Nuclear Regulatory Commission (NRC)

Overview of the NRC’s Cybersecurity Oversight Program & Inspection Common Issues

Mario Fernandez, Branch Chief (Acting)
Cyber Security Branch (CSB)
Division of Physical and Cyber Security Policy (DPCP)
Office of Nuclear Security and Incident Response (NSIR)

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Agenda

- NRC’s Cybersecurity Branch
- The NRC Cyber Rule and Cybersecurity Plan (CSP) Objectives
- Inspection Common Issues and Lessons Learned
- Key Takeaways
- Q & A

CYBERSECURITY BRANCH

Central focal point for planning, coordinating, and managing agency-wide activities related to cybersecurity at NRC-licensed facilities, and working closely with other federal and international agencies to address cyber-related issues of mutual interest.

POLICY

- Rulemaking
- Licensing
- Resolve Policy Issues
- Guidance Development & Revisions:
  - RG 5.71
  - NEI 08-09

OVERSIGHT

- Inspection Program
- Cyber Events Assessment (CAT)
- Inspector Training
- Federal Partners Engagement

OTHER ACTVITIES

- International
  - IAEA Pubs
  - Training Development
  - Bi/Trilateral
- Research
  - New Technologies
    - Wireless Monitoring
    - SMRs
    - A.I., Drones

10 CFR 73.54 – Cyber Rule

Licensees *shall provide high assurance that digital computer and communication systems and networks associated with:*

Safety-Related, Important-to-Safety, **Security**, & Emergency Preparedness (SSEP) functions

are adequately protected against cyber attacks

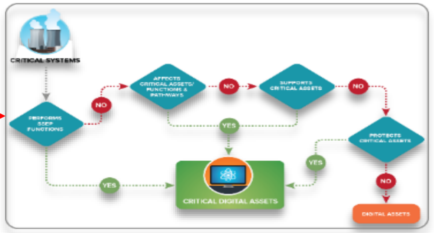
Requirements for a cybersecurity program for new applicants and operating nuclear power plants

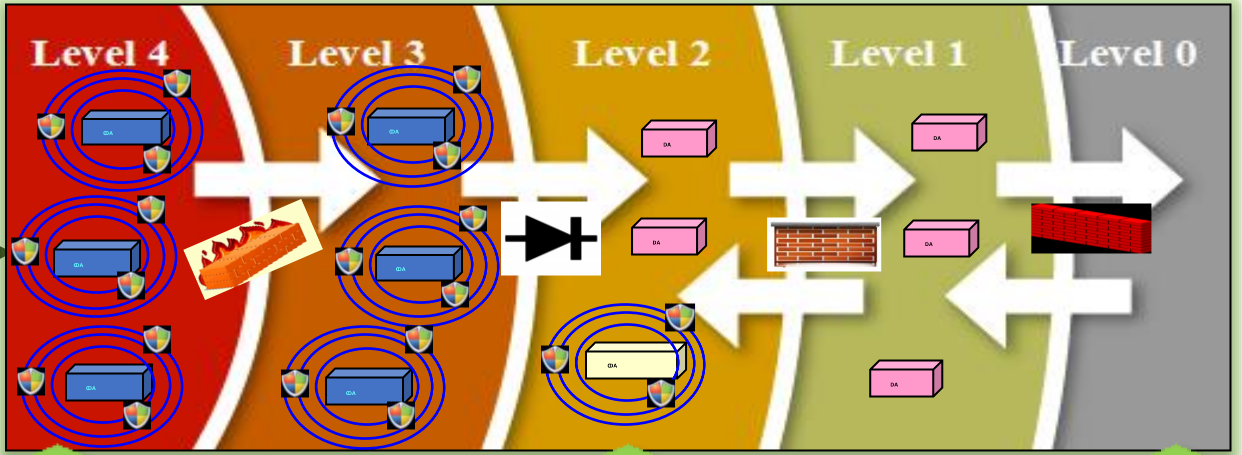
Focus: Prevention of Radiological Sabotage

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NRC 10 CFR 73.54 Rule and Cybersecurity Plan (CSP) Objectives

1. Cybersecurity Assessment Team
2. Identify Critical Digital Assets (CDAs)
3. Implement Defensive Architecture
4. Address Security Controls to CDAs per the CSP





CYBERSECURITY PROGRAM

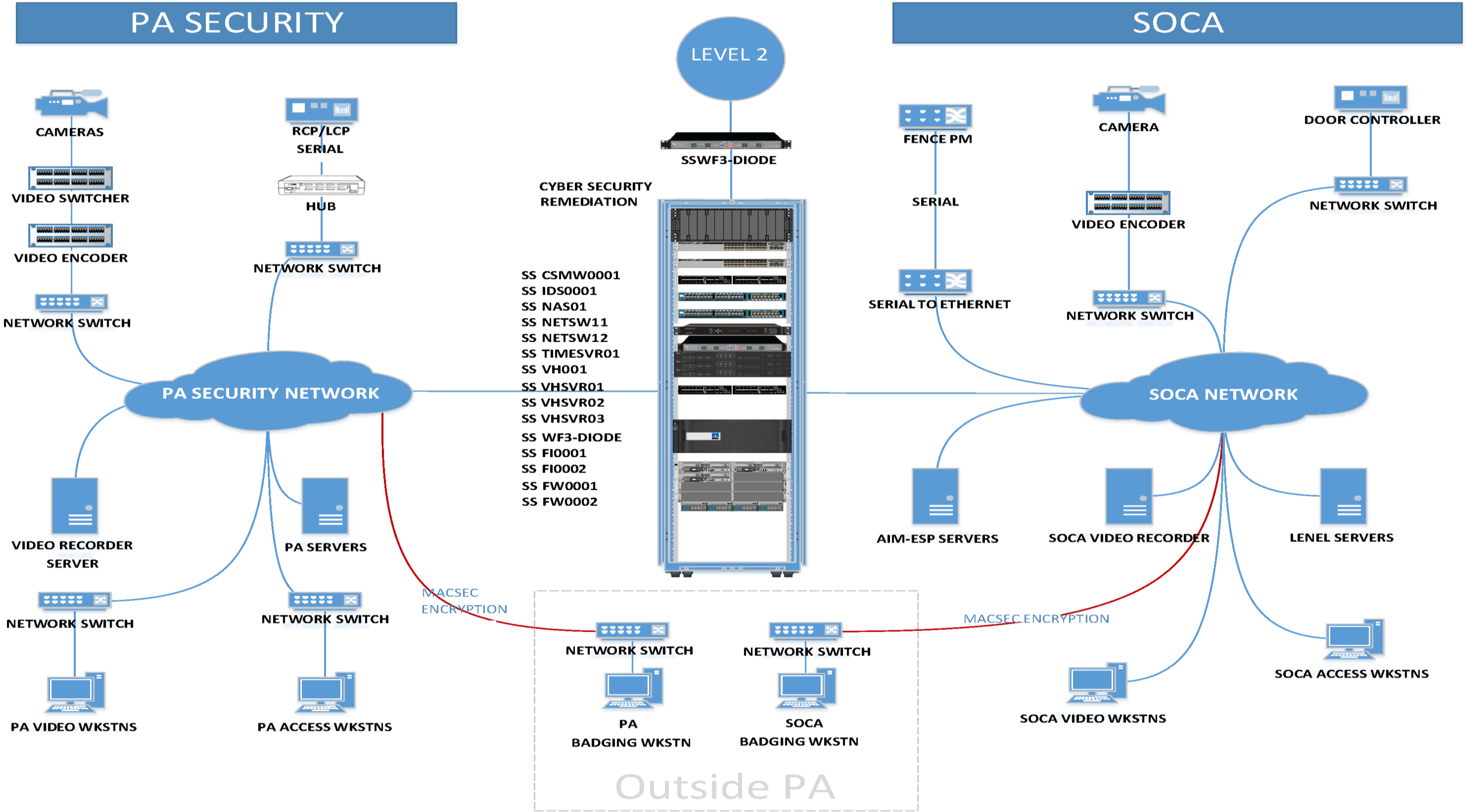
Systems Analysis & Identification	Implement Security Controls	Apply, & Maintain D-I-D	Personnel Training Programs	Evaluate & Manage Cyber Risks	Evaluate MODS	10 CFR 73.77 Cybersec Event Report
Detection & Incident Response	Consequence Mitigation	Vulnerability Management Remediation	Recovery of Affected Systems	Periodic Review	Procedures	Records Retention

Addressing Technical, Management, & Operational Controls and Objectives

- **Implement the controls as written**
- **Apply alternative controls**
  - Document the basis for:
    - Using alternate countermeasures
    - Confirm the alternate mitigates the threat/attack vector the original control intents to protect against
    - Implement the alternate countermeasures and the periodicity associated with the original control
- **Control not applicable**
  - Perform and document analysis
  - Document that attack vector does not exist

INSPECTION COMMON ISSUES AND LESSONS LEARNED

SECURITY NETWORK OVERVIEW



PA SECURITY

SOCA

LEVEL 2

SSWF3-DIODE

CYBER SECURITY
REMEDIATION

SS CSMW0001
SS IDS0001
SS NAS01
SS NETSW11
SS NETSW12
SS TIMESVR01
SS VH001
SS VHSVR01
SS VHSVR02
SS VHSVR03
SS WF3-DIODE
SS FI0001
SS FI0002
SS FW0001
SS FW0002

CAMERAS

VIDEO SWITCHER

VIDEO ENCODER

NETWORK SWITCH

RCP/LCP
SERIAL

HUB

NETWORK SWITCH

PA SECURITY NETWORK

VIDEO RECORDER
SERVER

PA SERVERS

NETWORK SWITCH

NETWORK SWITCH

PA VIDEO WKSTNS

PA ACCESS WKSTNS

MACSEC
ENCRYPTION

NETWORK SWITCH

NETWORK SWITCH

PA
BADGING WKSTN

SOCA
BADGING WKSTN

Outside PA

MACSEC ENCRYPTION

FENCE PM

SERIAL

SERIAL TO ETHERNET

CAMERA

VIDEO ENCODER

NETWORK SWITCH

DOOR CONTROLLER

NETWORK SWITCH

SOCA NETWORK

AIM-ESP SERVERS

SOCA VIDEO RECORDER

LENEL SERVERS

SOCA VIDEO WKSTNS

SOCA ACCESS WKSTNS

D.1.7 Unsuccessful Login Attempts & D.1.8 System Use Notification

Failure to implement threshold enforcement for unsuccessful logins and failure to implement a system use notification on a IVMS switch within the licensee’s security system.

D.5.1 Removal of Unnecessary Services and Programs

Printer used within the Security System was not hardened and had unnecessary programs installed within them. These programs included Novell/Netware networking software and AppleTalk.

D.1.4 Information Flow Enforcement

A security Network Video Recorder (NVR) was moved from Level 3 to Level 2 (LAN) without changing the permissions or status of the CDA.

D.4.3 Password Requirements

A CAS workstation was not enforcing password requirements and was found to have a password that was over 2 years old.

E.10.3 Baseline Configuration

- Failure to reflect an accurate real-time baseline when compared to a documented baseline of a CAS workstation. .
- A CAS workstation was not enforcing password requirements and was found to have a password that was over 2 years old.

A.2.2.11 Use of the Corrective Action Program

A Security System SIEM was out of service for a year. The site made efforts to repair the SIEM with the support of the vendor. The SIEM had reached the end of its life cycle. Review of the SIEM logs were performed manually; however, not all logs from the devices supported by the SIEM were reviewed.

E.6 Defense-in-Depth

Failure to Implement Cyber Security Controls on the Security Data Management System Servers (SMDS).

Upon review of a system assessment, the NRC Inspectors determined that adverse impact to the system was not an adequate basis to NOT implement cyber security controls to the SMDS. Therefore, only physical security controls were implemented for the plant security computer system.

KEY TAKEAWAYS

- The NRC's cybersecurity oversight framework objective is to provide reasonable assurance that digital computer and communication systems and networks associated with safety, important-to-safety, **SECURITY**, emergency preparedness (SSEP) and balance-of-plant functions are adequately protected against **cyber attacks**.

- Licensees' proper implementation of cybersecurity programs and security controls for systems that are heavily supported by vendors depend on a thorough understanding of the NRC requirements, proper documentation, and alternate solutions to meet the requirements of the regulation and their CSPs.

Questions