U.S. Department of Energy

Office of Electricity Delivery and Energy Reliability

Electric Sector Cybersecurity Risk Management Maturity Initiative

SANS SCADA 2012

Samara Moore, CISSP, PMP, CGEIT

Sr. IT and Cyber Security Advisor

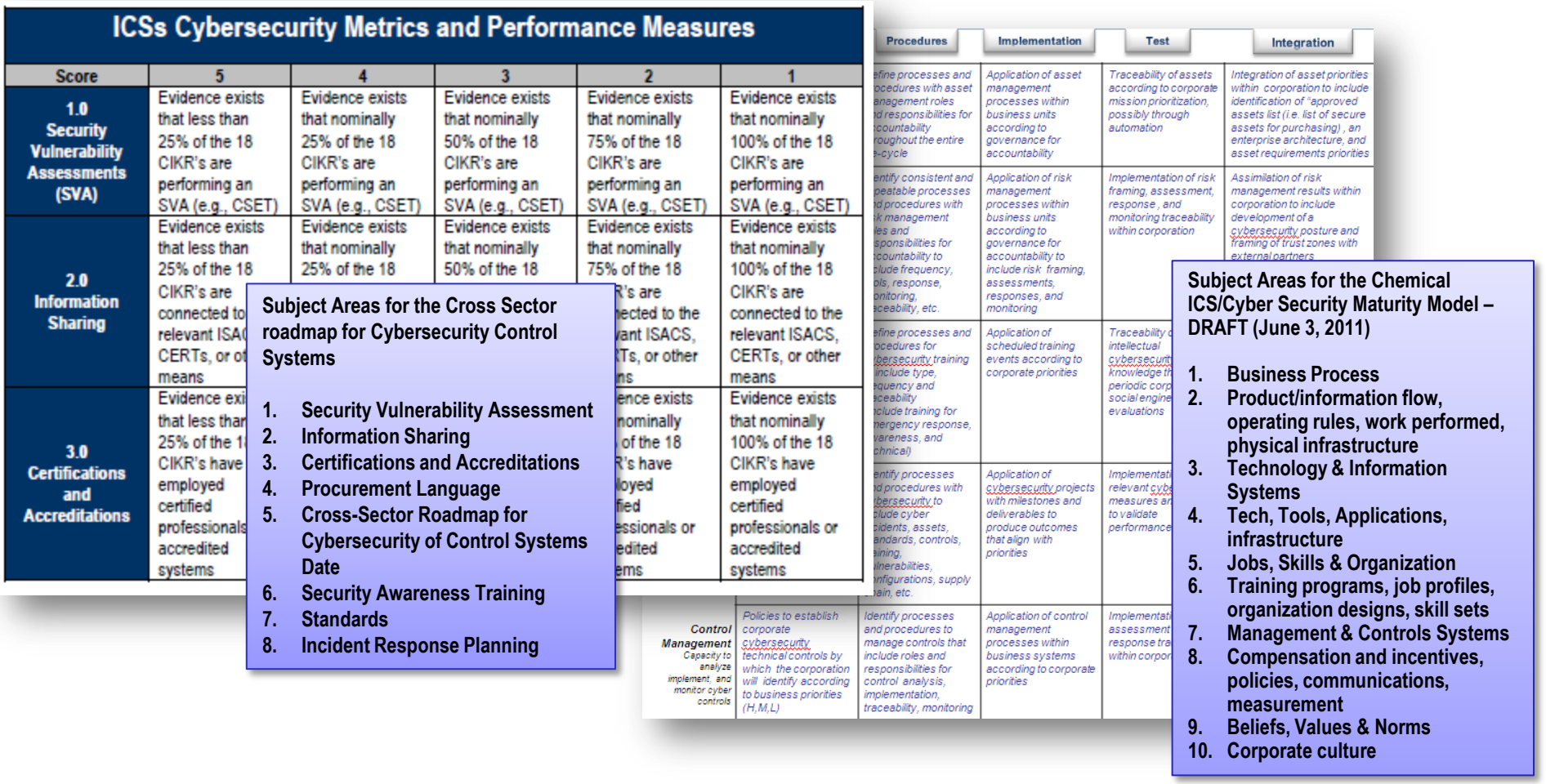
Electric Sector Cybersecurity Risk Management Maturity Initiative

- Power grid is in midst of major modernization effort
- Managing cybersecurity risk to the grid is a key part of the smart grid strategy
- Maturity model initiative aligned with:
  - Cyberspace Policy Review
  - Roadmap to for Energy Delivery Systems Cybersecurity
  - DHS Cross Sector Roadmap

Electric Sector Cybersecurity Risk Management Maturity Initiative

- White House initiative, led by DOE in partnership with DHS, and in collaboration with government and industry partners
  - A simple, usable model that industry can use to define their cybersecurity capabilities, identify gaps, and inform investment decisions
    - Provide common language and approach
    - Enable utilities to identify their cybersecurity capabilities
    - Encourage, guide, and support investment decisions
  - Over time, build a consistent understanding of cybersecurity capabilities across the electricity sector
    - Enable measurement of progress and comparison to peers
    - Communicate cybersecurity capabilities in a meaningful way

Electric Sector Cybersecurity Risk Management Maturity - Examples for Input



ICSs Cybersecurity Metrics and Performance Measures

Score	5	4	3	2	1
1.0 Security Vulnerability Assessments (SVA)	Evidence exists that less than 25% of the 18 CIKR's are performing an SVA (e.g., CSET)	Evidence exists that nominally 25% of the 18 CIKR's are performing an SVA (e.g., CSET)	Evidence exists that nominally 50% of the 18 CIKR's are performing an SVA (e.g., CSET)	Evidence exists that nominally 75% of the 18 CIKR's are performing an SVA (e.g., CSET)	Evidence exists that nominally 100% of the 18 CIKR's are performing an SVA (e.g., CSET)
2.0 Information Sharing	Evidence exists that less than 25% of the 18 CIKR's are connected to relevant ISA CERTs, or ot means	Evidence exists that nominally 25% of the 18	Evidence exists that nominally 50% of the 18	Evidence exists that nominally 75% of the 18 R's are ected to the ant ISACS, Ts, or other ns	Evidence exists that nominally 100% of the 18 CIKR's are connected to the relevant ISACS, CERTs, or other means
3.0 Certifications and Accreditations	Evidence exi that less thar 25% of the 1 CIKR's have employed certified professionals accredited systems			ence exists nominally of the 18 R's have loyed fied ssionals or edited ems	Evidence exists that nominally 100% of the 18 CIKR's have employed certified professionals or accredited systems

Subject Areas for the Cross Sector roadmap for Cybersecurity Control Systems

1. Security Vulnerability Assessment
2. Information Sharing
3. Certifications and Accreditations
4. Procurement Language
5. Cross-Sector Roadmap for Cybersecurity of Control Systems Date
6. Security Awareness Training
7. Standards
8. Incident Response Planning

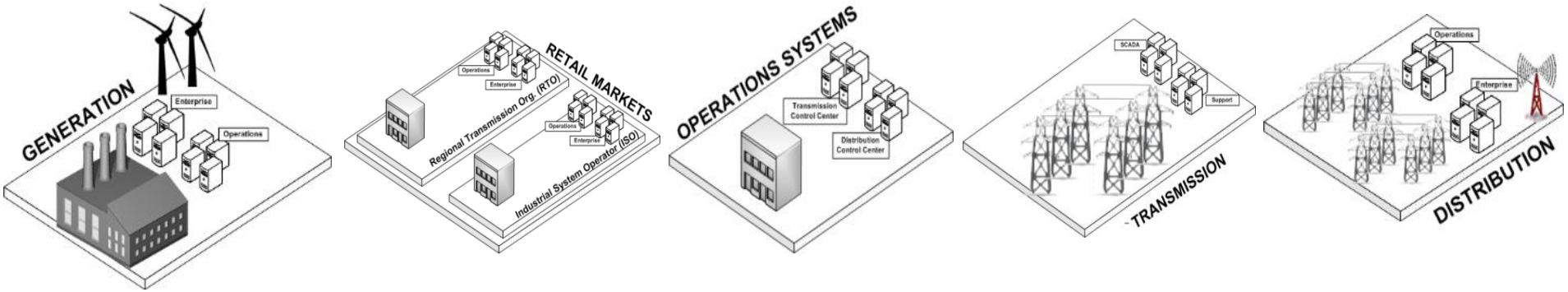
	Procedures	Implementation	Test	Integration
	efine processes and ocedures with asset anagement roles d responsibilities for countability roughout the entire e-cycle	Application of asset management processes within business units according to governance for accountability	Traceability of assets according to corporate mission prioritization, possibly through automation	Integration of asset priorities within corporation to include identification of "approved assets list (i.e. list of secure assets for purchasing) , an enterprise architecture, and asset requirements priorities
	entify consistent and peatable processes d procedures with k management es and sponsibilities for countability to clude frequency, ols, response, nitoring, ceability, etc.	Application of risk management processes within business units according to governance for accountability to include risk framing, assessments, responses, and monitoring	Implementation of risk framing, assessment, response , and monitoring traceability within corporation	Assimilation of risk management results within corporation to include development of a cybersecurity posture and framing of trust zones with external partners
	efine processes and ocedures for bersecurity training include type, equency and ceability clude training for ergency response, areness, and chnical)	Application of scheduled training events according to corporate priorities	Traceability intellectual cybersecurit knowledge th periodic corp social engine evaluations	
	entify processes d procedures with bersecurity to clude cyber idents, assets, andards, controls, ining, lnerabilities, nfigurations, supply ain, etc.	Application of cybersecurity projects with milestones and deliverables to produce outcomes that align with priorities	Implementati relevant cybs measures ar to validate performance	
Control Management Capacity to analyze, implement, and monitor cyber controls	Policies to establish corporate cybersecurity technical controls by which the corporation will identify according to business priorities (H,M,L)	Identify processes and procedures to manage controls that include roles and responsibilities for control analysis, implementation, traceability, monitoring	Application of control management processes within business systems according to corporate priorities	Implementati assessment response tra within corpor

Subject Areas for the Chemical ICS/Cyber Security Maturity Model – DRAFT (June 3, 2011)

1. Business Process
2. Product/information flow, operating rules, work performed, physical infrastructure
3. Technology & Information Systems
4. Tech, Tools, Applications, infrastructure
5. Jobs, Skills & Organization
6. Training programs, job profiles, organization designs, skill sets
7. Management & Controls Systems
8. Compensation and incentives, policies, communications, measurement
9. Beliefs, Values & Norms
10. Corporate culture

Performance areas for the Electric Sector may include: supply chain, incident management, workforce, continuous monitoring, etc.

Electric Sector Cybersecurity Risk Management Maturity Initiative - Scope



Type	Size	Systems	Regions
1.IOU 2.Public Power 3.Rural CooP 4.ISO/RT) 5.PMA	1.Large 2.Small 3.Medium	1.Control Systems 2.Business Systems	Considers regional differences

Electric Sector Cybersecurity Risk Management Maturity Initiative - Approach and Timeline

	Phase 1 **Develop** Jan-Mar 2012	Phase 2 **Assess** April 2012	Phase 3 **Analyze & Refine** April-May 2012	**Future Activities** May–Aug 2012
Activities	• Establish team and identify SMEs (public and private stakeholders) • Assess existing efforts • Develop initial draft model and assessment instrument	• Utilities pilot use of model • Facilitate assessment using draft model • Utilize scenario/exercise approach	• Analyze feedback and data from pilot • Revise draft model • Share feedback	• Information exchange • Outreach and awareness
Output	• Draft model • Assessment instrument	• Feedback on model and assessment • Non-attributable data from pilot	• Initial Electric Sector Cybersecurity Maturity Model • Summary report	

Managing Expectations

Model Expectations…

- Lightweight model
- Leverage existing efforts within sector
- Useful tool for industry
- Refined and expanded overtime
- As used by sector, will provide understanding of cybersecurity risk management capabilities

Will enable…

- Identification of gaps, improvement areas, and high performance areas
- Improved coordination across different groups
- Support for business case for cybersecurity investments
- Improved communication of security capabilities and needs

Electric Sector Cybersecurity Risk Management Maturity Initiative

For more information contact

oe-escyberpilot@hq.doe.gov