Pacific Northwest
NATIONAL LABORATORY

PNNL-SA-159884

Synchrophasor Cybersecurity for Grid Operations

February 24, 2021

Scott R. Mix, CISSP
Grid Cybersecurity Specialist, PNNL

U.S. DEPARTMENT OF ENERGY BATTELLE

PNNL is operated by Battelle for the U.S. Department of Energy

Agenda

- Uses of Synchrophasor Data
- Overview of Cybersecurity for Operational Technology
- Cybersecurity Controls
  - Applications to Synchrophasor environments

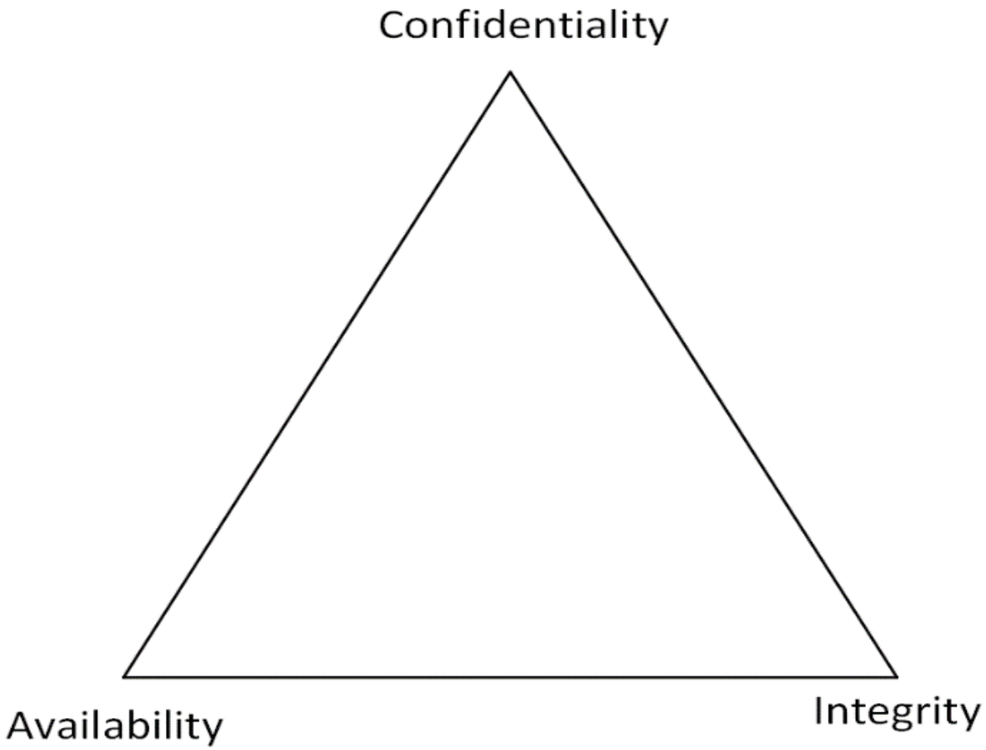
Uses for Synchrophasor Data

- Operator Situational Awareness
- Alarming
- Frequency Stability Monitoring
- Voltage Stability Monitoring
- Island Detection
- Linear State Estimator
- Oscillation Detection
- Disturbance Monitoring
- Postulated Preventative Actions
- Control Applications – e.g., Static and Dynamic Remedial Action Schemes (RAS)
- Automatic RAS Arming
- Out of Step Protection
- Stability Controls (Transient, Voltage, Frequency)
- Fault Location
- Equipment Performance and Maintenance Monitoring
- Model Validation
- Forensic Disturbance Analysis
- Restoration
- Adaptive Protection

Cybersecurity

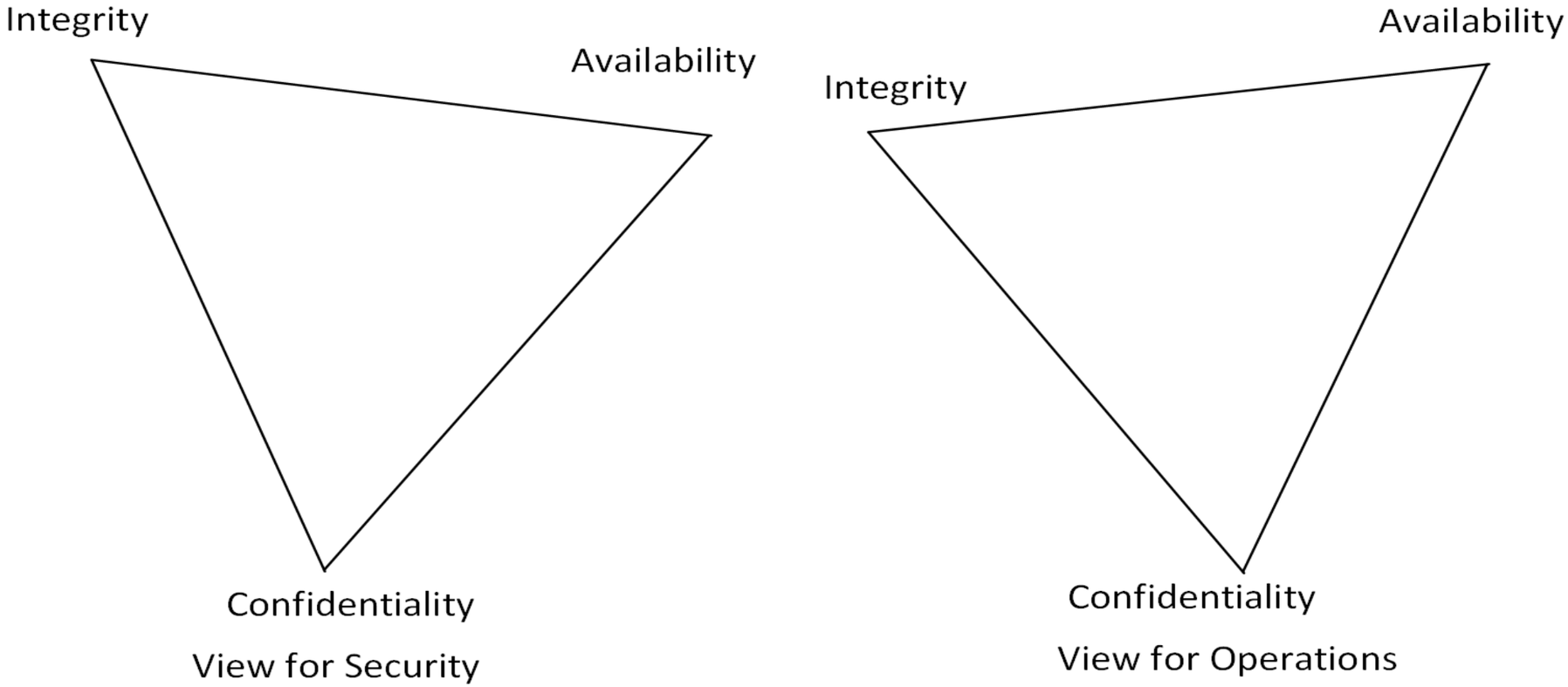
- Synchrophasor data is being used in real-time control applications and situational awareness
- Synchrophasor data use is functionally very similar to existing Remote Terminal Units (RTU) telemetry data in real-time analytical and protection applications
- Resource utilization for non-real time uses
- Operational decisions made using synchrophasor data expect the data to be available and correct
- Phasor Measurement Units (PMUs) and synchrophasor data should be protected in the same manner as telemetry RTUs, protection and control relays, or other sources of data

Traditional Information Technology (IT) Cybersecurity View



- Focus on protecting “information”
- Apparent preference for confidentiality
- Data has long life

Operational Technology (OT) Cybersecurity View



- Focus on protecting the “process” and its associated data
- Data often publicly available or easily obtained
- Data often has short life

Sources for Cybersecurity Controls

- Standard and Recommended practices are available from a number of organizations:
  - IEC – International Electrotechnical Commission
  - ISO – International Standards Organization
  - ISA – International Society of Automation
  - NERC – North American Electric Reliability Corporation
    - ✓ CIP – Critical infrastructure Protection standards
  - NIST – U.S. National Institute of Standards and Technology
    - ✓ SP 800 – Special Publication series 800
    - ✓ NISTIR – NIST Interagency or Internal Reports

Sources for Cybersecurity Controls

- ISO/IEC 27k family, specifically 27001, 27002, 27019
  - ISO/IEC 27001 and 27002 are general IT controls, but portions can be applied to OT systems
  - ISO/IEC 27019 contains controls and control modifications specific to process control systems in the energy industry
- NIST SP800-53 and SP 800-82
  - SP 800-53 contains general IT controls
  - SP 800-82 applies the 800-53 controls to OT systems
- NISTIR 7628 Rev. 1
  - Guidelines for Smart Grid Cyber Security
- ISA/IEC 62443 (formerly ISA-99)
  - Primarily for industrial control systems like those found at power plants
- NERC CIP
  - High level, few implementation specifics
  - Required* on transmission-level equipment for North-American utilities

* - if the PMUs are designated as BES Cyber Assets

Recommendations based on ISO/IEC 27k and NERC CIP

- ISO/IEC 27k standards are the international standard for information security
  - Primarily focused on Information Technology (IT) security
  - ISO/IEC 27019 (2017) provides extensions for the energy utility industry
    - ✓ Additional guidance on controls specified in ISO 27002 (marked with “+”)
    - ✓ Additional controls specific to energy utility industry (marked with “*”)
- Initial NERC CIP concepts (in 2002) were based on ISO 17799, which is now the ISO 27000 family

High-level Security Objectives in 27001/27002

- Information Security (Cybersecurity) Policies
- Organization of Information Security (Cybersecurity)
- Human Resource Security
- Asset Management
- Access Control
- Cryptography
- Physical and Environmental Security
- Operations Security
- Communications Security
- System Acquisitions, Development, and Maintenance
- Supplier Relationship
- Information Security (Cybersecurity) Incident Management
- Information Security (Cybersecurity) Aspects of Business Continuity Management
- Compliance

Information Security (Cybersecurity) Policies

- Cybersecurity policies define the framework for all other cybersecurity actions
  - Used to establish governance
  - Governance can be used to establish budgets and resource assignments
- Policies should be written at a high level describing overarching goals
  - For example, “Protect synchrophasor data from unauthorized modification or disclosure”
- Policies need to be approved by management, reviewed periodically, and updated when necessary
- Policies should be developed for all objectives and address all controls at a high level

ISO 27001 A.5; NERC CIP-003

Information Security (Cybersecurity) Policies

- Individual procedures and practices based on the cybersecurity policy need to be developed:
  - All practices and procedures should trace back to a policy statement – if they don't, either a policy is missing, or the practice is unnecessary
  - Each policy statement may have multiple practices; each practice may have multiple procedures
  - Practices should implement the policies through individual procedures
    - ✓ May need different practices for different environments (i.e., securing PMUs in the field may be different than securing Phasor Data Concentrators (PDC) in the control center)
    - ✓ Will need different procedures for different hardware or environments (i.e., the procedure for securing a Vendor X PMU may be different than securing a Vendor Y PMU)
  - For example:
    - ✓ Practices for controlling access to PMUs and their configuration, and for protecting synchrophasor data from modification or disclosure in transit
    - ✓ Procedures for password construction and group/role accesses, and for configuring levels of digital hashes or encryption for communications

Organization of Information Security (Cybersecurity)

- + Responsibility for cybersecurity functions should be defined and resources allocated
- Responsibilities should be segregated to minimize unauthorized misuse
- + Contacts should be established and maintained with professional organizations and groups, and with government or law enforcement organizations
- Cybersecurity should be included in all project planning activities
- * Risks from third parties should be identified and mitigated
- * Identified security requirements should be addressed prior to use in operational environments
- + Mobile device and teleworking policies and procedures should be created and enforced

ISO 27001 A.6; *ISO 27019 6, +ISO 27019 6; NERC CIP-003, CIP-013, EOP-004

Organization of Information Security (Cybersecurity)

- OT knowledgeable staff should be included in the cybersecurity organization
  - OT may have its own cybersecurity organization that focuses only on OT concepts and practices
- Information sharing should be part of the risk assessment process
  - Some information sharing may be mandated by policy or regulation
  - Some information sharing may be voluntary
- Incident response procedures should consider the operational environment and equipment when establishing contacts
- The E-ISAC (Electricity Information Sharing and Analysis Center) should be a prime resource for sharing OT cybersecurity information

Human Resource Security

- + Human resources security includes pre-employment checking and ongoing verification
  - Staff with access to critical functions may need more scrutiny
  - + Contracted staff should indicate responsibilities in their contracts
- Procedures for re-verification on job transfer and promotions
- Procedures for removal of access when no longer needed (termination or transfer)
- + Cybersecurity awareness and training should be provided to all staff and contractors
- Formal disciplinary actions for failure to follow cybersecurity policies
- Post-employment obligations should be defined and enforced in contracts and termination agreements

ISO 27001 A.7; +ISO 27019 7; NERC CIP-004, CIP-013

Human Resource Security

- Cybersecurity awareness and training specific to field locations and substation equipment
  - Updated when equipment or environments change
  - Annual refresher
  - Include in tailgates (similar to “safety minutes”)
  - Include for contractors and vendors, as well as staff
- Background checks – initial and on-going
  - Formal review every 5-10 years
  - On-going supervisor observation and oversight
  - Consider different levels of checks for different job classes
  - Verification / audit process for contractors

Asset Management

- + Tracking of equipment – Asset inventory
  - Includes software/firmware management
  - May also include software and data/information as an asset – for example, application programs, network models
  - + Ownership tracking for all assets in inventory
  - Return of personally-assigned assets (such as laptops and access credentials) upon termination or transfer
- + Information classification
  - Labeling
  - Information handling
- Media handling
  - Management of removeable media
  - Disposal of media
  - Physical transfer of media

ISO 27001 A.8; +ISO 27019 8; NERC CIP-002, CIP-003, CIP-004, CIP-007, CIP-010, CIP-011

Asset Management

- Generally fixed in location, function, and number for equipment
  - Make and model of hardware
  - Software/firmware versions and patch level
  - Hardware or software installed features (even if not “enabled”)
  - Track laptops used for testing and maintenance
  - Track removeable media used for data, configuration, or software updates
- Understand sensitivity of data where appropriate
  - Disturbance data may be more sensitive than steady-state data

Access Control

- Network and network services access
  - + Access granted based on busines need
- User access
  - + Registration and de-registration process
  - Provisioning process
  - Restricted and controlled privileged access
  - + Controlled access to “secret authentication information” (shared passwords)
  - Access granted and controlled based on policy
  - + Access controlled by “secure log-on procedure”
  - Removal of access on termination or job change

ISO 27001 A.9; +ISO 27019 9; NERC CIP-003, CIP-004, CIP-005, CIP-006, CIP-007, CIP-011

Access Control

- User responsibilities
  - Especially when using shared accounts
- System and application access control
  - Access to information
  - Password Management
  - Use of privileged utility programs
  - + Access to source code

ISO 27001 A.9; +ISO 27019 9; NERC CIP-003, CIP-004, CIP-005, CIP-006, CIP-007, CIP-011

Access Control

- What staff (individually or by job function) have logical or physical access?
  - Tracking access
  - Provisioning and revocation procedures
  - Pre-requisite requirements for granting access (e.g., training)
  - Oversight and review of access
- What systems have autonomous access to other systems?
  - Tracking access
  - Provisioning and revocation procedures
  - Oversight and review of access
- Procedure in place for staff transfer
- Shared accounts
  - Credential tracking
  - Procedures for changing passwords following transfer or termination

Cryptography

- Key management
  - + Procedures for protecting private keys

ISO 27001 A.10; +ISO 27019 10; CIP-006

Cryptography

- Appropriate uses for cryptography
  - Ensuring Confidentiality, Integrity
- Considerations for autonomous and real-time operations
  - Selection, Location and Maintenance of Certificate Authorities (CA)
  - Handling expired keys
  - Handling revoked keys
  - Handling loss of CA access
  - IEC 62351-9 for additional suggestions – especially for certificate management
  - Digital certificates can be used for Identity, which can be linked to Authorization

Physical and Environmental Security

- Secure areas
  - + Physical security perimeter
  - + Physical entry controls
  - Room and facility security
  - External and environmental threats
  - Working in secure locations
  - Delivery and loading areas
  - * Securing control centers
  - * Securing equipment rooms
  - * Securing peripheral sites (e.g., substations)

ISO 27001 A.11; *ISO 27019 11, +ISO 27019 11; NERC CIP-003, CIP-006, CIP-007, CIP-014

Physical and Environmental Security

- Equipment security
  - + Siting and protection
  - + Support infrastructure (power, other utilities, heating, ventilation, and air conditioning [HVAC], etc.)
  - + Cabling security
  - Equipment maintenance
  - Removal of assets
  - Security of off-premises assets
  - Secure disposal or reuse of assets
  - Unattended user equipment
  - + Clear desk and clear screen
  - * Security in external party premises
  - * Security for customer-sited assets
  - * Interconnected control and communication systems

ISO 27001 A.11; *ISO 27019 11, +ISO 27019 11; NERC CIP-003, CIP-006, CIP-007, CIP-014

Physical and Environmental Security

- Secure equipment against tampering
- Protect local (intra-substation) communications (physically and logically)
- Work orders for maintenance activities
- Track physical access to unstaffed locations
  - Track physical access against work orders

Operations Security

- + Documented operating procedures
- + Controlled changes to management procedures
- Capacity management
- + Separation of development, testing, and operational environments
- + Malware protection
- Information backup
- + Event logging
  - Protection of logged information
  - Administrator and operator logs

ISO 27001 A.12; +ISO 27019 12; NERC CIP-003, CIP-006, CIP-007, CIP-009, CIP-010

Operations Security

- + Clock synchronization
- + Software installation procedures
- + Vulnerability Management
- Restrictions on software installation
- Audit control
- * Legacy systems
- * Safety systems

ISO 27001 A.12; *ISO 27019 12, +ISO 27019 12; NERC CIP-003, CIP-006, CIP-007, CIP-009, CIP-010

Operations Security

- Establish a testing lab
  - Validate testing and installation procedures
  - Verify new equipment (especially new models or suppliers)
  - Verify software updates
  - Calibration
- Establish backup and recovery procedures
  - Maintain the ability to re-create environments (backups or equivalent)
  - Procedures / Instructions for recovery
- Secure time sources and time distribution
  - Coordinated Universal Time (UTC) vs International Atomic Time (TAI) vs local time
    - ✓ Daylight savings time
    - ✓ Leap Seconds
  - Consistent time source for operational and non-operational (e.g., logging) functions

Communications Security

- + Network controls
- Security of network services
- * Segregation of networks
- * Security of process control data communications
- * Logical connection of external process control systems
- Information transfer
  - Agreements for information transfer
  - Electronic messaging
  - Confidentiality and non-disclosure agreements

ISO 27001 A.13; *ISO 27019 13 +ISO 27019 13; NERC CIP-005, CIP-012

Communications Security

- Segregate operational networks from non-operational networks
- Protect wide-area networks from compromise (confidentiality, integrity, and availability)
  - Data may be operationally sensitive or may be market sensitive
- Consider redundant communications paths
- Establish information sharing agreements with third parties to include non-disclosure
  - Reliability Coordinators, Independent System Operators (ISO), Regional transmission Organizations (RTO)
  - Academic and research organizations

System Acquisitions, Development, and Maintenance

- + Cybersecurity requirements in specifications for new systems
- Securing applications on public networks
- Protecting application services transactions
- Secure development
- System change control
- Technical review of applications after operating platform changes
- Restrictions on software changes
- Secure system engineering principles
- Secure development environment

ISO 27001 A.14; +ISO 27019 14; NERC CIP-007, CIP-010, CIP-013

System Acquisitions, Development, and Maintenance

- Outsourced development
- System security testing
- System acceptance testing
- * Principle of least functionality
- Test data

ISO 27001 A.14; *ISO 27019 14; NERC CIP-007, CIP-010, CIP-013

System Acquisitions, Development, and Maintenance

- Agreements with third party designers, integrators, suppliers, and construction
- Factory and site acceptance tests
  - Test data (sources) used, especially in factory tests
  - Include functionality and security tests
- Third party maintenance agreements
  - Full service
  - Advisory (e.g., update notification services)

Supplier Relationship

- Supplier access risk mitigation in agreements
- + Addressing security within supplier agreements
- Technology supply chain
- Review and audit of supplier services
- Managing changes to supplier services

ISO 27001 A.15; +ISO 27019 15; NERC CIP-013

Supplier Relationship

- Establish working relationships with suppliers
  - Contracts
  - User groups
- Return-to-factory service
  - Procedures to protect embedded data
- Considerations on how to switch suppliers
  - Failure to perform
  - Supplier stops supporting product
  - Supplier goes out of business

Information Security (Cybersecurity) Incident Management

- Responsibilities of staff
- Reporting cybersecurity events
- Reporting cybersecurity weaknesses
- Assessment of cybersecurity events
- + Response to cybersecurity incidents
- Learning from cybersecurity incidents
- Collection of evidence

ISO 27001 A.16; +ISO 27019 16; NERC CIP-003, CIP-008, EOP-004

Information Security (Cybersecurity) Incident Management

- Plan for continued operation during incident
- Post-event analysis
  - Document lessons learned
- Test and exercise incident response plans
  - Use laboratory environment if available
- Incident may trigger recovery plans even if no damage
  - For example, outdated software containing vulnerability should be replaced on other installations

Information Security (Cybersecurity) Aspects of Business Continuity Management

- Planning cybersecurity continuity
- Implementing cybersecurity continuity
- Verify, review, evaluate cybersecurity continuity
- + Redundancies
- * Emergency communication

ISO 27001 A.17; *ISO 27019 17, +ISO 27019 17; NERC CIP-009, EOP-004

Information Security (Cybersecurity) Aspects of Business Continuity Management

- Plan for continued operation during incident
- Recovery procedures
  - Focus on restoration
  - May also be used to update systems to latest tested versions
- Post-event analysis
  - Document lessons learned
- Test and exercise recovery plans
  - Use laboratory environment if available

Compliance

- + Identify applicable legislation and contractual requirements
- Intellectual property rights
- Protection of records
- Privacy and protection of Personally identifiable information (PII)
- Regulations concerning cryptographic controls
- Independent review of cybersecurity
- Compliance with policies and procedures
- + Technical compliance review

ISO 27001 A.18; +ISO27019 18; NERC CMEP

Compliance

- Determines whether the cybersecurity policies and procedures have been followed
  - For NERC CIP, this may be an actual or mock audit
  - For other standards or practices (including internally developed and enforced practices), could be self-assessments or assessments from independent third parties

Compliance

- Compliance activities can include internal assessments, checklists completed during maintenance activities, third party assessments, etc.
  - Compliance is *not necessarily* a formal audit
- Cybersecurity reviews or informal audits may also be conducted and engagements with external assessors and auditors may be performed
  - Formal internal audits should be conducted by an independent department
    - ✓ "Independent" of the organization that manages development of the policy, practice, and procedure documents
    - ✓ Often performed by the independent "Internal Audit" function of an organization
  - May include a review of cybersecurity policies and procedures for completeness and effectiveness
    - ✓ Sharing of best practices (e.g., through the North American Transmission Forum [NATF]) can also be used to verify completeness of policies and procedures

Compliance

- Periodic review of applicable regulations
  - New technical requirements
  - Record keeping requirements
    - ✓Contents
    - ✓Retention limits
  - New administrative requirements
    - ✓PII requirements
    - ✓General Data Protection Regulation (GDRP) requirements (for international organizations)

Compliance

- Office checklists:
  - Account authorization and verification (stale accounts, transfers, etc.)
  - Training records
  - Physical security authorizations
  - Known vulnerabilities
  - Logging and response procedures
  - Backup and recovery procedures
  - Development and deployment procedures (including redundancy and resilience)
  - Supplier relationships and contracts

Compliance

- Field checklists:
  - Physical inspection
  - Physical security testing
  - Alarm testing
  - Network configuration and filtering verification (isolation, access restrictions, etc.)
  - Asset verification
  - Asset/media labeling
  - Configuration parameters
  - Installed software versions

Pacific Northwest
NATIONAL LABORATORY

Thank you

Scott R. Mix, CISSP

scott.mix@pnnl.gov