Secure Power Systems Professional Project Phase 2 Closeout Briefing

Lori Ross O'Neil, PNNL and Michael Assante, NBISE

- Background
- Challenges
- Project description
- Outcomes and Findings

NBISE
NATIONAL BOARD OF INFORMATION SECURITY EXAMINERS

Pacific Northwest NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

Challenge facing the North American Power Grid: Vast and ever growing cyber-attack surface

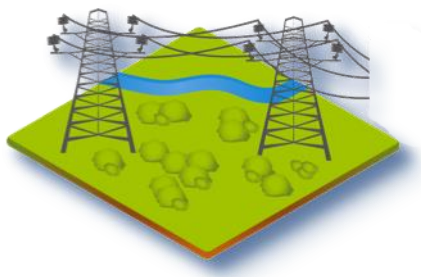
- **Complex technology-reliant operations**
- **Lack of a viable cybersecurity workforce**
- **Grid modernization efforts require advanced, continually maturing cybersecurity capabilities**

Modern Pillars of the Electricity Sector

Traditional Pillars

Generation

Transmission



Distribution

Automated Generation Control
Plant Systems (PCS/Safety/Historian)
Auxiliary systems
Emission monitoring systems

System Control Center SCADA EMS
Substation (Control & DA/Protection)
Phasors, Data Concentrators, Gateways

Advanced Metering
System Control Center SCADA DMS
Substation (Control & DA/Protection)
Distribution Automation (Remote Disconnect)
Phasors, Data Concentrators, Gateways
Outage Management Systems

Information & Communication Technology

Market Systems
OASIS
Automated Generation Control

Markets

New Pillars

Examples of Electricity Sector Operational Technology (OT)

Industrial Control Systems (ICS): A term used to encompass the many applications and uses of industrial and facility control and automation systems.

Types of Industrial/Facility Automation & Control	Uses & Applications	Examples
SCADA & EMS – Supervisory Control & Data Acquisition and Energy Management System	Control and data acquisition over large geographic areas	Electricity transmission & distribution
DCS - Distributed Control System	Systems which control, monitor, and manage industrial processes that are disbursed but operated as a coupled system	Thermal plant auxiliary systems
PCS – Process Control System	Systems which control, monitor, and manage an industrial processes	Thermal power plant, nuclear power plant systems, wind farm, etc.

NBISE
NATIONAL BOARD OF INFORMATION SECURITY EXAMINERS

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

Electricity Sector Cyber Challenges

- **Smart Grid – emerging technology**
- **Security Operations – poorly defined**
- **Skills and operational job roles – poorly defined**
- **Education and training – are poorly aligned with Operational Technology (OT)/Smart Grid application**
- **Methods for assessing OT competency – inadequate**
- **Skill and knowledge required across diverse stakeholders**

NBISE
NATIONAL BOARD OF INFORMATION SECURITY EXAMINERS

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

Energy OT Systems Lifecycle

IT Security Concepts

Application Driven (IT/OT) Convergence

Energy OT Systems Lifecycle

Design	Development	Implementation	Integration	Operations & Maintenance	Refresh/Retire

Cybersecurity Operations

SPSP Project Focus

Suppliers Integrators Utilities

Technologists Experts

SPSP SME Panel Members

SPSP Project Goals and Timelines

- Phase 1: Competency Analysis Study – **Complete**
  - Developed a comprehensive set of cybersecurity competencies needed for Secure Power Systems Professionals to do their job effectively.
- Phase 2: Analysis of workforce resources – **Complete**
  - Competencies identified in Phase 1 were analyzed against current workforce development frameworks, certifications and education to determine how well these fulfill the current workforce needs.
- Phase 3: Performance Analysis, Final Report, Recommendations - **8 months**
  - Data from the previous phases will be refined, analyzed and measured. Results will be published and presented.

NBISE
NATIONAL BOARD OF INFORMATION SECURITY EXAMINERS

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

Phase 2 Tasks : COMPLETE

Task 9: Certification review and job skill identification

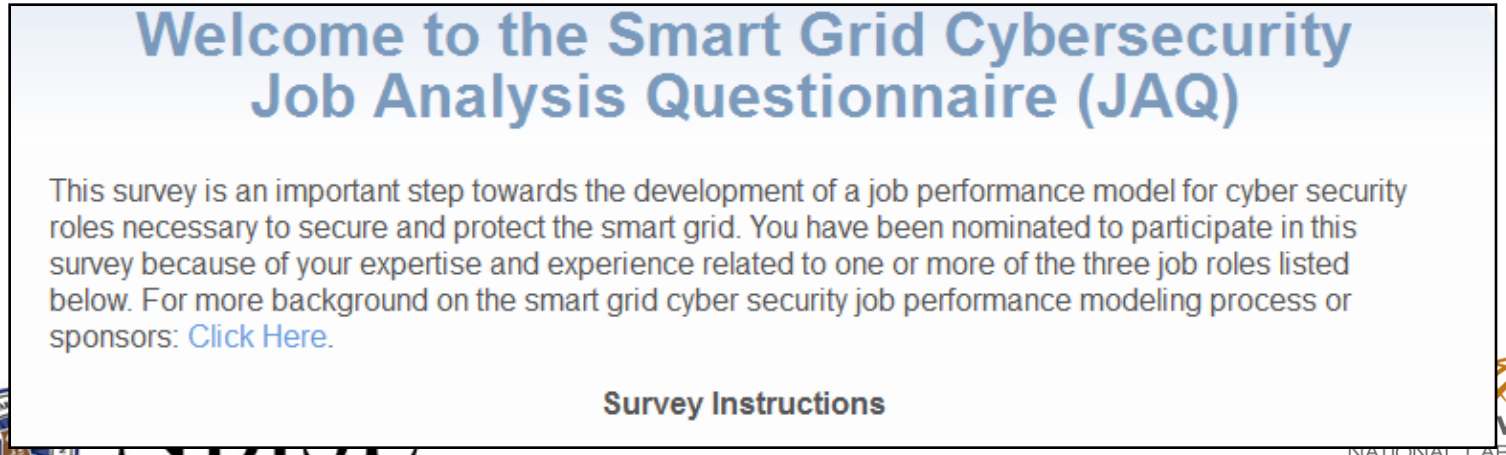
Task 10: Develop a review mechanism of Task 9 results

Task 11: SPSP Panel review and assessment of Task 9 results

Task 12: Wider audience review and comment on Task 9 results

Task 13: Prepare final results for DOE and contributors

Task 14: Phase 2 project management



Welcome to the Smart Grid Cybersecurity Job Analysis Questionnaire (JAQ)

This survey is an important step towards the development of a job performance model for cyber security roles necessary to secure and protect the smart grid. You have been nominated to participate in this survey because of your expertise and experience related to one or more of the three job roles listed below. For more background on the smart grid cyber security job performance modeling process or sponsors: Click Here.

Survey Instructions

NATIONAL BOARD OF INFORMATION SECURITY EXAMINERS

NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

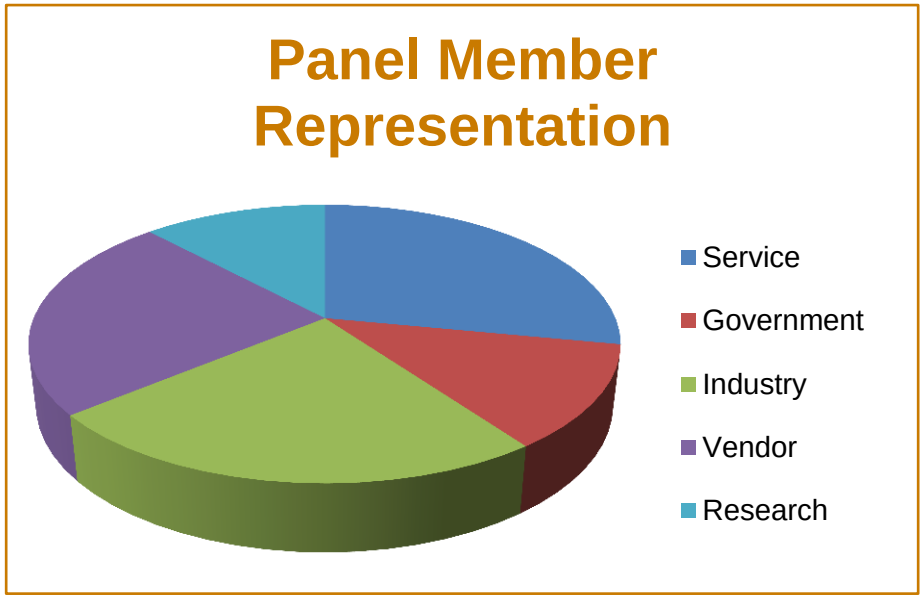
SPSP SME Panel Group Members

Panel Officers

Tim Conway, NiSource (Chair)
Karl Perman, NATF (Vice-chair)

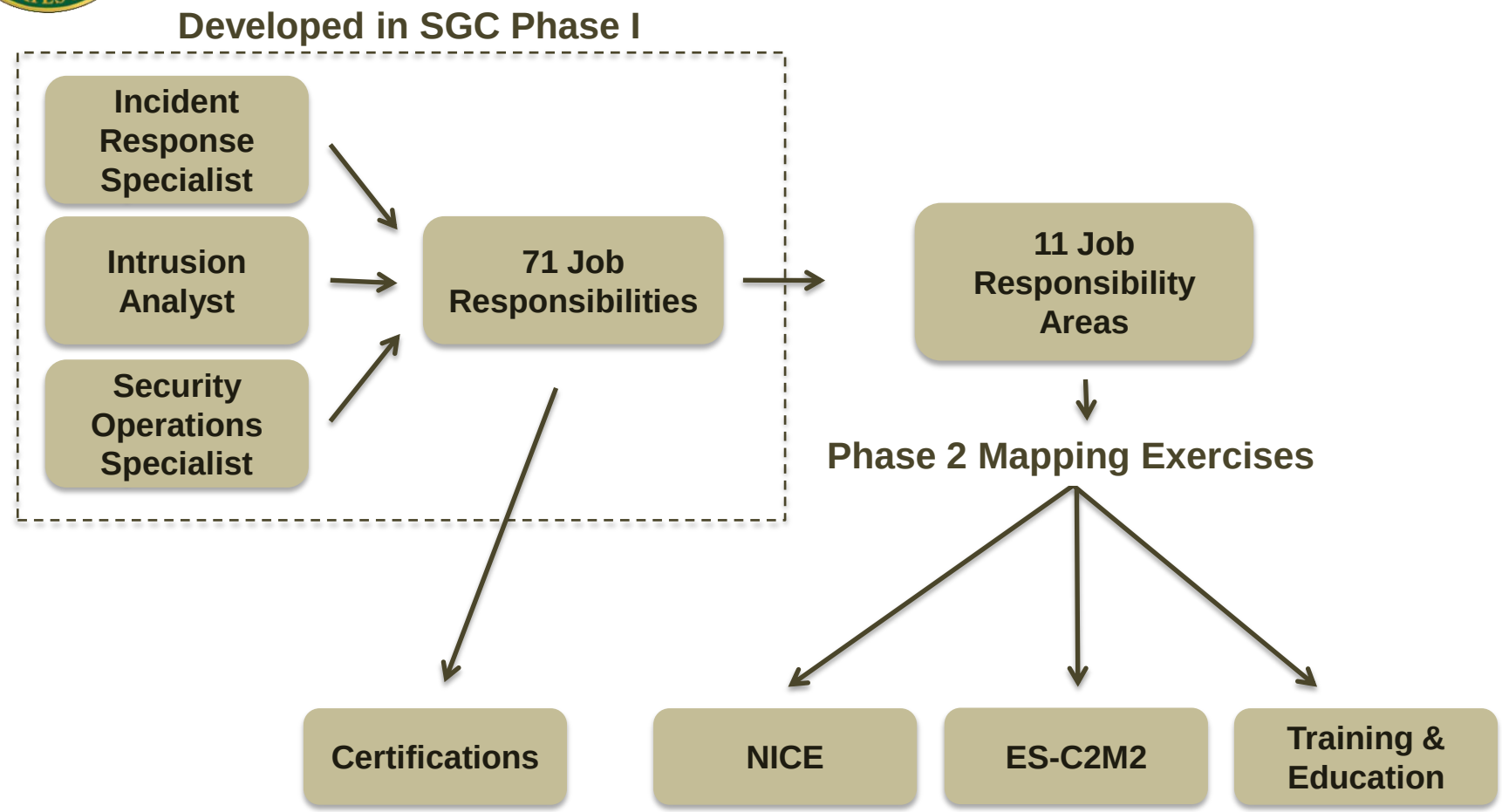
Panel Members

Lee Aber - OPower
Sandeep Agrawal - Neilsoft Limited
Bora Akyol - PNNL
Balusamy Arumugam - Infosys
Michael Assante - NBISE
Leonard Chamberlin - FERC (OER)
Jason Christopher - FERC
Benjamin Damm - Silver Springs Network
Aaron Fansler - Northrup Grumman
Maria Hayden – Pentagon
Joseph Januszewski - NIH
Steven Keller - Southwest Power Pool Regional Entity
Karl Kersey - Schneider Electric
Ross Leo - Consultant
Matthew Luallen - Industry Contractor
Patrick Miller - Energy Sec
Donald Morris - CenterPoint Energy
Gilbert Perez - The Structure Group
Galen Rasche - EPRI
James Sample - PG&E



Chris Sawall - Ameren
Anthony David Scott - Accenture
Paul Skare - PNNL
Gilbert Sorebo - SAIC
Thomas Strickland - KEMA
Michael Terebussy - CISCO
Dan Thanos - GE Digital Energy
Kevin Tydings - SAIC
Donald Weber - InGuardians
Mike Wenstrom - Mike Wenstrom Development Partners
Tim Yardley - University of Illinois

Phase 2 Mapping Overview



NBISE
NATIONAL BOARD OF INFORMATION SECURITY EXAMINERS

Pacific Northwest NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

Frameworks Reviewed

NICE | ES-C2M2

NICE (National Initiative for Cybersecurity Education)

- Led by the National Institute of Standards and Technology, this multi-agency effort seeks to provide a consistent and broad approach to cybersecurity education.
- As the primary federal government initiative in this space, the nomenclature and definitions outlined here provide a common reference for classification of skills and competencies.

ES-C2M2 (Electricity Subsector Cybersecurity Capability Maturity Model)

- A public-private endeavor led by Department of Energy in partnership with Department of Homeland Security, this model provides a sector-specific listing of essential capabilities, functions and activities for cybersecurity in the electric utility industry and is commonly referenced for enterprise maturity assessment and improvement.

NBISE
NATIONAL BOARD OF INFORMATION SECURITY EXAMINERS

Pacific Northwest NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

SPSP Panel Identified Certifications

Certifications

Certification	Organization
Certified Information Systems Security Professional (CISSP)	(ISC)^2
System Operator Certification (SOC)	NERC
Certified Ethical Hacker (CEH)	EC-Council
Certified Information Security Auditor (CISA)	ISACA
Certified Information Security Manager (CISM)	ISACA
Certified in Risk and Information Systems Control (CRISC)	ISACA
Certified Incident Handler (GCIH)	GIAC
Certified Intrusion Analyst (GCIA)	GIAC
Penetration Tester (GPEN)	GIAC

NBISE
NATIONAL BOARD OF INFORMATION SECURITY EXAMINERS

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

Certifications Associated with Job Roles

Certifications → Job Roles

Job Roles	Certifications	# of Resp.	% of Resp.
Cyber secure power engineer (9 responsibilities)*	CISSP	3	33.3%
	CISM	1	11.1%
	Not covered by certification	6	66.7%
Incident response (10 responsibilities)	CISM	4	40.0%
	CISSP	3	30.0%
	GCIH	9	90.0%
	Not covered by certification	0	0.0%
Intrusion analysis (10 responsibilities)	CISM	3	30.0%
	CISSP	2	20.0%
	GCIH	7	70.0%
	CEH	1	10.0%
	GCIA	1	10.0%
	Not covered by certification	2	20.0%
Security operations (16 responsibilities)	CISM	8	50.0%
	CISSP	7	43.8%
	GCIH	3	18.8%
	Not covered by certification	5	31.3%

* Added power engineer role, as cybersecurity work being performed by other roles was found to be dependent upon those who oversee real-time energy control systems and need to have relevant knowledge and skills

NBISE
NATIONAL BOARD OF INFORMATION SECURITY EXAMINERS

Pacific Northwest NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

Job Role Coverage by Certification

Security Operations Specialist | rusion nalyst | cident sponse ecialist → **Certifications**

Job Role	CEH	CISM	CISSP	GCIA	GCIH	SOC
Cyber Secure Power Eng.	0.0%	11.1%	33.3%	0.0%	0.0%	0.0%
Incident Response	0.0%	40.0%	20.0%	0.0%	90.0%	0.0%
Intrusion Analysis	10.0%	30.0%	20.0%	10.0%	70.0%	0.0%
Security Operations	0.0%	50.0%	37.5%	0.0%	18.8%	0.0%

Note: A responsibility may be covered by more than one certification and may be assigned to more than one job role, so the rows and columns may exceed 100%.

NBISE
NATIONAL BOARD OF INFORMATION SECURITY EXAMINERS

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

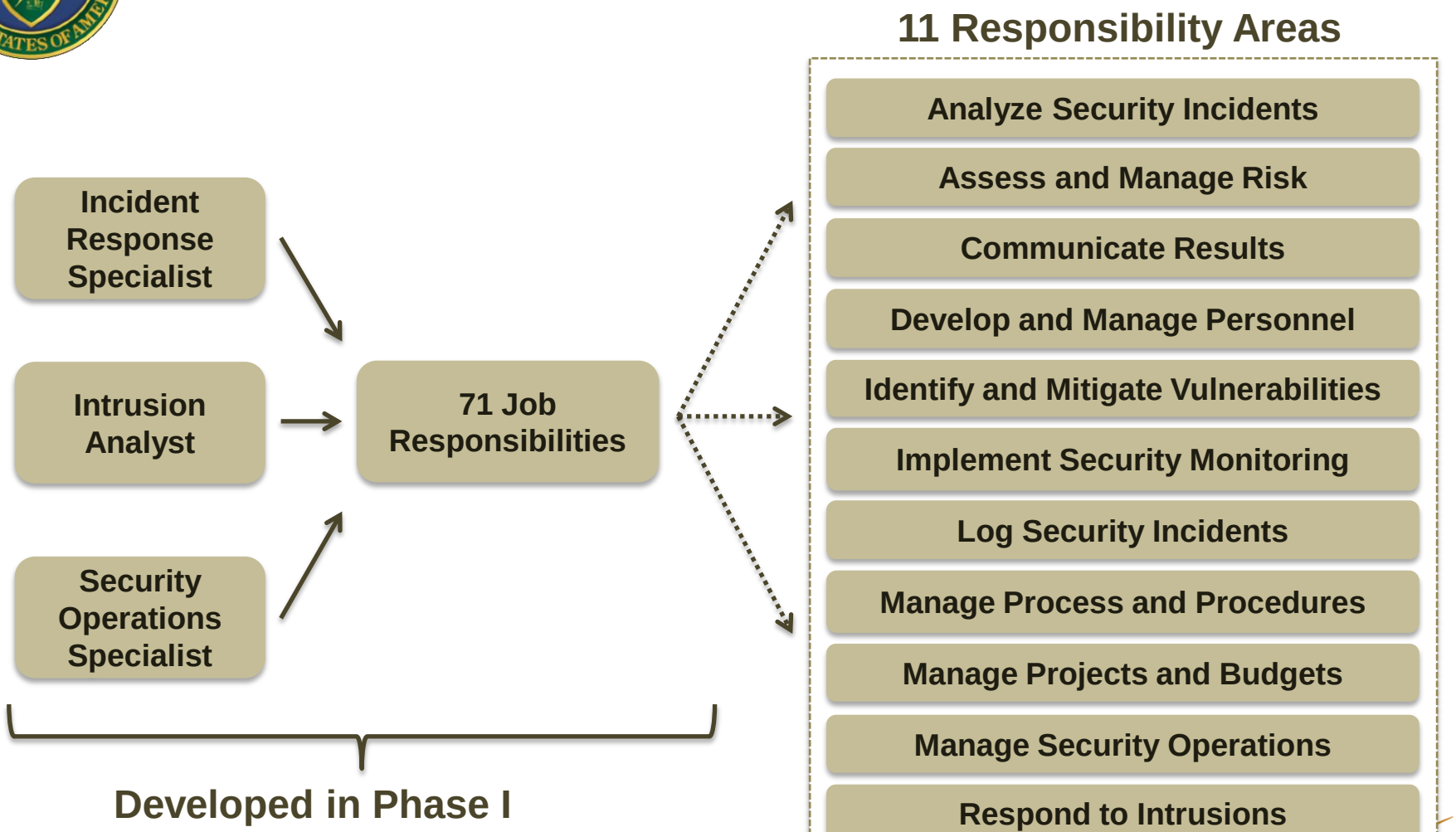
Key Certification Findings

- No single certification adequately tests job proficiency.
- Significant gaps exist in emphasis on power system operator cybersecurity responsibilities.
- The NERC SOC does not cover any cybersecurity responsibilities identified for the four job roles.
- The SPSP Job Performance Model enabled identification of potential alignment and gaps in certification exams

NBISE
NATIONAL BOARD OF INFORMATION SECURITY EXAMINERS

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Mapping to Responsibility Areas



NBISE
NATIONAL BOARD OF INFORMATION SECURITY EXAMINERS
Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Coverage of Responsibility Areas in Frameworks and Education Courses

NICE | ES-C2M2 | Training & Education

Responsibility Area	NICE Tasks	ES-C2M2 Objective	Course Topics
Analyze security incidents	14	2	2
Assess and manage risk	9	4	9
Respond to intrusions	10	3	1
Communicate results	11	3	0
Identify and mitigate vulnerabilities	11	2	11
Implement security monitoring	2	1	6
Log security incidents	6	2	3
Manage process and procedures	3	8	2
Manage projects and budgets	1	1	0
Manage security operations	3	8	5
Develop and manage personnel	0	4	1

NBISE
NATIONAL BOARD OF INFORMATION SECURITY EXAMINERS

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

Key Findings from Framework and Education Course Mapping

- Technical responsibilities are a significant focus of the NICE task list and the education and training course topics.
- ES-C2M2 provides the greatest weighting to individual responsibility areas that reflect a managerial focus.
- NICE tasks provide the most weight to analyzing security incidents.
- None of the three competency development programs were found by the panel to have elements focused on managing projects and budgets.
- NICE tasks and course topics lack an emphasis on developing and managing personnel.
- Education and training course topics provide the most emphasis on identifying and mitigating vulnerabilities.

NBISE
NATIONAL BOARD OF INFORMATION SECURITY EXAMINERS

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle Since 1965

Key Education &Training Findings

- Courses tend to focus on risk and vulnerability assessment at the exclusion of other technical roles such as intrusion analysis and incident response.
- The courses tended to be offered in Computer Science or Electronics departments. We did not find any courses related to cybersecurity in power engineering programs.
- Most of the courses addressing power system cybersecurity were special topics and not a part of the regular/required curriculum.
- Curricula should be expanded to improve proficiency in communication, process/project management, and staff development.

NBISE
NATIONAL BOARD OF INFORMATION SECURITY EXAMINERS

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

Target Workforce Program Emphasis of Responsibility Areas

Responsibility Area	Competency Frameworks		Workforce Development	
	NICE	ES-C2M2	Certs	Courses
Manage projects and budgets				
Develop and manage personnel		D		
Manage process and procedures				
Log security incidents				D
Respond to intrusions				
Implement security monitoring				
Identify and mitigate vulnerabilities			D	
Analyze security incidents				D
Communicate results				
Manage security operations	D		D	
Assess and manage risk				

Shading indicates emphasis on a responsibility area in a competency framework or a workforce development program.

D indicates mappings with disagreement between panel and public respondents.

NICE = National Initiative for Cybersecurity Education

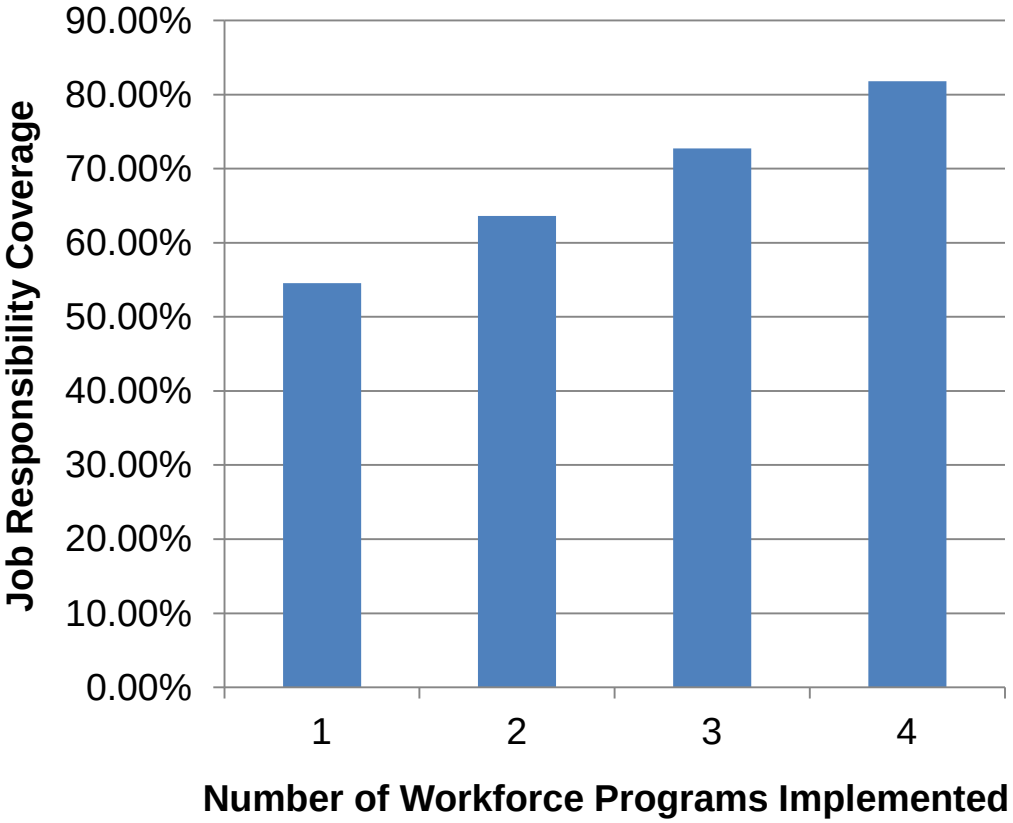
ES-C2M2 = Energy Systems Cybersecurity Capability Maturity Model

NBISE
NATIONAL BOARD OF INFORMATION SECURITY EXAMINERS

Pacific Northwest NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

Overview of Workforce Programs



- No combination of programs addresses all job roles
- Using 1 program = 54% coverage
- Using 2 programs = 63%
- Using 3 programs = 72%
- Using all 4 programs = 81%

NBISE
NATIONAL BOARD OF INFORMATION SECURITY EXAMINERS

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

Summary of Key Phase 2 Findings

- Workforce development programs commonly provide uneven coverage of job responsibility areas, posing a challenge for comprehensive development across essential skills.
- Traditional IT roles are fairly well defined with well-established competency frameworks and credentials, while OT roles do not have a well-defined alignment to existing programs.
- The common lack of emphasis on the individual skills of managing people, projects, and budgets may limit development of managerial competencies necessary to improve cybersecurity posture at the organizational level.

NBISE
NATIONAL BOARD OF INFORMATION SECURITY EXAMINERS

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

Summary of Key Findings, cont.

- Lack of alignment among workforce programs suggests an unequal distribution of competencies across the industry may result as organizations choose to implement various programs to varying degrees.
- Certifications may provide the best guidance for establishing fundamental competence in the workforce, while the ES-C2M2 framework may provide the best guidance for ascertaining specific competencies that differentiate individuals (or organizations).

NBISE
NATIONAL BOARD OF INFORMATION SECURITY EXAMINERS

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Concluding Phase 2 Recommendations

- Qualification and training criteria need to ensure the same progression and program maturity for the Secure Power Systems Professional as currently exists for the system operator role.
- Industry, academia, and government need to collaborate to design assessment instruments to guide recruitment, selection, development, retention and performance evaluation.
- Workforce frameworks need to specify competency at the task execution level with measures developed to confidently assess and compare job candidates.

NBISE
NATIONAL BOARD OF INFORMATION SECURITY EXAMINERS

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

Concluding Recommendations, cont.

- Research is needed to assess the effectiveness of existing credentialing programs in determining the appropriate “fit” of a candidate for a given SPSP role.
- Accreditation of education and certification programs need to require documentation of learning objective alignment with the job responsibilities emphasized in the competency frameworks and the SPSP Job Performance Model.
- Industry and educational programs need to define what cybersecurity knowledge is important for power engineers and technical professions involved in system planning, design, and operations.

NBISE
NATIONAL BOARD OF INFORMATION SECURITY EXAMINERS

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle Since 1965

SPSP Panel Member Insights

While the industry experiences this transitory phase of developing a "Smart Grid", the "Smart" portion of security is receiving the bulk of the attention, and there seems to be less emphasis on the power end… "we" seem to be focused primarily on the areas that have been "historically" viewed as "information security"… This does seem to be leaving an aspect of power generation control "in the dark" (no pun) during this process.

- **Joseph J. Januszewski, III**, Panel Member

I believe these results confirm a common belief within [power and utility] entities that; traditional IT roles are fairly well defined with credentials and available credentials, while Operations Technology roles do not have a well-defined alignment to existing [cybersecurity] programs.

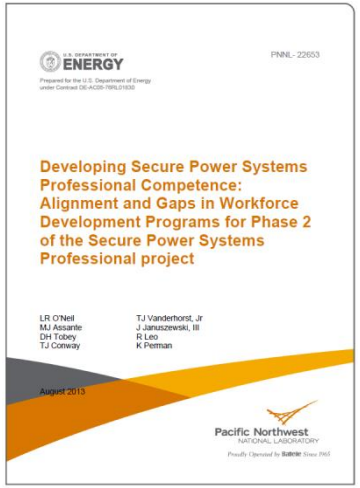
- **Tim Conway**, Panel Chair

NBISE
NATIONAL BOARD OF INFORMATION SECURITY EXAMINERS

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

Phase 2 Project Information Sharing



- **Presentations**
  - CIPC Meeting (Albuquerque, NM), June 6, 2012
  - Google+ Hangout, May 4, 2012
- **Interest**
  - Department of Homeland Security Skills Task Force
- **Reports**
  - Phase 2 Final Reports: Developing Secure Power Systems Professional Competence: Alignment and Gaps in Workforce Development Programs (PNNL-22653, PNNL-22641)
- **Related Articles (online)**
  - NPR The Next Disaster Scenario Power Companies Are Preparing For, August 15, 2013 (and on air)
  - Grid Modernization and Cyber Security Training Trends, June 18, 2013

NBISE
NATIONAL BOARD OF INFORMATION SECURITY EXAMINERS

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

Next Steps – Phase 3:
August 2013 through March 2014

- Phase 1: Complete
- Phase 2: Complete
- Phase 3: Performance Analysis, Final Report, and Recommendations - 8 months
  - Task 15: Refine and analyze data and observations across Phase 1 and Phase 2
  - Task 16: Identify additional work and potential projects and resources to accelerate power system cyber workforce development
  - Task 17: Complete final report and recommendations

NBISE
NATIONAL BOARD OF INFORMATION SECURITY EXAMINERS

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

Contacts

For more information, contact:

Lori Ross O'Neil, PNNL lro@pnnl.gov

Michael Assante, NBISE michael.assante@nbise.org