U.S. DEPARTMENT OF ENERGY

PNNL- 22641

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Developing Secure Power Systems Professional Competence: Alignment and Gaps in Workforce Development Programs—Summary Report

LR O'Neil
MJ Assante
DH Tobey
TJ Conway
TJ Vanderhorst, Jr
J Januszewski, III
R Leo
K Perman

July 2013

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
email: orders@ntis.gov <http://www.ntis.gov/about/form.aspx>
Online ordering: http://www.ntis.gov


This document was printed on recycled paper.
(8/2010)

PNNL- 22641

Developing Secure Power Systems Professional Competence: Alignment and Gaps in Workforce Development Programs—Summary Report

LR O'Neil
MJ Assante
DH Tobey
TJ Conway
TJ Vanderhorst, Jr
J Januszewski, III
R Leo
K Perman

Contributors:
SGC Panel Members

July, 2013

Prepared by:
Pacific Northwest National Laboratory and
NBISE Secure Power Systems Professional Project Team

This document is a summarization of the report, *Developing Secure Power Systems Professional Competence: Alignment and Gaps in Workforce Development Programs*, PNNL- 22653, available from lro@pnnl.gov or www.nbise.org.

Summary

The U.S. Department of Energy has recognized that the electricity industry needs workforce development resources that can aid in the accelerating need for Secure Power Systems Professionals, while at the same time identifying capabilities and competencies to protect and enable the modernized grid currently being built. In the spring of 2011 a project was initiated by Pacific Northwest National Laboratory with National Board of Information Security Examiners for the U.S. Department of Energy to identify those capabilities and competencies along with assessing the need and qualifications for a certification program for Secure Power Systems Professionals. The first phase of this three-phase project was to identify operational security functions for day-to-day power systems operations (but not development, engineering, and architecture), and power system environments. The project examined the technical, problem-solving, social and analytical skills identified by stakeholders as used by existing power systems cybersecurity staff in the daily execution of their responsibilities resulting in a comprehensive Job Performance Model (JPM) for Smart Grid.[1]

The second phase of the project applied the JPM to ascertain the alignment and gaps among existing workforce development programs. The JPM from Phase 1 included 82 job responsibilities; 71 of these were assigned by the Smart Grid Cybersecurity Subject Matter Expert panel to 11 job responsibility areas. These responsibility areas became the basis for studying the gaps and overlaps between four cybersecurity workforce development programs (Figure 1):

1. the National Initiative for Cybersecurity Education (NICE) National Cybersecurity Workforce Framework;[2]
2. the Energy Systems Cybersecurity Capability Maturity Model (ES-C2M2);[3]
3. power systems cybersecurity education courses; and
4. cybersecurity certifications.

The Subject Matter Expert panel's findings were validated through a public survey; both the panel's findings and the survey identified responsibility areas lacking sufficient coverage in the currently available workforce programs.

[1] http://energy.gov/oe/downloads/smart-grid-cybersecurity-job-performance-model-report-and-phase-1-overview-august-2012

[2] http://csrc.nist.gov/nice/framework/national_cybersecurity_workforce_framework_v1_1_august2012_for_printing.pdf

[3] http://energy.gov/oe/services/cybersecurity/electricity-subsector-cybersecurity-capability-maturity-model

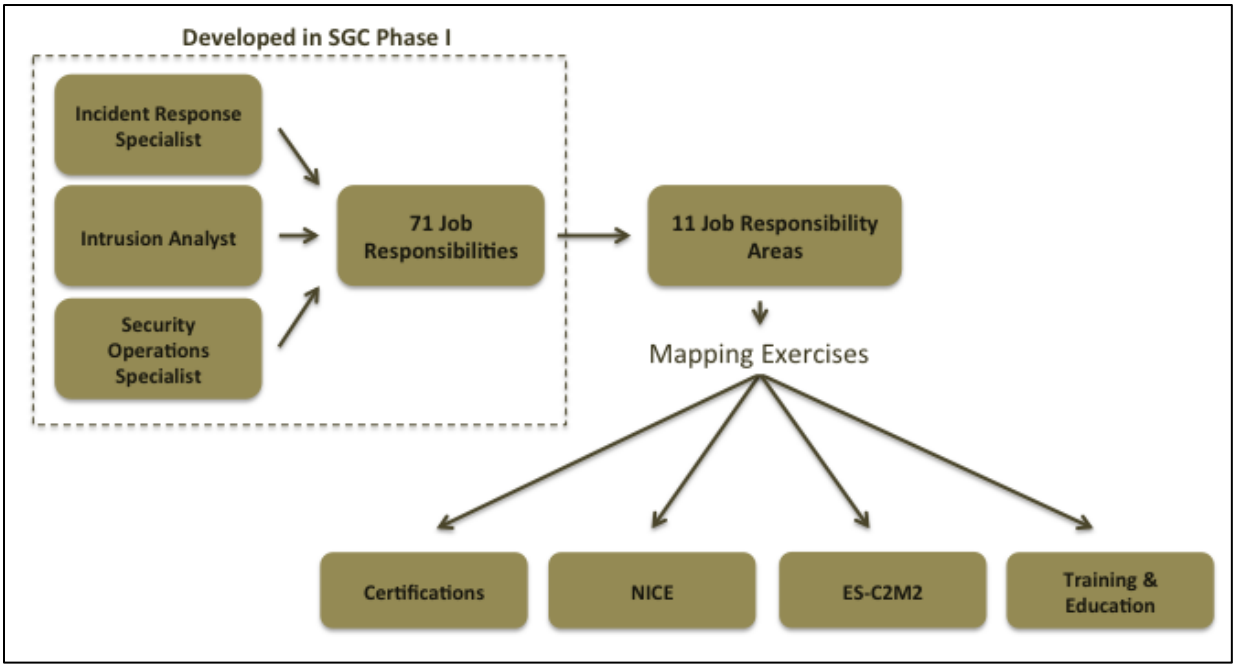

Figure 1. Phase 2 Overview

The analysis of certifications yielded nine vendor-neutral certifications that panel members indicated were valuable for determining job competency (Figure 2). The results indicate that no single certification exists for a Secure Power Systems Professional. A combination of certifications has value in determining a base level of competency or for enhancing an existing employee's knowledge base. For example, someone with a North American Electric Reliability Corporation System Operator Certification could expand their cybersecurity knowledge and verify it by obtaining a cybersecurity-centric certification such as one listed in Figure 2. *Rather than trying to force existing certifications to meet the needs of the modern power grid, it is the recommendation of the panel to develop a Secure Power Systems specific certification.*

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
Web Application Penetration Tester (GWAPT)	GIAC

Figure 2. Valuable Vendor-Neutral Certifications

The NICE and the ES-C2M2 are both workforce competency frameworks intended to serve as guides to those developing the other two workforce programs: education and training courses and/or assessment or certification programs. The analysis of these two frameworks indicated that technical responsibilities are a significant focus of the NICE tasks while the ES-C2M2 emphasizes managerial responsibilities.

Both frameworks emphasized two job responsibility areas: assessing and managing risk and communicating results. Neither framework emphasized developing and managing personnel, implementing security monitoring, logging security incidents, and managing projects and budgets.

The results of the education and training course review identified that there were very few educational offerings with a focus on cybersecurity for power systems. We did find special courses and seminars, usually within Computer Science or Electronics departments or offered by organizations such as SANS[1] or Internal Security Associates, but no courses related to cybersecurity in power engineering programs as part of a college or vocational program to graduate work-ready employees. *Cybersecurity of power systems education needs to be available to college students now so that they are ready to defend and protect the modern power grid when they graduate and enter the workforce.*

There are several useful conclusions that can be implemented by stakeholders immediately:

1. Entities can use the job roles identified as having a strong alignment with applicable certifications to adjust job postings or staff development programs to align with identified job roles.

> "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

2. For the areas where strong alignment with an existing certification does not exist, entities can first adjust job descriptions and career paths to remove credential requirements that do not align with job-identified roles.
3. Organizations can begin developing or working with partners to utilize existing or develop new training programs that best fill the identified gaps.

It is recommended that work continue to validate the predictive accuracy of the JPM developed in Phase I of this project and to apply the validated model to accredit workforce programs based on the job role(s), responsibility areas and expertise levels at which they are targeted. We also recommend the development of self-assessment tools to help organizations determine whether they have a holistic approach to workforce development and if they don't, how to implement one.

Panel members have indicated that a certification would be well received and a smart community investment. The continued implementation of digital technology into every aspect of power systems helps us reach the goal of a fully integrated power system without boundaries—from end to end, generation to distribution. It is incumbent on power system stakeholders to lead the effort to redefine critical power system job functions and expand those job functions to develop a workforce that can tackle the cybersecurity challenges of the country's new edgeless power system.

[1] http://www.sans.org/

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by **Battelle** *Since 1965*

U.S. DEPARTMENT OF
ENERGY

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99352
1-888-375-PNNL (7665)
www.pnnl.gov