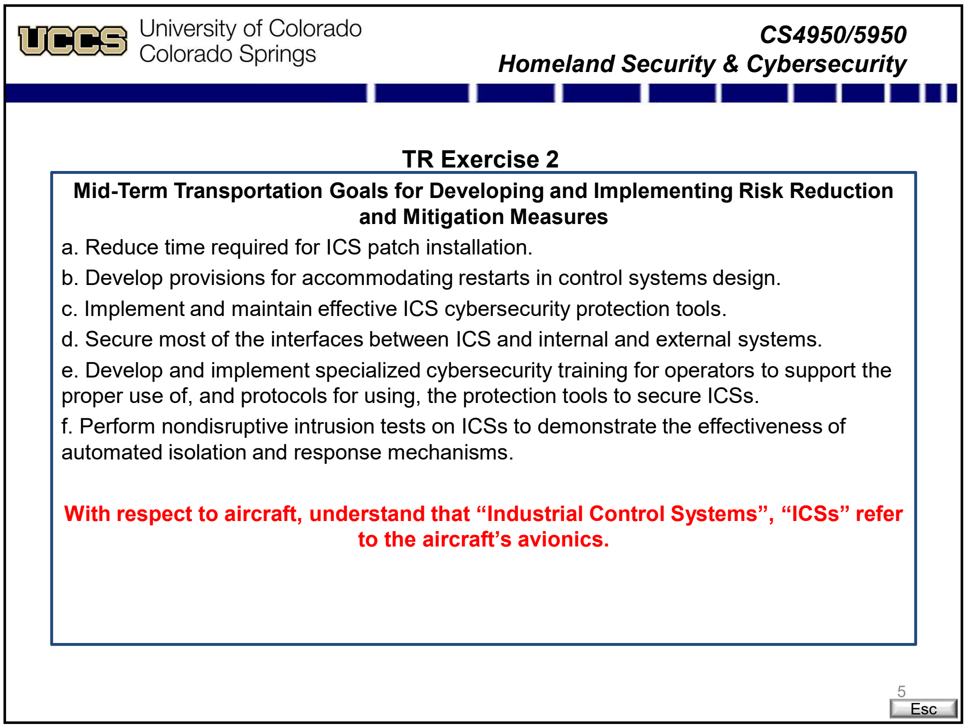
TR Exercise 2

- To start, let us return to the alleged hacking by a passenger into an aircraft's avionics back in April 2015.
- **Recall that a passenger was removed from a flight after tweeting that they could hack the airplane's in-flight entertainment system.**

TR Exercise 2

- The passenger claimed they were able to access the aircraft's Thrust Management System and order one of its engines to increase thrust for a climb, resulting in a temporary yaw.
- While the aircraft designer asserted the claim was false, the passenger was nonetheless barred from flying with the airline again.





University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

TR Exercise 2

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

a. Reduce time required for ICS patch installation.

b. Develop provisions for accommodating restarts in control systems design.

c. Implement and maintain effective ICS cybersecurity protection tools.

d. Secure most of the interfaces between ICS and internal and external systems.

e. Develop and implement specialized cybersecurity training for operators to support the proper use of, and protocols for using, the protection tools to secure ICSs.

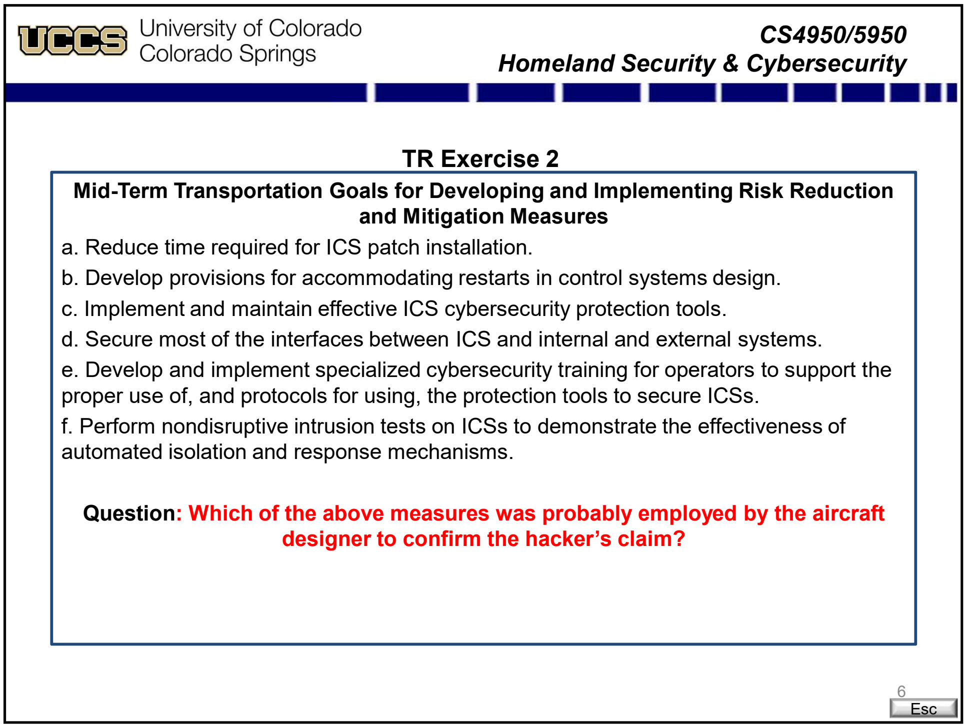
f. Perform nondisruptive intrusion tests on ICSs to demonstrate the effectiveness of automated isolation and response mechanisms.

With respect to aircraft, understand that “Industrial Control Systems”, “ICSs” refer to the aircraft’s avionics.

5

Esc

5



University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

TR Exercise 2

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

a. Reduce time required for ICS patch installation.

b. Develop provisions for accommodating restarts in control systems design.

c. Implement and maintain effective ICS cybersecurity protection tools.

d. Secure most of the interfaces between ICS and internal and external systems.

e. Develop and implement specialized cybersecurity training for operators to support the proper use of, and protocols for using, the protection tools to secure ICSs.

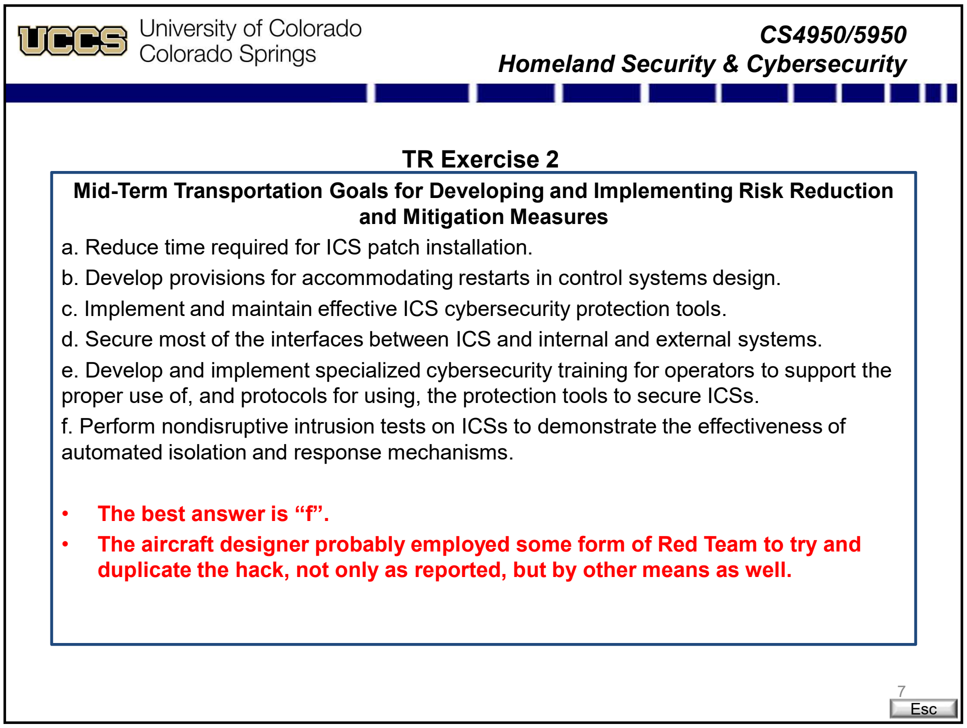
f. Perform nondisruptive intrusion tests on ICSs to demonstrate the effectiveness of automated isolation and response mechanisms.

Question: Which of the above measures was probably employed by the aircraft designer to confirm the hacker’s claim?

6

Esc

6



University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

TR Exercise 2

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

a. Reduce time required for ICS patch installation.

b. Develop provisions for accommodating restarts in control systems design.

c. Implement and maintain effective ICS cybersecurity protection tools.

d. Secure most of the interfaces between ICS and internal and external systems.

e. Develop and implement specialized cybersecurity training for operators to support the proper use of, and protocols for using, the protection tools to secure ICSs.

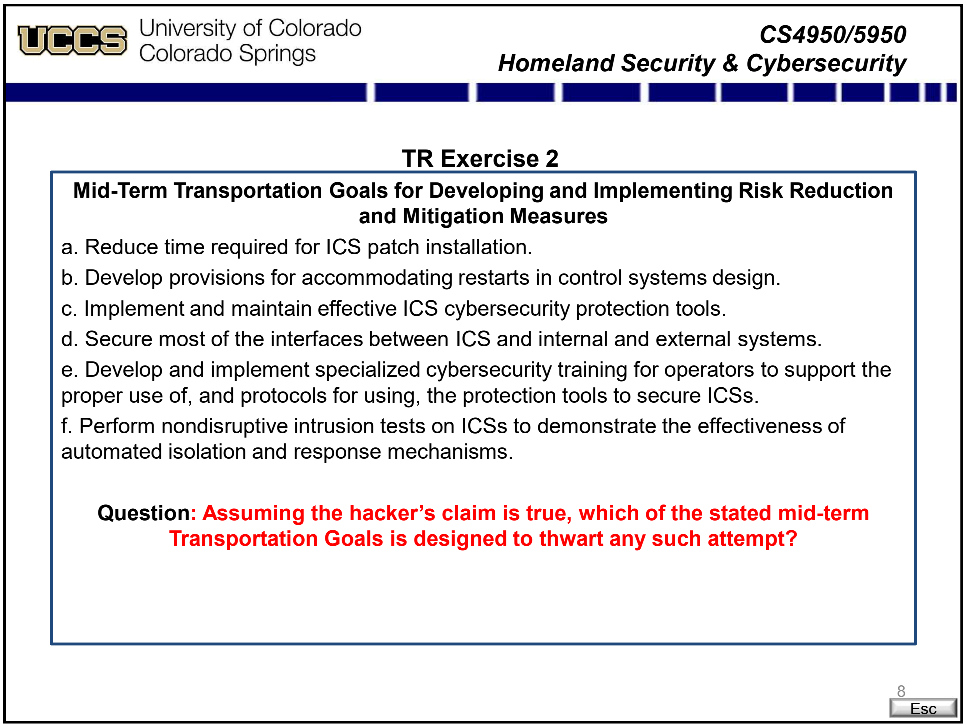
f. Perform nondisruptive intrusion tests on ICSs to demonstrate the effectiveness of automated isolation and response mechanisms.

- **The best answer is "f".**
- **The aircraft designer probably employed some form of Red Team to try and duplicate the hack, not only as reported, but by other means as well.**

7

Esc

7



University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

TR Exercise 2

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

a. Reduce time required for ICS patch installation.

b. Develop provisions for accommodating restarts in control systems design.

c. Implement and maintain effective ICS cybersecurity protection tools.

d. Secure most of the interfaces between ICS and internal and external systems.

e. Develop and implement specialized cybersecurity training for operators to support the proper use of, and protocols for using, the protection tools to secure ICSs.

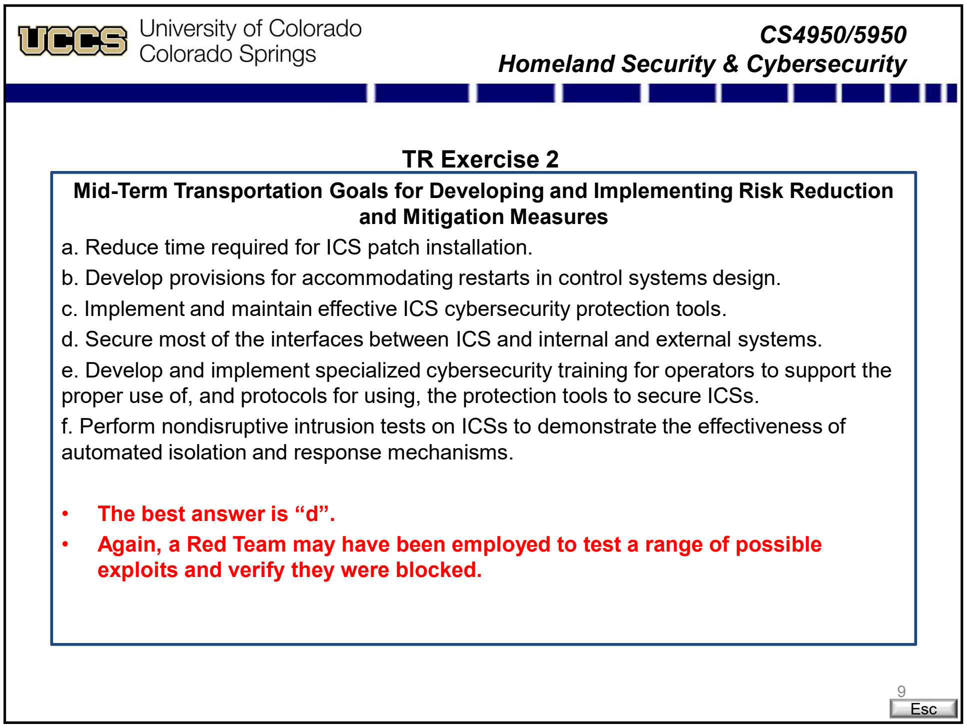
f. Perform nondisruptive intrusion tests on ICSs to demonstrate the effectiveness of automated isolation and response mechanisms.

Question: Assuming the hacker's claim is true, which of the stated mid-term Transportation Goals is designed to thwart any such attempt?

8

Esc

8



TR Exercise 2

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

a. Reduce time required for ICS patch installation.

b. Develop provisions for accommodating restarts in control systems design.

c. Implement and maintain effective ICS cybersecurity protection tools.

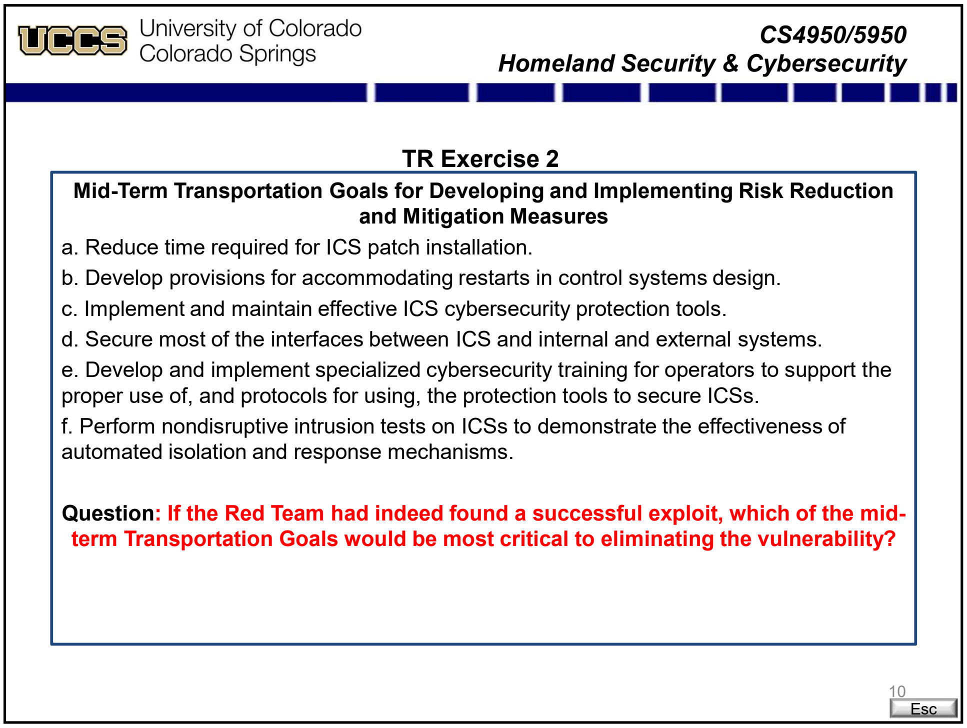
d. Secure most of the interfaces between ICS and internal and external systems.

e. Develop and implement specialized cybersecurity training for operators to support the proper use of, and protocols for using, the protection tools to secure ICSs.

f. Perform nondisruptive intrusion tests on ICSs to demonstrate the effectiveness of automated isolation and response mechanisms.

- **The best answer is "d".**
- **Again, a Red Team may have been employed to test a range of possible exploits and verify they were blocked.**

9



TR Exercise 2

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

a. Reduce time required for ICS patch installation.

b. Develop provisions for accommodating restarts in control systems design.

c. Implement and maintain effective ICS cybersecurity protection tools.

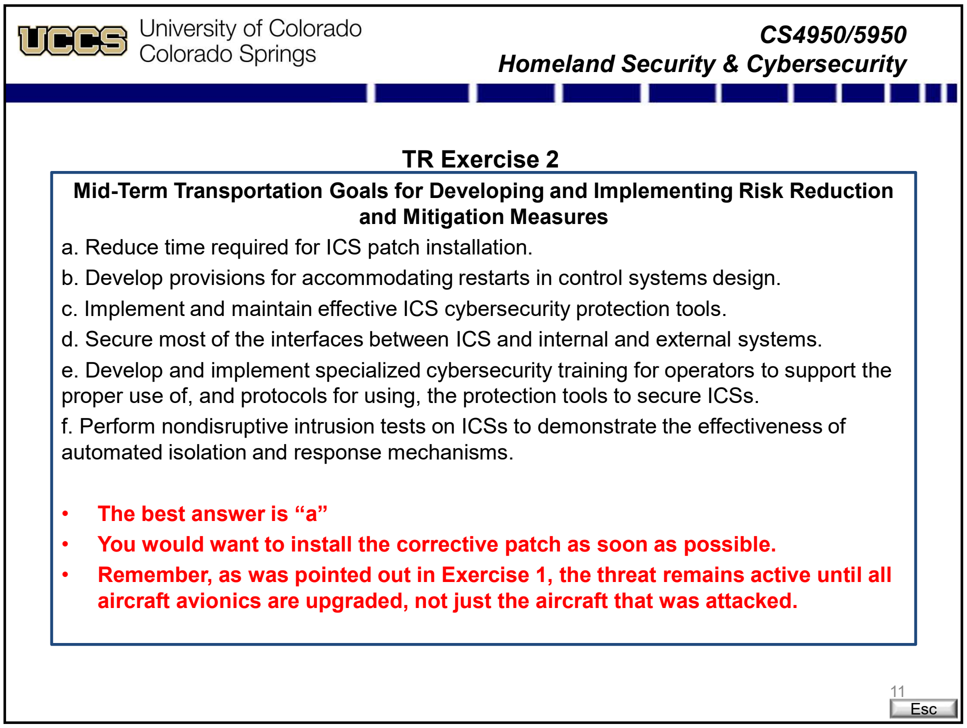
d. Secure most of the interfaces between ICS and internal and external systems.

e. Develop and implement specialized cybersecurity training for operators to support the proper use of, and protocols for using, the protection tools to secure ICSs.

f. Perform nondisruptive intrusion tests on ICSs to demonstrate the effectiveness of automated isolation and response mechanisms.

Question: If the Red Team had indeed found a successful exploit, which of the mid-term Transportation Goals would be most critical to eliminating the vulnerability?

10



University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

TR Exercise 2

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

a. Reduce time required for ICS patch installation.

b. Develop provisions for accommodating restarts in control systems design.

c. Implement and maintain effective ICS cybersecurity protection tools.

d. Secure most of the interfaces between ICS and internal and external systems.

e. Develop and implement specialized cybersecurity training for operators to support the proper use of, and protocols for using, the protection tools to secure ICSs.

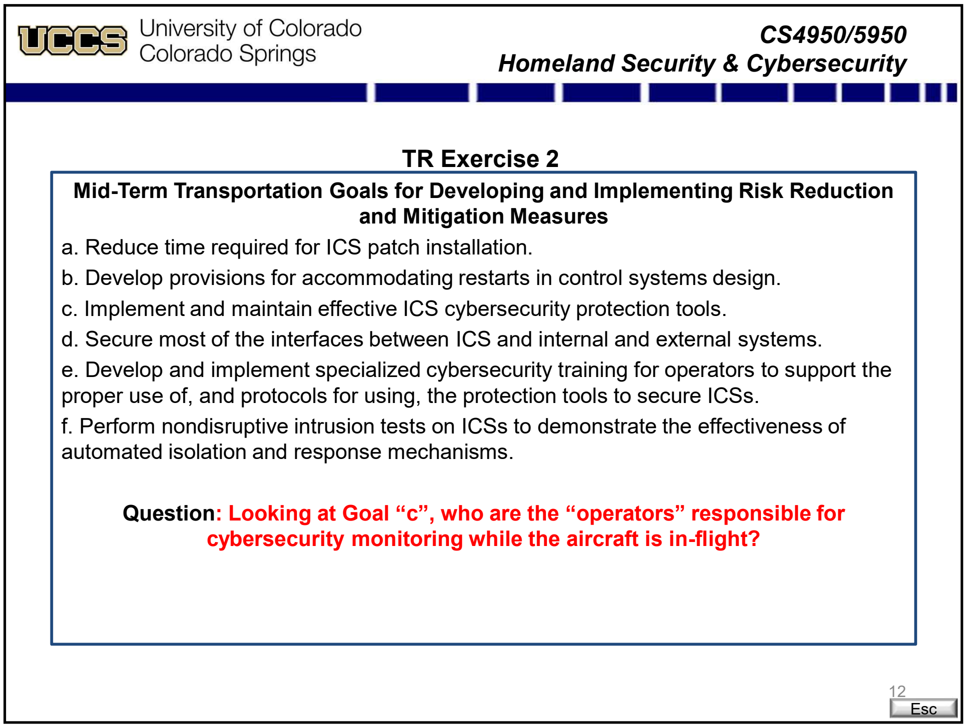
f. Perform nondisruptive intrusion tests on ICSs to demonstrate the effectiveness of automated isolation and response mechanisms.

- **The best answer is “a”**
- **You would want to install the corrective patch as soon as possible.**
- **Remember, as was pointed out in Exercise 1, the threat remains active until all aircraft avionics are upgraded, not just the aircraft that was attacked.**

11

Esc

11



University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

TR Exercise 2

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

a. Reduce time required for ICS patch installation.

b. Develop provisions for accommodating restarts in control systems design.

c. Implement and maintain effective ICS cybersecurity protection tools.

d. Secure most of the interfaces between ICS and internal and external systems.

e. Develop and implement specialized cybersecurity training for operators to support the proper use of, and protocols for using, the protection tools to secure ICSs.

f. Perform nondisruptive intrusion tests on ICSs to demonstrate the effectiveness of automated isolation and response mechanisms.

Question: Looking at Goal “c”, who are the “operators” responsible for cybersecurity monitoring while the aircraft is in-flight?

12

Esc

12

TR Exercise 2

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

a. Reduce time required for ICS patch installation.

b. Develop provisions for accommodating restarts in control systems design.

c. Implement and maintain effective ICS cybersecurity protection tools.

d. Secure most of the interfaces between ICS and internal and external systems.

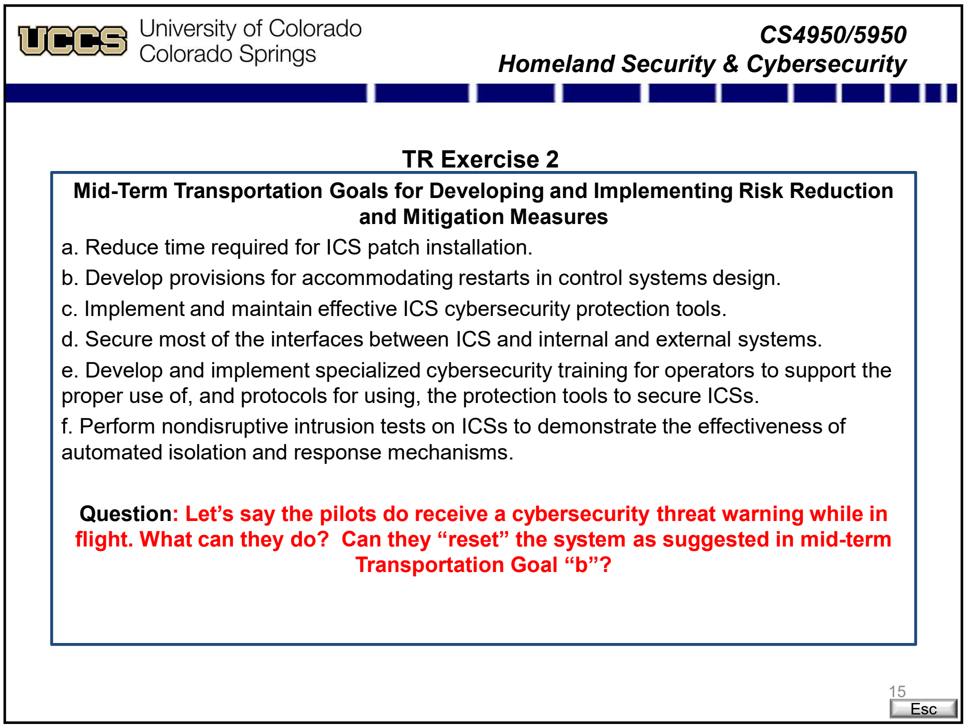
e. Develop and implement specialized cybersecurity training for operators to support the proper use of, and protocols for using, the protection tools to secure ICSs.

f. Perform nondisruptive intrusion tests on ICSs to demonstrate the effectiveness of automated isolation and response mechanisms.

- **Answer: The Pilots.**
- **Do you suppose this Transportation Goal is suggesting that aircraft carry a System Security Officer?**

TR Exercise 2

This Transportation Goal was meant to apply to ground systems only, perhaps the air traffic control system.



University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

TR Exercise 2

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

a. Reduce time required for ICS patch installation.

b. Develop provisions for accommodating restarts in control systems design.

c. Implement and maintain effective ICS cybersecurity protection tools.

d. Secure most of the interfaces between ICS and internal and external systems.

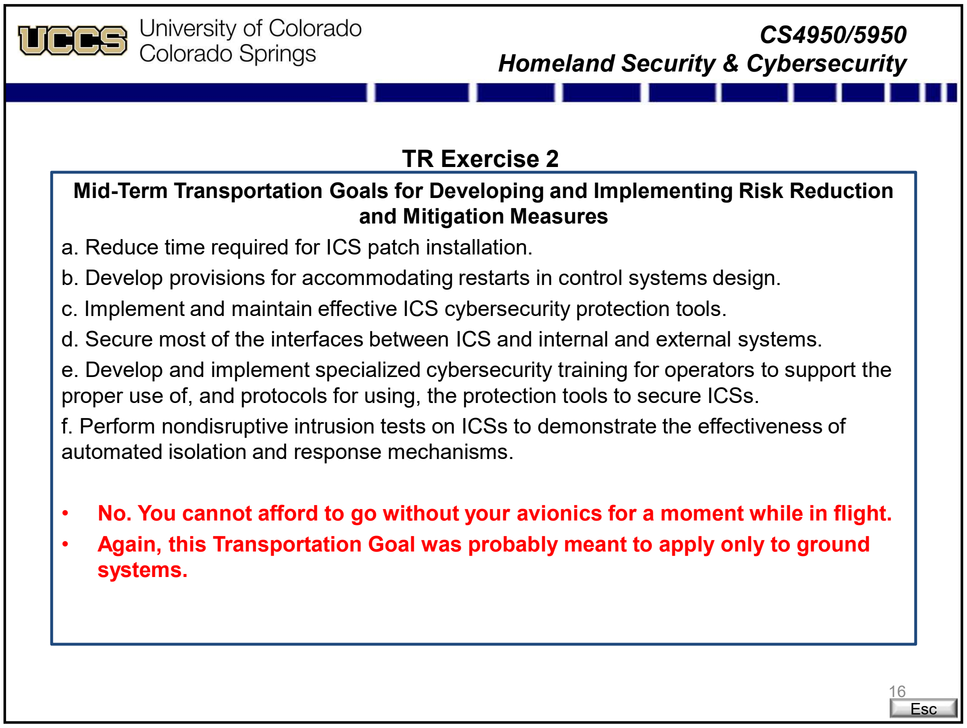
e. Develop and implement specialized cybersecurity training for operators to support the proper use of, and protocols for using, the protection tools to secure ICSs.

f. Perform nondisruptive intrusion tests on ICSs to demonstrate the effectiveness of automated isolation and response mechanisms.

Question: Let's say the pilots do receive a cybersecurity threat warning while in flight. What can they do? Can they "reset" the system as suggested in mid-term Transportation Goal "b"?

15

15



University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

TR Exercise 2

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

a. Reduce time required for ICS patch installation.

b. Develop provisions for accommodating restarts in control systems design.

c. Implement and maintain effective ICS cybersecurity protection tools.

d. Secure most of the interfaces between ICS and internal and external systems.

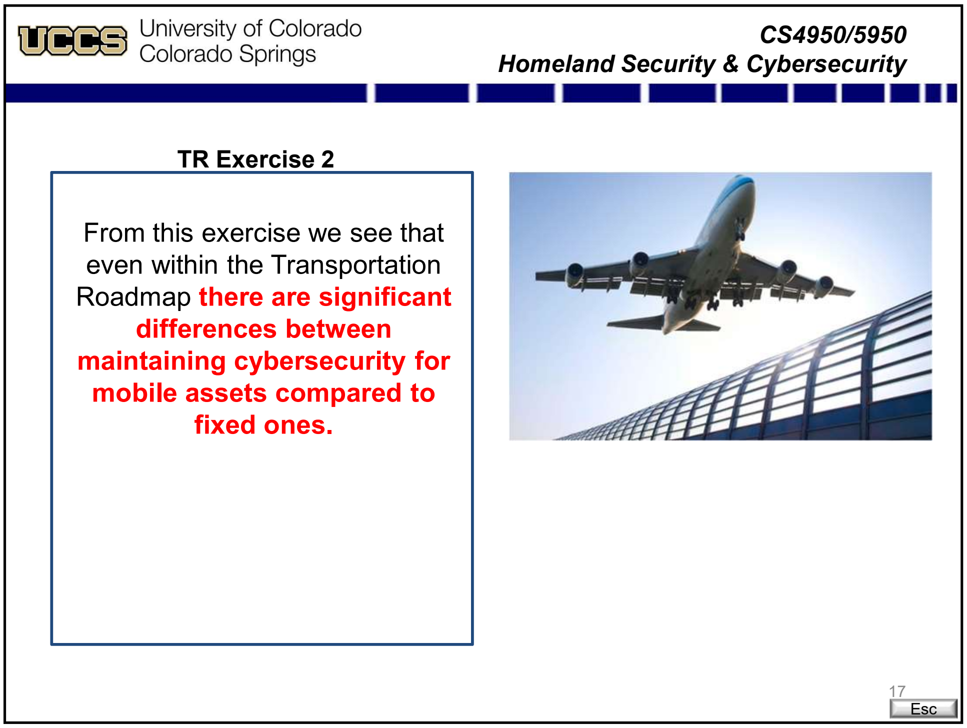
e. Develop and implement specialized cybersecurity training for operators to support the proper use of, and protocols for using, the protection tools to secure ICSs.

f. Perform nondisruptive intrusion tests on ICSs to demonstrate the effectiveness of automated isolation and response mechanisms.

- **No. You cannot afford to go without your avionics for a moment while in flight.**
- **Again, this Transportation Goal was probably meant to apply only to ground systems.**

16

16



University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

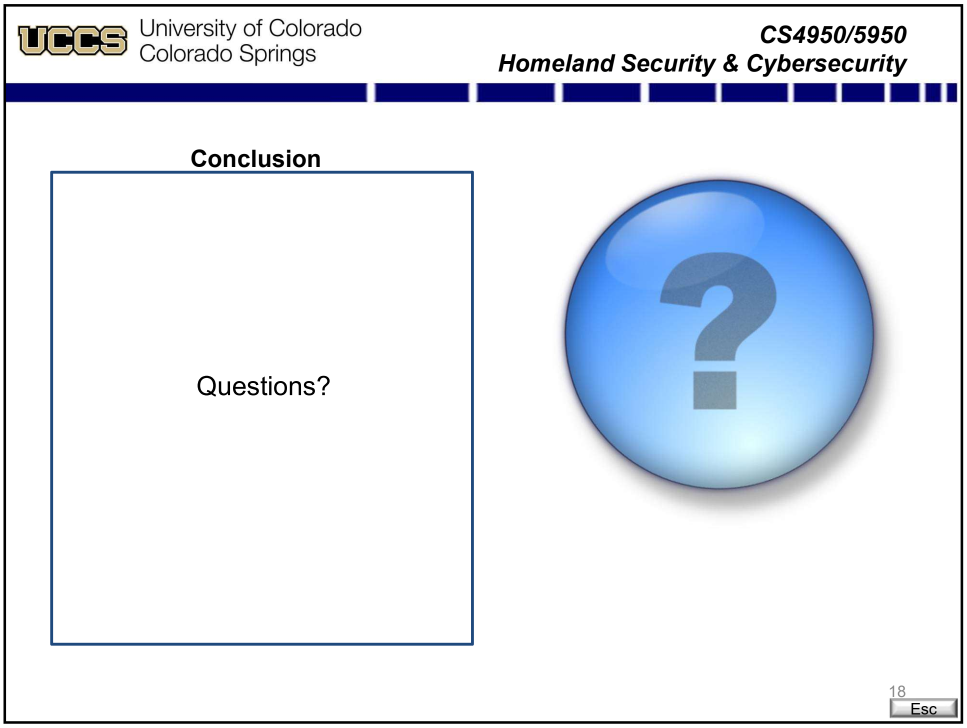
TR Exercise 2

From this exercise we see that even within the Transportation Roadmap **there are significant differences between maintaining cybersecurity for mobile assets compared to fixed ones.**

17

Esc

17



University of Colorado
Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

Conclusion

Questions?

18

Esc

18