Don’t Forget the Little Guy: Vulnerability Management in Operational Technology

Alex Assante and Kylie McClanahan

Who Are We

- Kylie McClanahan
  - CTO at Bastazo
  - GCIP

- Alex Assante
  - Security Consultant at NST
  - GCIP, GRID

This Talk

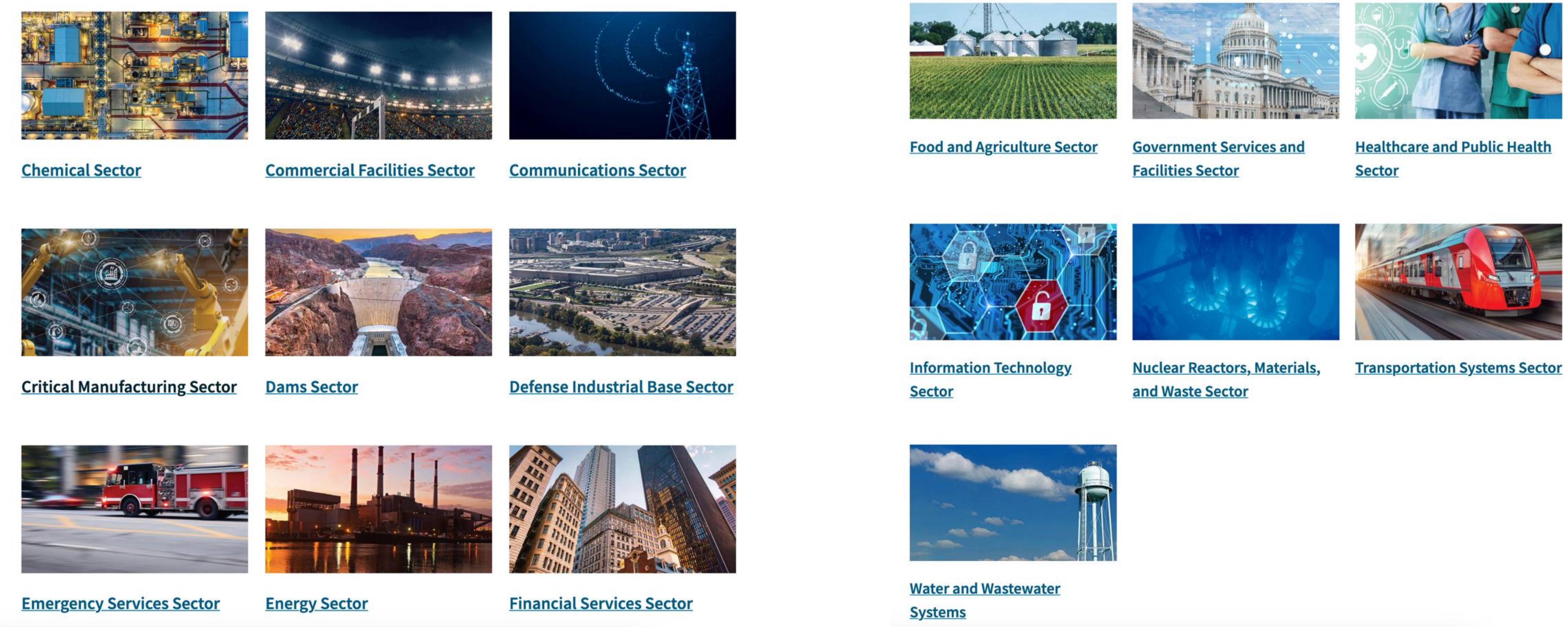
- Is:
    - A conversation about common problems faced in OT
    - Reasons why vulnerability management in OT must be approached differently
- Is not:
    - Not vulnerability management instructions
    - Not a NERC CIP tutorial
    - Not a technical deep dive

What is OT?

Terminology

- Operational Technology
  - Programmable systems or devices that deal with physical environments or consequences
- Industrial Control System
  - A system that controls industrial processes
- Critical Infrastructure
  - Systems vital to national interests

Critical Infrastructure



Chemical Sector

Commercial Facilities Sector

Communications Sector

Critical Manufacturing Sector

Dams Sector

Defense Industrial Base Sector

Emergency Services Sector

Energy Sector

Financial Services Sector

Food and Agriculture Sector

Government Services and Facilities Sector

Healthcare and Public Health Sector

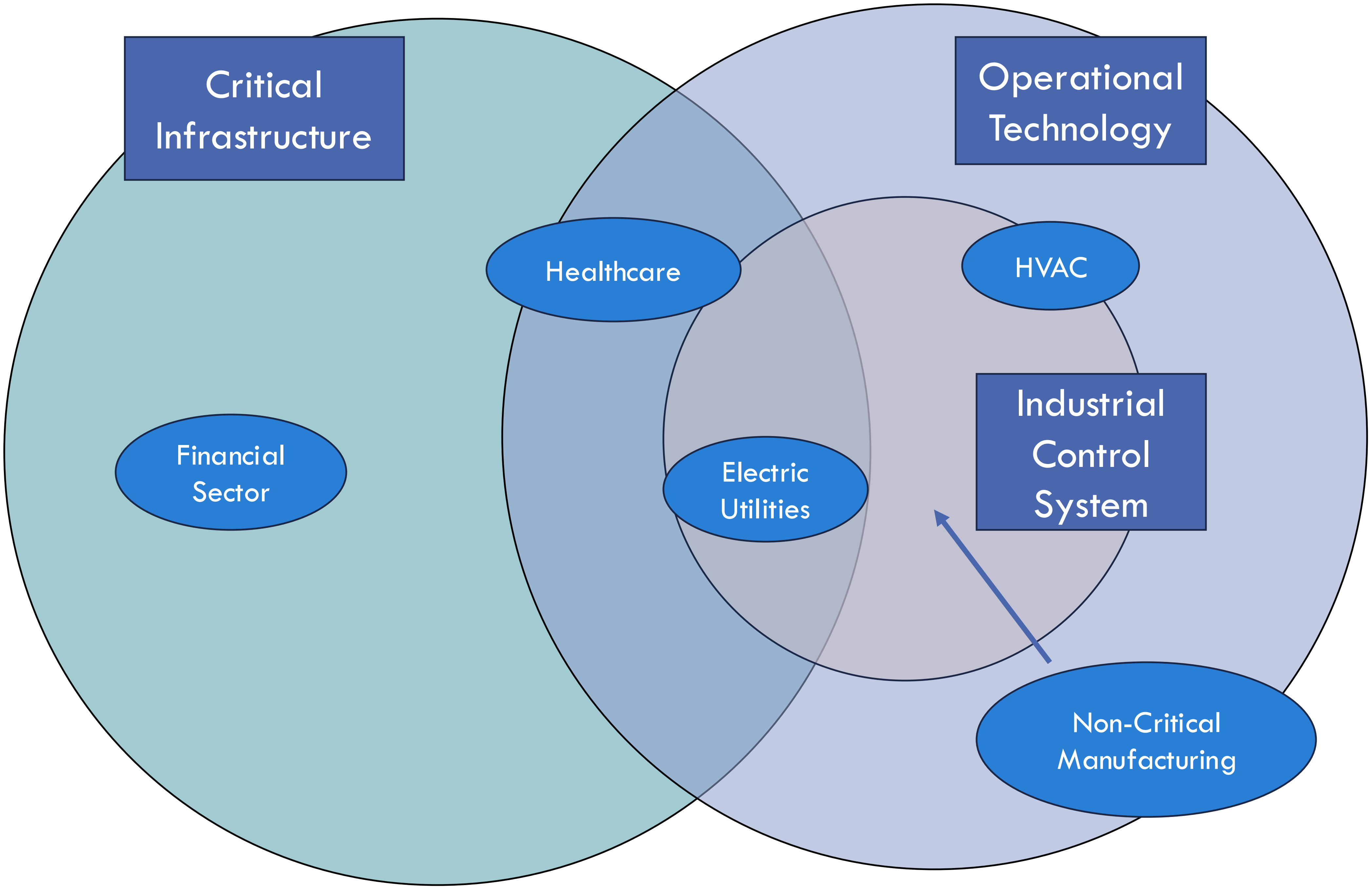
Information Technology Sector

Nuclear Reactors, Materials, and Waste Sector

Transportation Systems Sector

Water and Wastewater Systems

https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors


Critical Infrastructure
Operational Technology
Healthcare
HVAC
Industrial Control System
Financial Sector
Electric Utilities
Non-Critical Manufacturing

The CIA Triad

CONFIDENTIALITY

INTEGRITY

AVAILABILITY

An Entirely Different Perspective

SAFETY

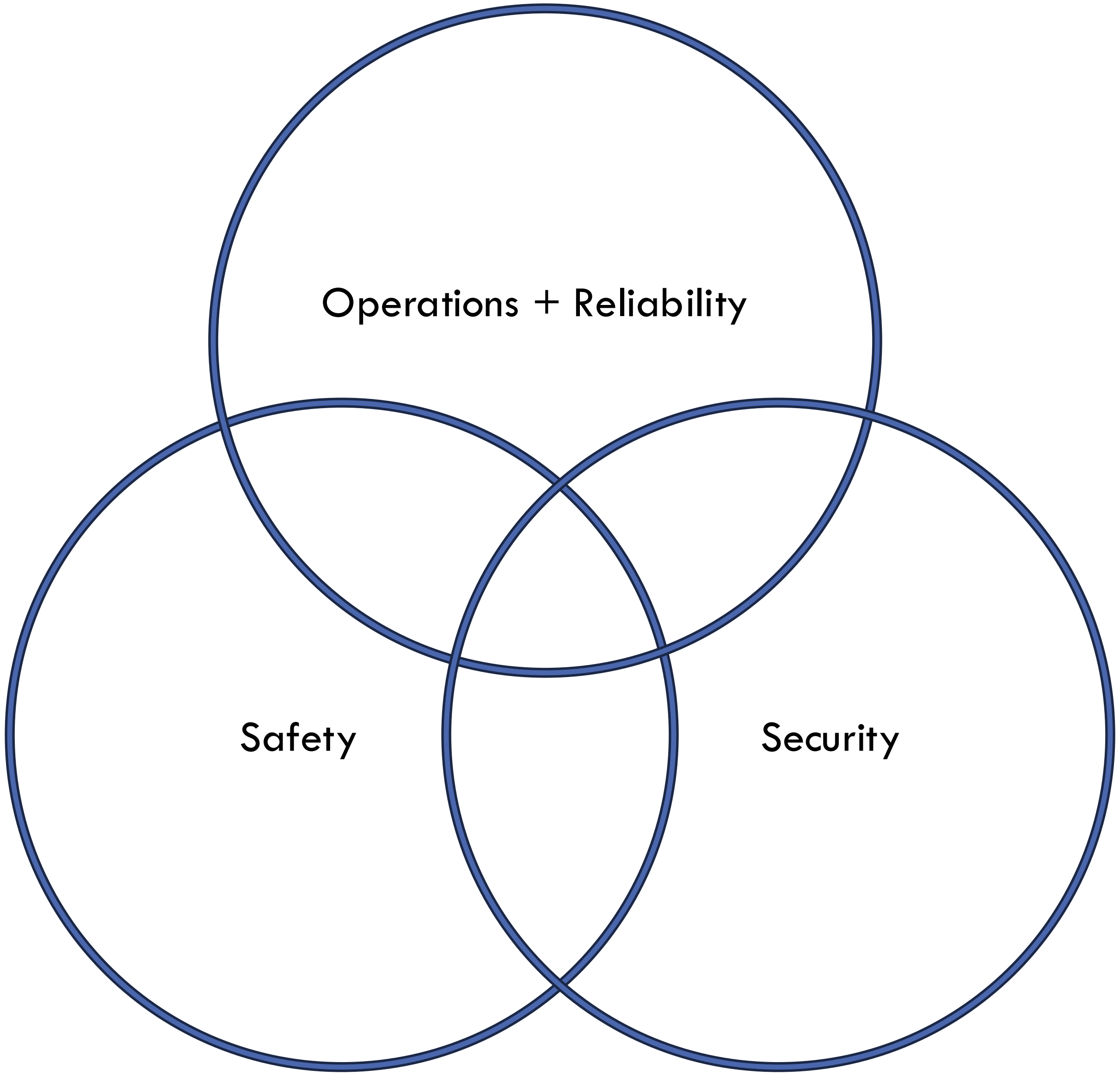
RELIABILITY

PERFORMANCE

Priority of Utilities

Balance is key. Cybersecurity is critical for ensuring safe and reliable operations! What isn't essential is security for security's sake.

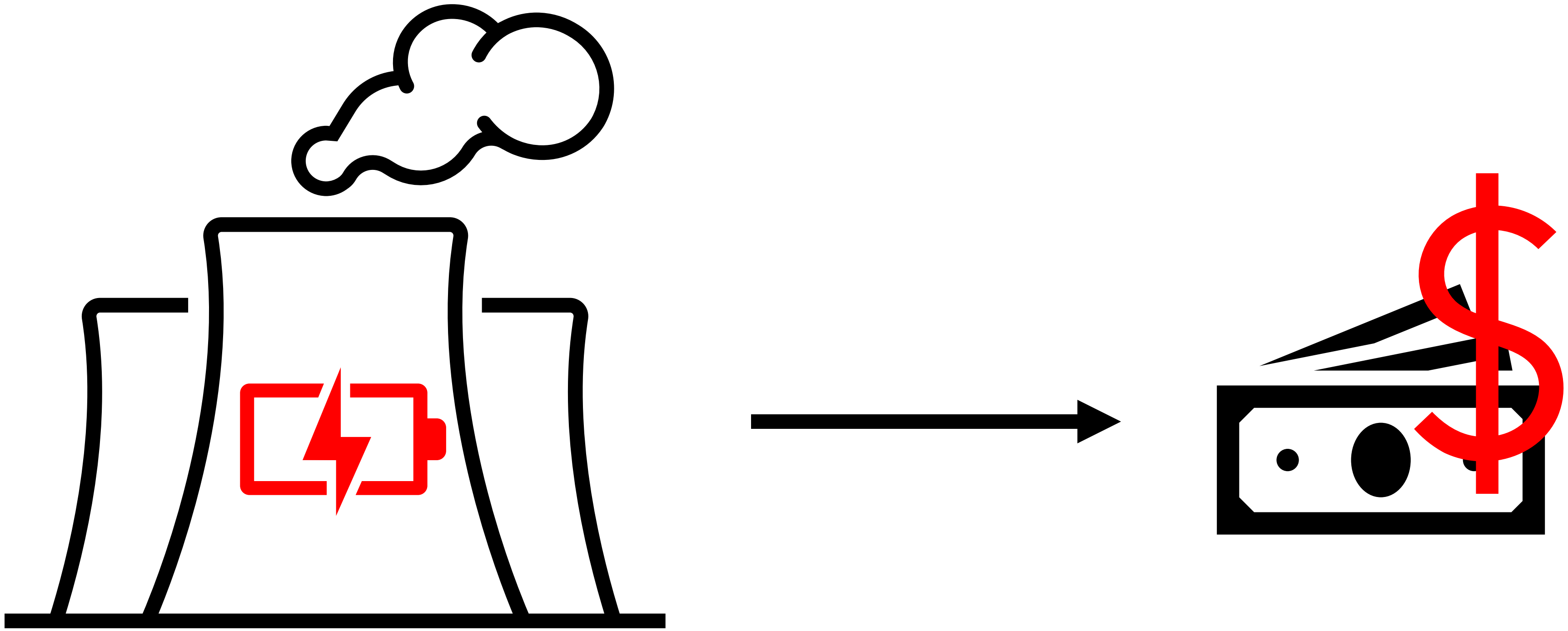
It's about managing risk, not chasing perfection.



What’s at Stake?

Vulnerability management affects core utility priorities: operations + reliability, safety, and security. Patching isn’t just about security or compliance – it’s about keeping the lights on!

A Dark Day At The Plant



You Should Care If…

- You work in industry
  - Regulated or unregulated!
- You’re a vulnerability researcher
- You do vulnerability response
- You work at a vendor/OEM

OT Reality Check

- Reliability first!
- Continuous operations
- Maintenance and cybersecurity patches can't easily interrupt production

Why Is Vulnerability Management Hard?

- Non-Homogenous Environments
- Asset Discovery
- EOL/EOS/Legacy systems
- Devices for Operation and not for Security
- Geographical Dispersion
- The Availability Problem
- Limited Resources
- Vendor Maintenance

Compliance vs. Security

Compliance ≠ Security
Security ≠ Compliance

STANDARDS INTERPRETATION

MINIMUM LEVEL OF SECURITY

NERC CIP Standards

Standard	Title	Standard	Title
CIP-002	BES Cyber System Categorization	CIP-009	Recovery Plans for BES Cyber Systems
CIP-003	Security Management Controls	CIP-010	Configuration Change Management and Vulnerability Assessments
CIP-004	Personnel & Training	CIP-011	Information Protection
CIP-005	Electronic Security Perimeter(s)	CIP-012	Communications Between Control Centers
CIP-006	Physical Security of BES Cyber Systems	CIP-013	Supply Chain Risk Management
CIP-007	System Security Management	CIP-014	Physical Security
CIP-008	Incident Reporting and Response Planning		

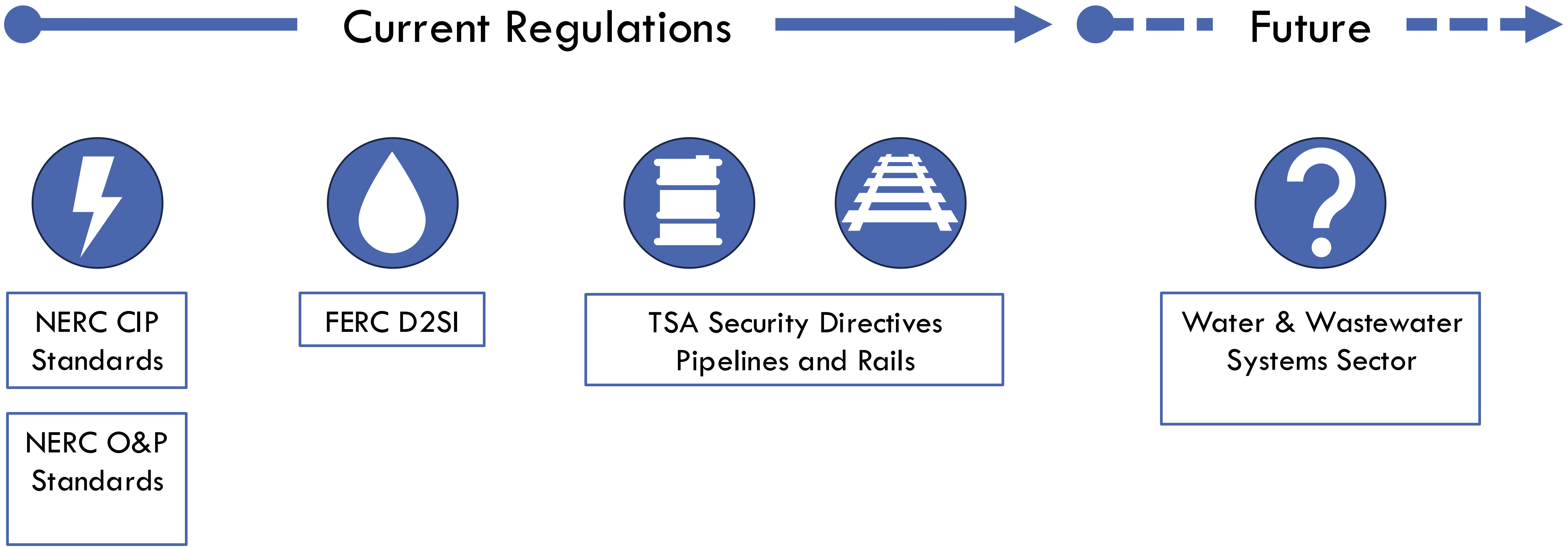
CIP-007 System Security Management

- R1: Logical and Physical Port Security
- R2: Security Patch Management
  - Discovery and notification of available cybersecurity patches
  - Once every **35 Calendar Days** evaluate security patches for applicability
  - Within **35 Calendar Days** of the evaluation: apply the patch; or create a dated mitigation plan; or revise an existing mitigation plan
- R3: Malicious Code Prevention
- R4: Security Event Monitoring
- R5: System Access Control

CIP Calendar of Doom

70 Days = **35 days** for evaluation + **35 days** for application

The OT Regulatory Landscape



Current Regulations

Future

NERC CIP Standards

NERC O&P Standards

FERC D2SI

TSA Security Directives Pipelines and Rails

Water & Wastewater Systems Sector

Once Is Enough

- The future of regulation is written by today's vulnerabilities
- It only takes one incident to become regulated.

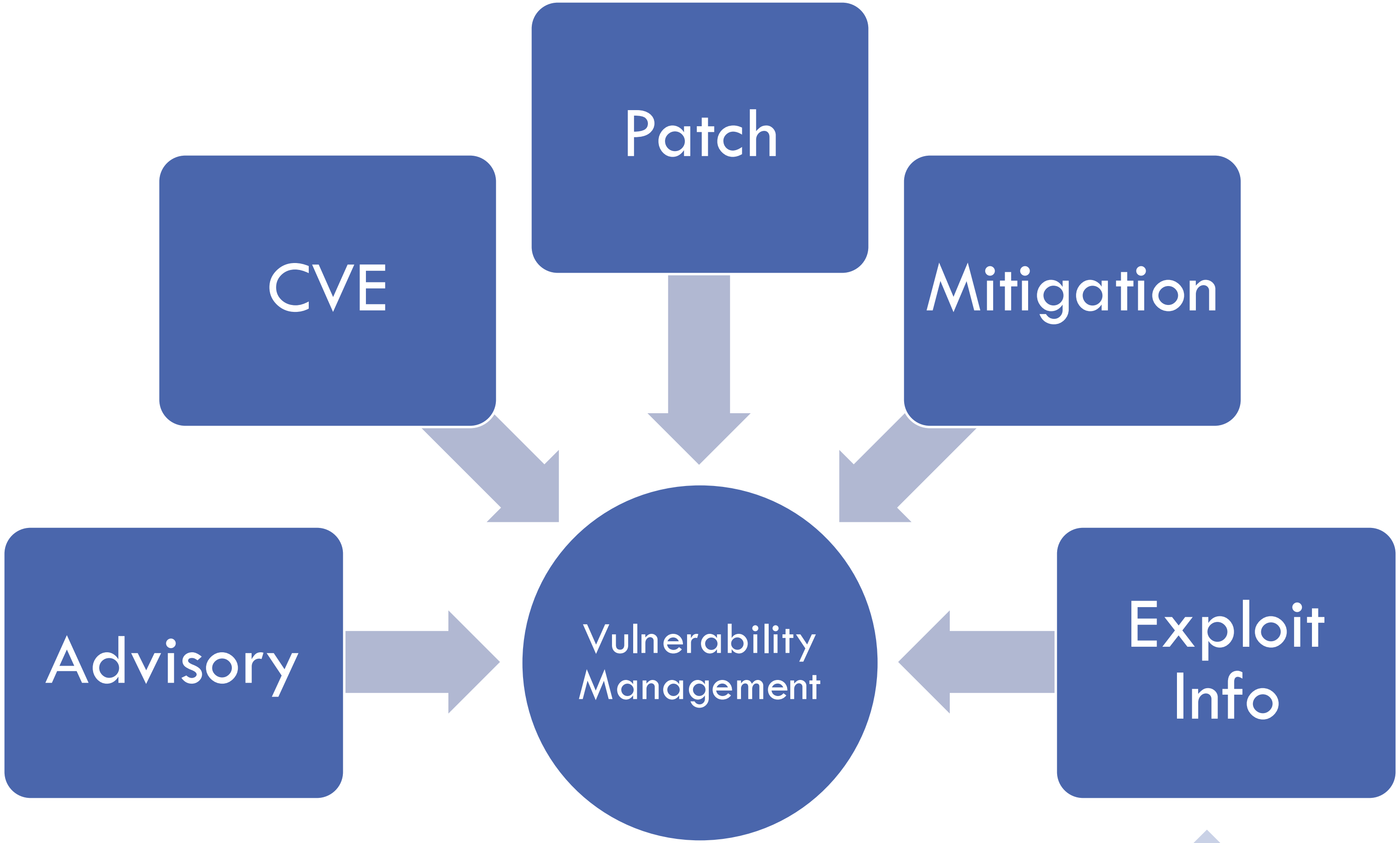
By Lokal_Profil, CC BY-SA 2.5, https://commons.wikimedia.org/w/index.php?curid=3201241

Data Needs

Vulnerability Metadata

- Not always helpful for practitioners
  - Does it impact the approach to remediation?
  - Does it require cybersecurity knowledge?
- Data quality
  - Missing, out-of-date, or incorrect CPEs

Complex Data Relationships



Patch

CVE

Mitigation

Advisory

Vulnerability Management

Exploit Info

Vendor Security Advisories

- Provide crucial information
  - Affected products and versions
  - CVE-to-patch mapping
  - Mitigation/workaround
  - Revision history
- And yet…
  - Aren’t machine readable
  - No access to a published feed
  - Are behind a login

https://imgflip.com/i/9pyowt

Common Security Advisory Format

- Structured language to create, update, and exchange security advisories
- Machine-readable
- Provides CVE-to-remediation mapping
- Allows for automation
  - Audit evidence in regulated spaces

Out of 447 CNAs, 18 provide CSAF

(that we know of, as of April 2025)

Call To Action

- For OT:
  - Change your mindset
  - Proactive vulnerability focus
  - Secure operations sustainably
- For IT or vulnerability folks:
  - Consider operational limitations
  - Provide CSAF

Thank you!

- Kylie McClanahan
  - kylie@bastazo.com
  - LinkedIn
  - https://bastazo.com

- Alex Assante
  - aassante@nst.us
  - LinkedIn
  - https://nst.us