



Cyber Security Outreach Program

Jenifer Wallace

Assessment Process

- 1-2 day onsite review:
 - High level network architecture review
 - Physical inspection of control system
 - CIS Critical Security Controls review

CIS Controls

BASIC CIS Controls

1) Inventory and Control of Hardware Assets

2) Inventory and Control of Software Assets

3) Continuous Vulnerability Management

4) Controlled Use of Administrative Privileges

5) Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

6) Maintenance, Monitoring, and Analysis of Audit Logs

CIS Controls

Foundational CIS Controls

7) Email and Web Browser Protections

8) Malware Defenses

9) Limitation and Control of Network Ports, Protocols, and Services

10) Data Recovery Capabilities

11) Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches

12) Boundary Defense

13) Data Protection

14) Controlled Access Based on the Need to Know

15) Wireless Access Control

16) Account Monitoring and Control

CIS Controls

Organizational CIS Controls

17) Implement a Security Awareness and Training Program

18) Application Software Security

19) Incident Response and Management

20) Penetration Tests and Red Team Exercises

Assessment Report

- Onsite debrief and confidential non-public report:
 - Positive observations
 - Better practice elements

Assessment Examples

Current Practice

- Using sticky note for password storage
- 8 char password length
- No formal asset inventory
- Does not build / maintain secure images

Better Practice Elements

- Use secure password manager
- Use passphrases that are longer than 14 char
- Use centralized asset repository
- Remove bloatware, configure security settings, and store secure images in air-gapped environment

Questions?

Jenifer Wallace, CISSP, CISA

Senior CIP Analyst

jvallace@npcc.org