Cyber and Physical and Human, Oh My!

JESS SMITH, PHD, CISSP

PNNL
Data Analytics for the Smart Grid at WSU
PNNL-SA-128736
Lions and Tigers and Bears!

The current buzzword: Cyber/Physical/Human

Translation: Intelligent electronic devices and their networks, the world they interact with, and the humans that interact with them.
Two Problems in ICS Security Data Analytics:

1. Getting data
2. Understanding data
Getting Data From Devices

▶ In edge devices:
  - Lack of flexibility
  - Lack of capability
  - Lack of proper configuration

▶ In network devices:
  - Lack of proper configuration

Device Designers, Manufacturers
Implementers and Operators
Getting Data Over the Network

Bandwidth and Speed
Getting Data Over the Network

Priority

- Operational data comes first!
- Status data comes second
- Security data comes third
Humans and Getting Data

- Getting data ON humans
- Getting data FROM humans
How do we combine the cyber, physical, and human data?
Designing For Understanding

- Complex system designs and interfaces obscure relevant information and can cause users to act incorrectly during a security event.
Lab-Directed R&D

- Analysis In Motion (AIM)
- Proactive Adaptive Cybersecurity Framework for Control (PACiFiC)
- Information and Infrastructure Integrity Initiative

INFORMATION AND INFRASTRUCTURE INTEGRITY INITIATIVE (IIII)
Questions?

Jess Smith, PhD, CISSP
Jess.Smith@PNNL.gov

PNNL-SA-128736