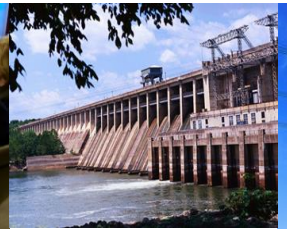
RELIABILITY FIRST

Metric Challenges

Bheshaj Krishnappa

Risk Analysis & Mitigation

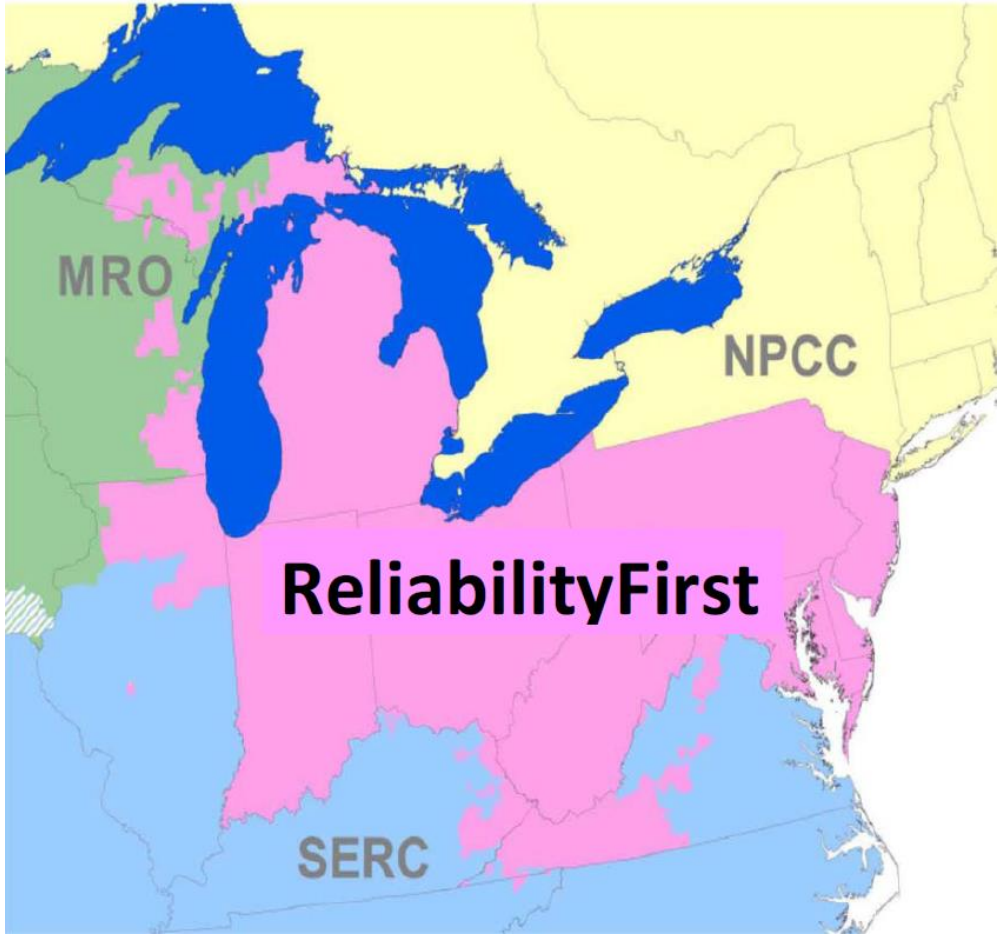





About RF

ReliabilityFirst preserves and enhances bulk power system reliability and security across 13 states and the District of Columbia.

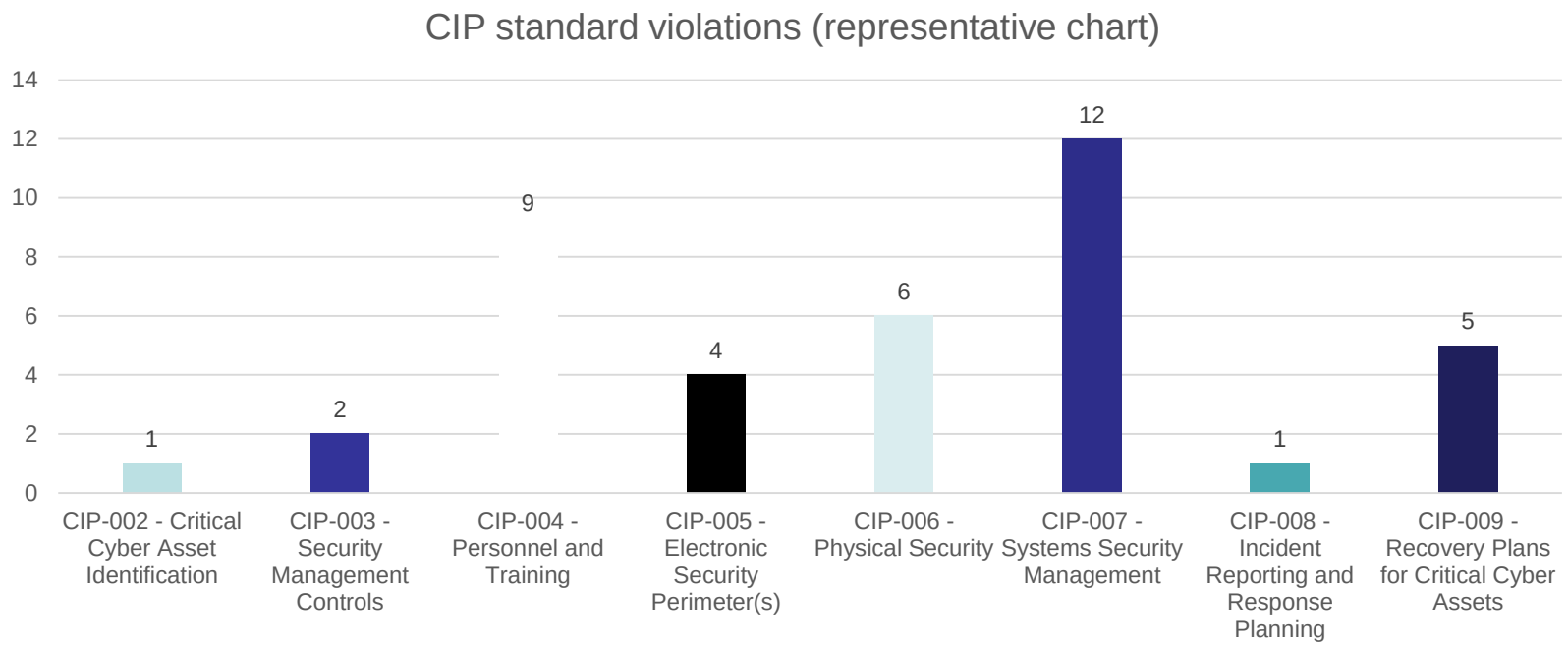
The Boundaries of ReliabilityFirst include all of New Jersey, Delaware, Pennsylvania, Maryland, District of Columbia, West Virginia, Ohio, Indiana, Lower Michigan and portions of Upper Michigan, Wisconsin, Illinois, Kentucky, Tennessee and Virginia.



Data sets and Metrics approach -1

➢ NERC CIP and O&P standards

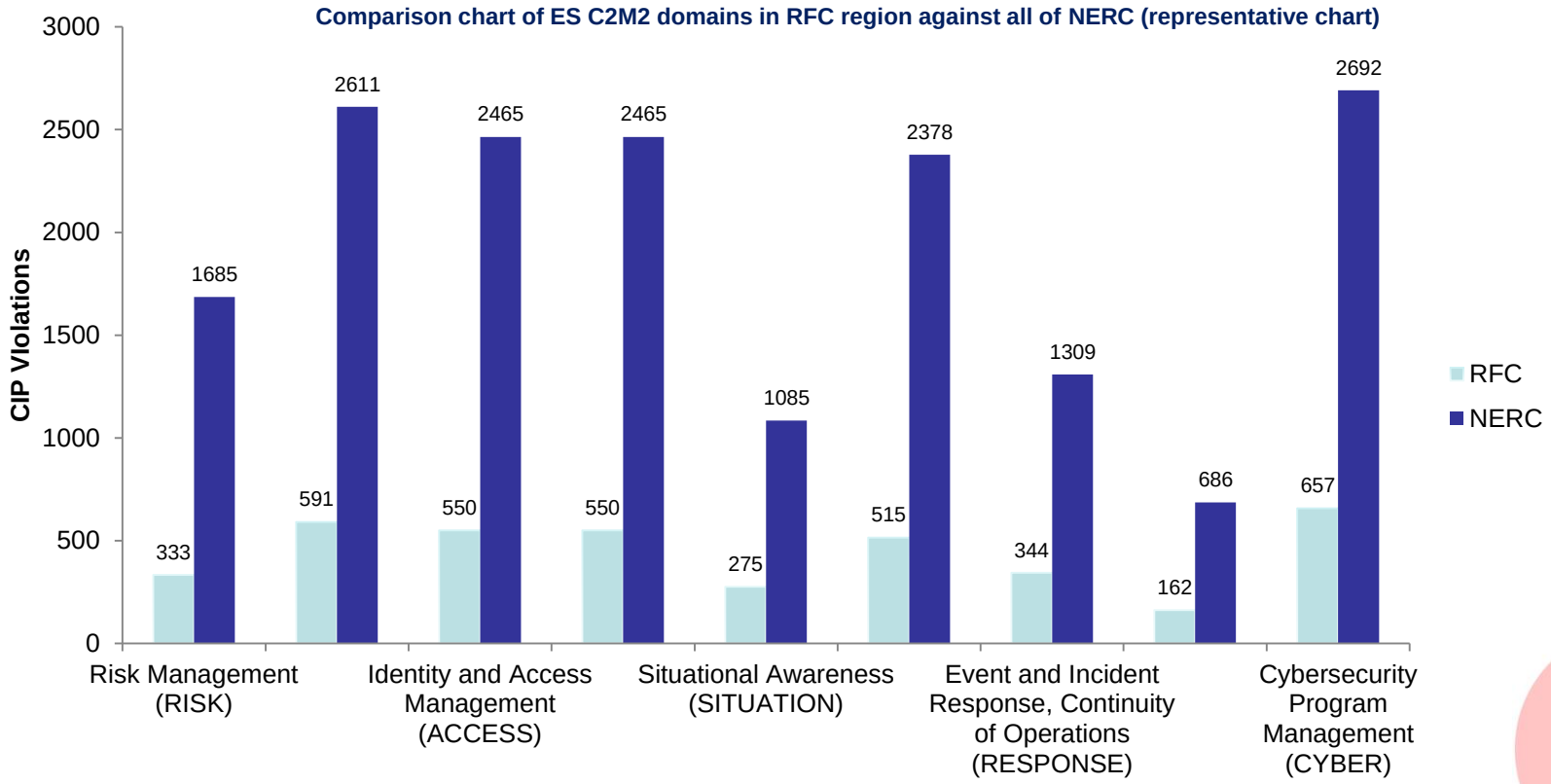
- NERC Standards CIP-002 through CIP-014 covering areas of BES Cyber System Categorization, Security Management Controls, Personnel & Training, Electronic Security Perimeter(s), Physical Security of BES Cyber Systems, Systems Security Management, Incident Reporting and Response Planning, Recovery Plans for BES Cyber Systems, Configuration Change Management and Vulnerability Assessments, Information Protection and Physical Security



Data sets and Metrics approach -2

➢ DOE Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)

- A maturity model to evaluate, prioritize, and improve cybersecurity capabilities. The areas assessed are Cybersecurity Program Management (CYBER), Asset, Change, and Configuration Management (ASSET), Information Sharing and Communications (SHARING), Identity and Access Management (ACCESS), Threat and Vulnerability Management (THREAT), Event and Incident Response, Continuity of Operations (RESPONSE), Risk Management (RISK), Situational Awareness (SITUATION), Workforce Management (WORKFORCE)



Challenges to Resilience metrics

- Point in time data
  - Compliance statistics
    - Violation history based on audits
    - Cyber assets and vulnerabilities
- Lack of Incident Response metrics
  - Dwell time, Containment time, Remediation time
- Lack of benchmark data for "Mean Time To Repair" or "Mean Time To Restore“ to measure resilience
- Lack of adoption of NIST CSF and availability of real-time data to assess Prevent, Detect, Respond, and Recover capabilities

Resilience metrics - Opportunities

- **Research on measurement of resilience indicators**
  - **Share existing methods of cyber resilience measurement/ approaches**
  - **Engage larger or targeted stakeholders to pilot projects and build upon**
- **Explore centralized data store and access**
  - **ICS CERT, Assets database, threats and vulnerability database, etc.,**
- **Explore NIST Cybersecurity Framework / CERT Resilience Management Model to derive resilience metrics**

Questions & Answers

Forward Together ReliabilityFirst