Center for Development of Security Excellence

CDSE

Learn. Perform. Protect.

Secure Configurations for Hardware and Software

Presenter: Ms. Melissa Vice

Ms. Vice joined CDSE as an Information Technology Specialist and Courseware Developer in May 2009.

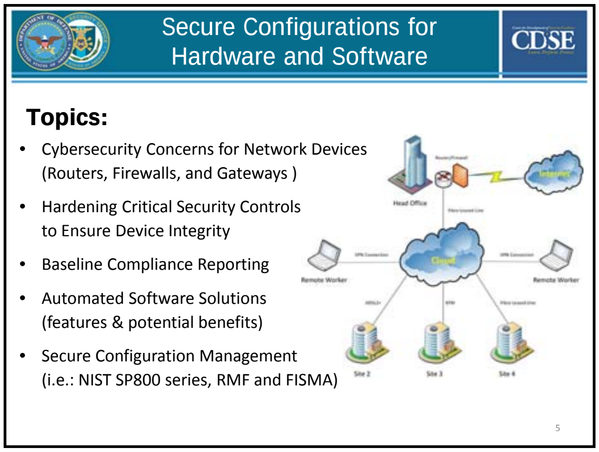
Prior to joining CDSE, Ms. Vice was the Global Database Administrator for commercial and military aircraft engine repairs worldwide at General Electric Aviation Division.

Ms. Vice holds two Associates Degrees (Science of Advertising Design and Computer Information Science), an Undergrad Certificate in Information Assurance, and is wrapping up a dual Bachelors / Masters in Cybersecurity at the University of Maryland. She is the 2010 winner of the University of Maryland's Gordon Prize for Managing Cybersecurity Resources.

Navigating the Meeting Room

Poll
Poll #1
View Votes
How many s
Process
○ 3
○ 4
○ 5
○ 6
● No Vote
Enlarge Screen
Clo
Cap
b
Q & A
Notes & Announcements
File Share

Secure Configurations for Hardware and Software

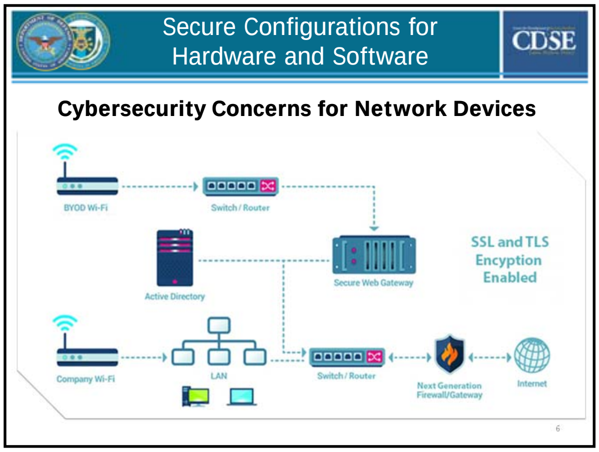


Secure Configurations for Hardware and Software

Topics:

- Cybersecurity Concerns for Network Devices (Routers, Firewalls, and Gateways)
- Hardening Critical Security Controls to Ensure Device Integrity
- Baseline Compliance Reporting
- Automated Software Solutions (features & potential benefits)
- Secure Configuration Management (i.e.: NIST SP800 series, RMF and FISMA)

5

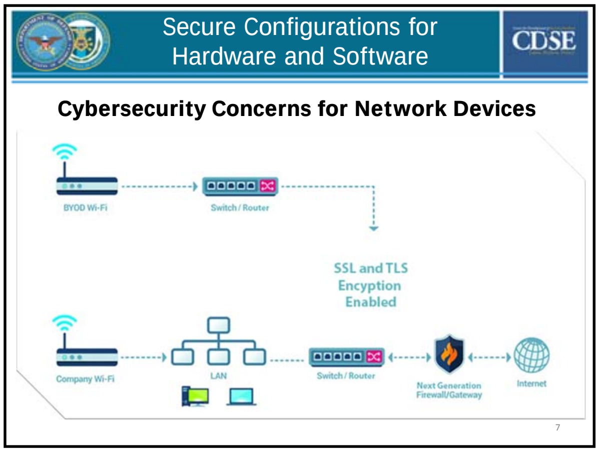


Secure Configurations for Hardware and Software

Cybersecurity Concerns for Network Devices

SSL and TLS Encryption Enabled

6

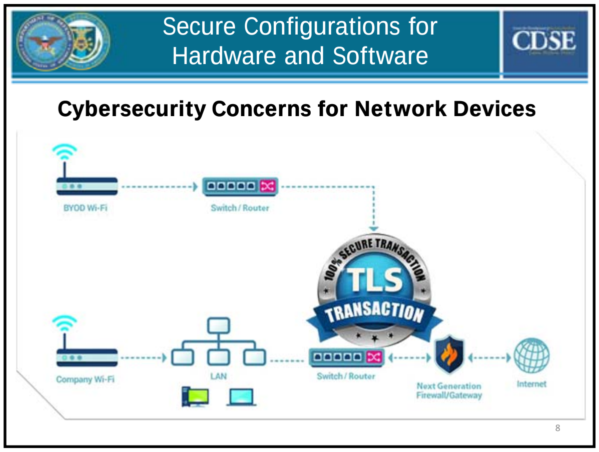


Secure Configurations for Hardware and Software

CDSE

Cybersecurity Concerns for Network Devices

7

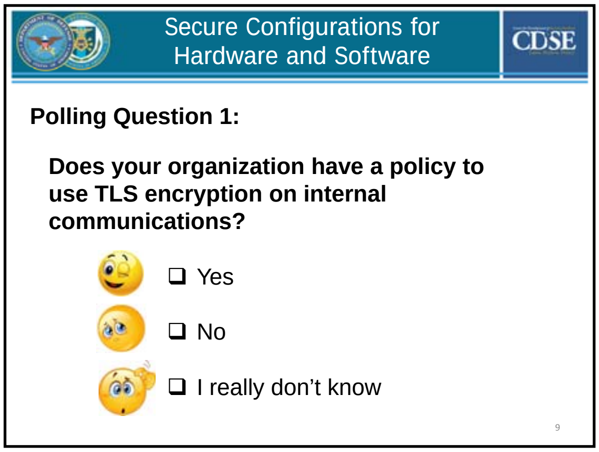


Secure Configurations for Hardware and Software

CDSE

Cybersecurity Concerns for Network Devices

8



Secure Configurations for Hardware and Software

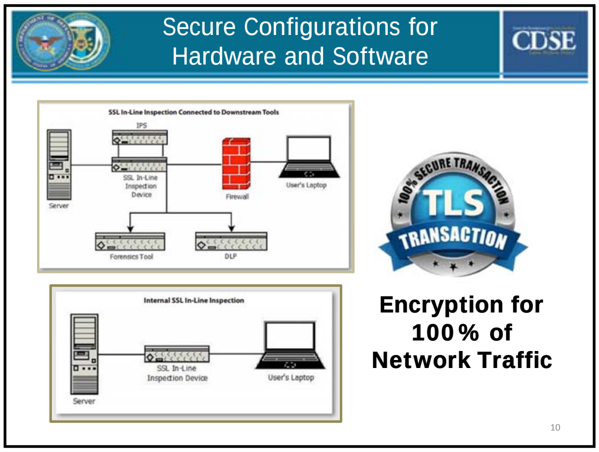
CDSE

Polling Question 1:

Does your organization have a policy to use TLS encryption on internal communications?

- ❑ Yes
- ❑ No
- ❑ I really don’t know

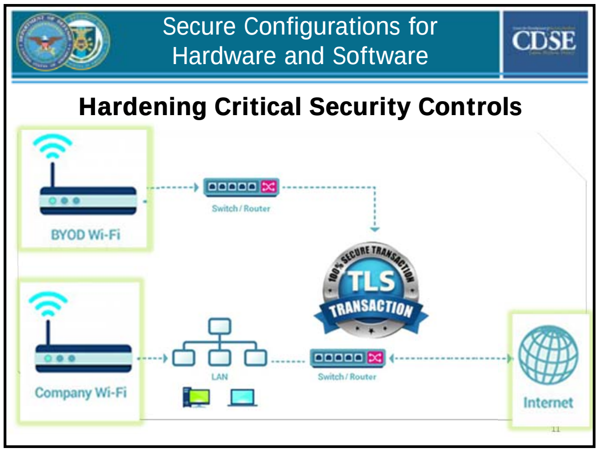
9



Secure Configurations for Hardware and Software

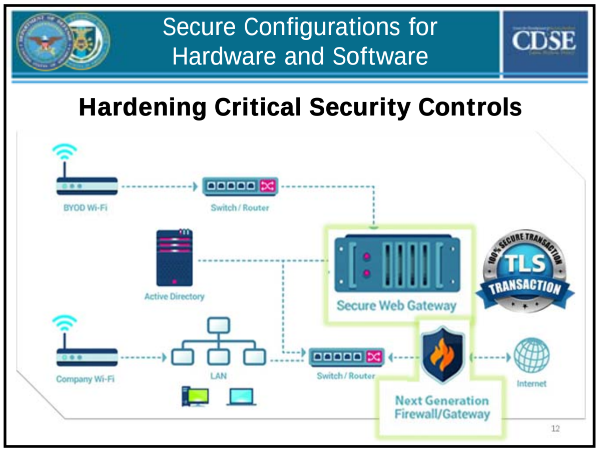
CDSE
SSL In-Line Inspection Connected to Downstream Tools
IPS
Server
SSL In-Line Inspection Device
Firewall
User's Laptop
Forensics Tool
DLP
Internal SSL In-Line Inspection
Server
SSL In-Line Inspection Device
User's Laptop
100% SECURE TRANSACTION
TLS
TRANSACTION
10

Encryption for 100% of Network Traffic



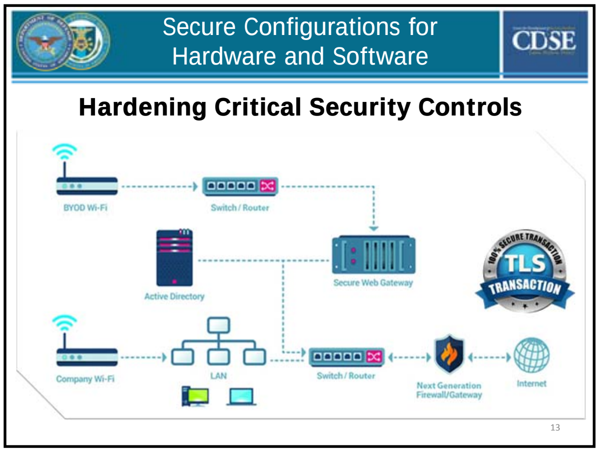
Secure Configurations for Hardware and Software

Hardening Critical Security Controls



Secure Configurations for Hardware and Software

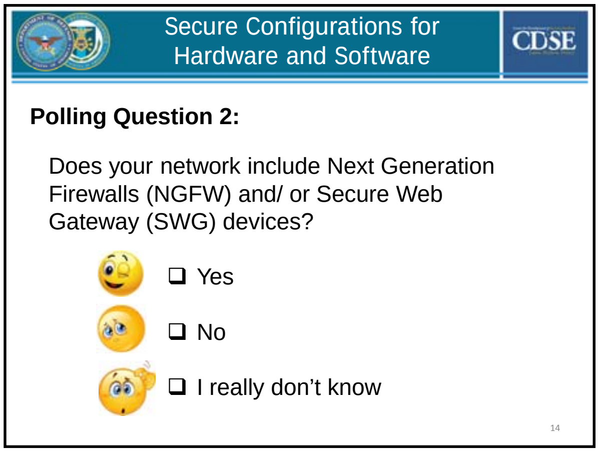
Hardening Critical Security Controls



Secure Configurations for Hardware and Software

Hardening Critical Security Controls

13



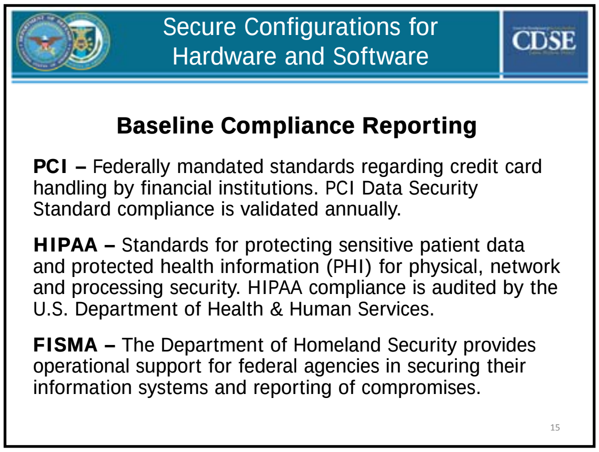
Secure Configurations for Hardware and Software

Polling Question 2:

Does your network include Next Generation Firewalls (NGFW) and/ or Secure Web Gateway (SWG) devices?

- ❑ Yes
- ❑ No
- ❑ I really don’t know

14



Secure Configurations for Hardware and Software

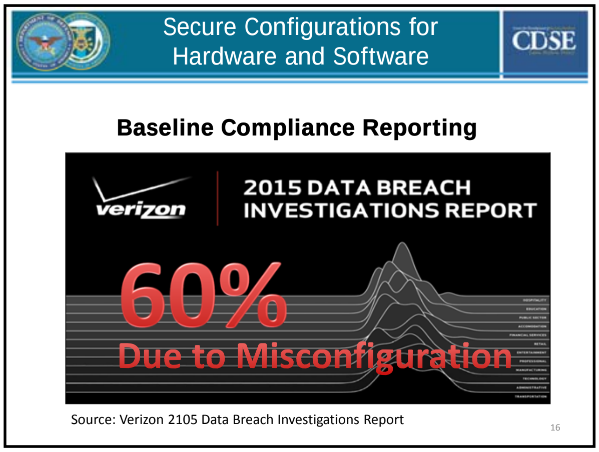
Baseline Compliance Reporting

PCI – Federally mandated standards regarding credit card handling by financial institutions. PCI Data Security Standard compliance is validated annually.

HIPAA – Standards for protecting sensitive patient data and protected health information (PHI) for physical, network and processing security. HIPAA compliance is audited by the U.S. Department of Health & Human Services.

FISMA – The Department of Homeland Security provides operational support for federal agencies in securing their information systems and reporting of compromises.

15



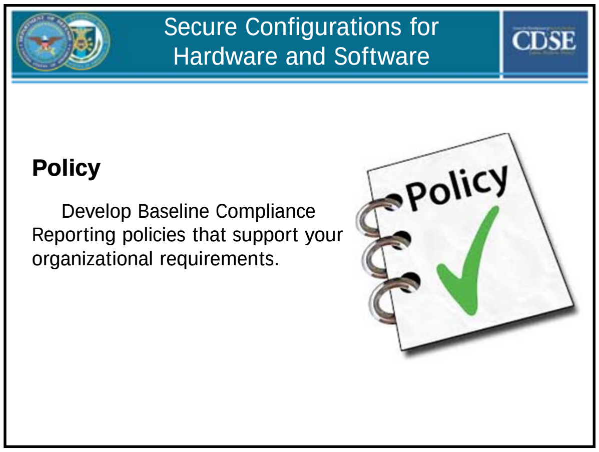
Secure Configurations for Hardware and Software

CDSE

Baseline Compliance Reporting

Source: Verizon 2105 Data Breach Investigations Report

16

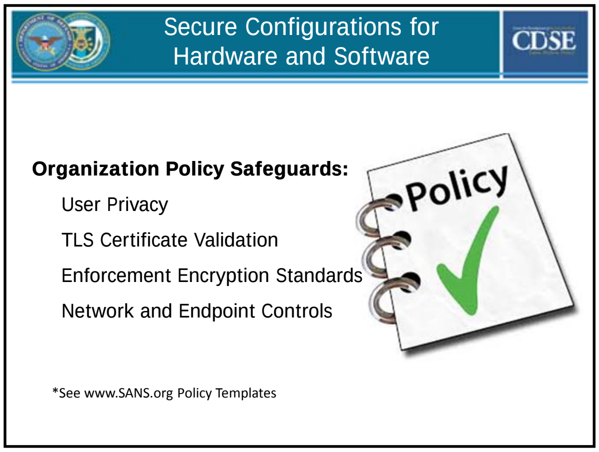


Secure Configurations for Hardware and Software

CDSE

Policy

Develop Baseline Compliance Reporting policies that support your organizational requirements.



Secure Configurations for Hardware and Software

CDSE

Organization Policy Safeguards:

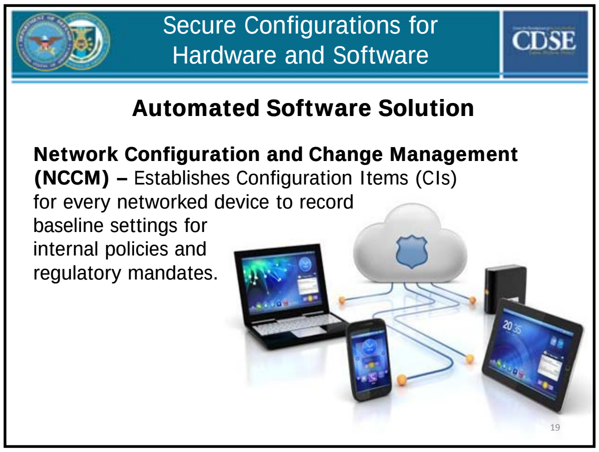
User Privacy

TLS Certificate Validation

Enforcement Encryption Standards

Network and Endpoint Controls

*See www.SANS.org Policy Templates



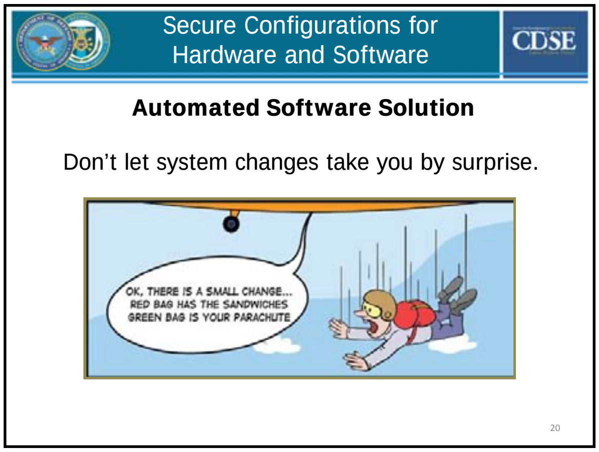
Secure Configurations for Hardware and Software

CDSE

Automated Software Solution

Network Configuration and Change Management (NCCM) – Establishes Configuration Items (CIs) for every networked device to record baseline settings for internal policies and regulatory mandates.

19



Secure Configurations for Hardware and Software

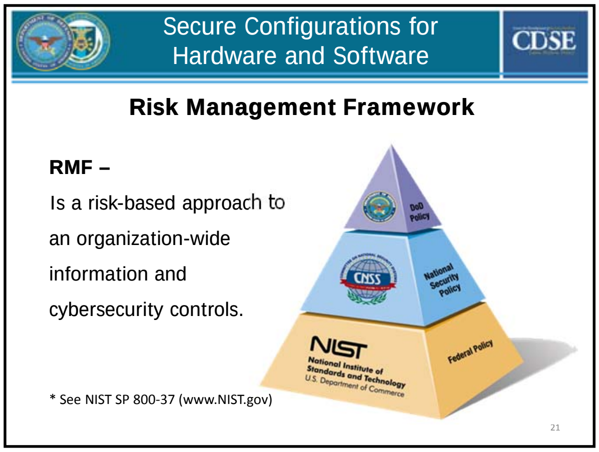
CDSE

Automated Software Solution

Don’t let system changes take you by surprise.

OK, THERE IS A SMALL CHANGE...
RED BAG HAS THE SANDWICHES
GREEN BAG IS YOUR PARACHUTE

20



Secure Configurations for Hardware and Software

CDSE

Risk Management Framework

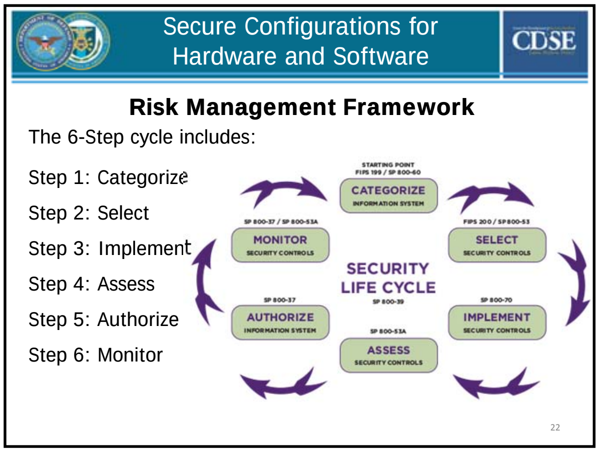
RMF –

Is a risk-based approach to an organization-wide information and cybersecurity controls.

DoD Policy
CNSS
National Security Policy
NIST
National Institute of Standards and Technology
U.S. Department of Commerce
Federal Policy

* See NIST SP 800-37 (www.NIST.gov)

21



Secure Configurations for Hardware and Software

CDSE

Risk Management Framework

The 6-Step cycle includes:

Step 1: Categorize

Step 2: Select

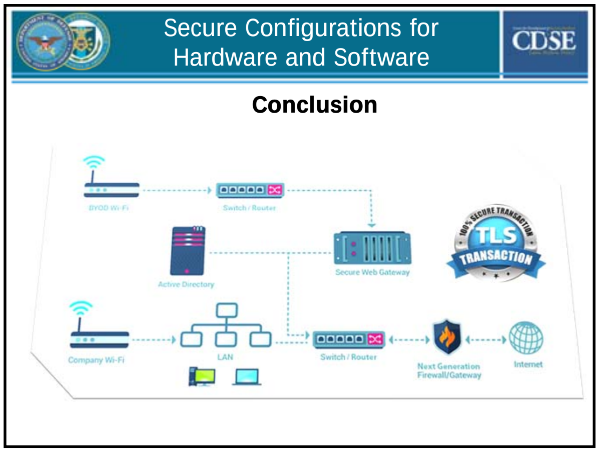
Step 3: Implement

Step 4: Assess

Step 5: Authorize

Step 6: Monitor

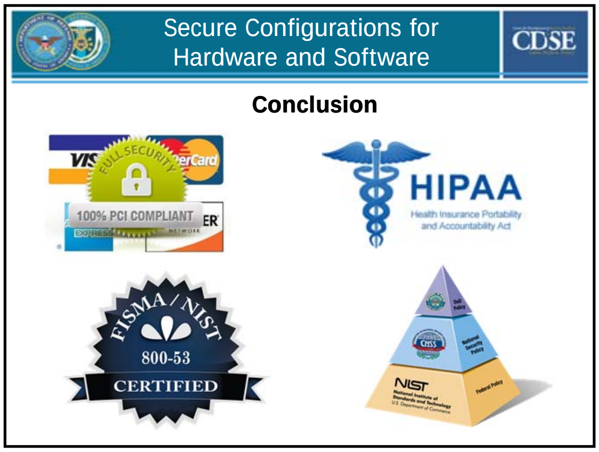
22



Secure Configurations for Hardware and Software

CDSE

Conclusion



Secure Configurations for Hardware and Software

CDSE

Conclusion

Secure Configurations for Hardware and Software

CDSE's website: http://www.cdse.edu

Defense Security Service
Center for Development of Security Excellence
NATIONAL CYBER SECURITY AWARENESS MONTH
IACET
ACE CREDIT

25

Secure Configurations for Hardware and Software

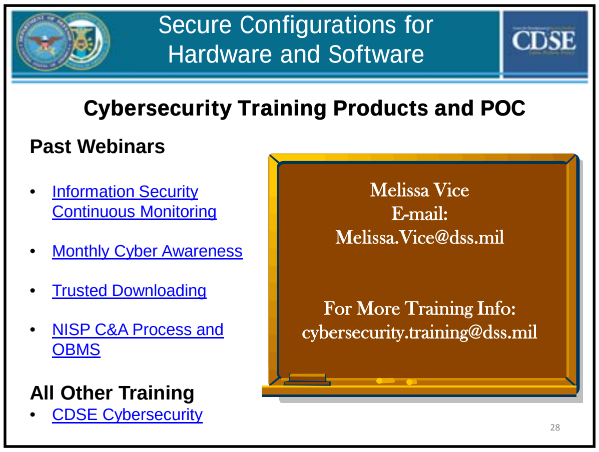
Questions

26

Secure Configurations for Hardware and Software

Feedback

Before we conclude today's presentation, we hope you'll take a moment to participate in our feedback questionnaire. Your feedback is very helpful to us and is greatly appreciated. If you have ideas for future webinar topics, you're able to share these in the questionnaire.



Secure Configurations for Hardware and Software

CDSE

Cybersecurity Training Products and POC

Past Webinars

- Information Security Continuous Monitoring
- Monthly Cyber Awareness
- Trusted Downloading
- NISP C&A Process and OBMS

Melissa Vice
E-mail:
Melissa.Vice@dss.mil

For More Training Info:
cybersecurity.training@dss.mil

All Other Training

- CDSE Cybersecurity

28