



U.S. DEPARTMENT OF  
**ENERGY**

PNNL- 21638

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

# Smart Grid Cybersecurity Certification Phase 1 Overview Report

LR O'Neil, PNNL  
MJ Assante, NBISE  
DH Tobey, NBISE

August 2012

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



**Pacific Northwest**  
NATIONAL LABORATORY

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



**DISCLAIMER**

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes **any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights.** Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

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](mailto: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](mailto:orders@ntis.gov) <<http://www.ntis.gov/about/form.aspx>>  
Online ordering: <http://www.ntis.gov>



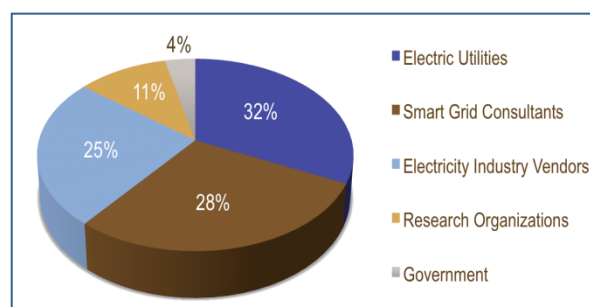
## Background and Project Overview

Faced with an aging power infrastructure and growing energy demand, the U.S. has embarked on an ambitious endeavor to expand and modernize the electric power grid, leading to a digital, highly adaptable, and demand-driven smart grid. With the current lack of cybersecurity practitioners, who will implement, secure and defend the emerging smart grid?

To address this challenge, the U.S. Department of Energy has taken the initiative to establish a cybersecurity smart grid workforce project to identify a measurement method of the identified job skills for the purpose of developing a certification. A smart grid cybersecurity certification will greatly help employers identify qualified cybersecurity professionals to protect and secure the national electric smart grid infrastructure. Pacific Northwest National Laboratory, in partnership with the National Board of Information Security Examiners (NBISE), is leading this three-phase project. Phase I of the project was completed in June 2012. This report provides a brief review of Phase I activities and documents the results to date. The complete report is available upon request.

### Phase 1: Approach and Results

In Phase I, NBISE leveraged their job performance model process to identify the roles, responsibilities, and tasks needed by smart grid cybersecurity professionals in order to perform effectively on the job. Elicitation of experts and a structured survey were employed as the primary research methods. NBISE recruited experts from diverse electric power organizations and formed a panel of subject matter experts to guide and implement the research plan. This panel (listed in the Appendix and summarized by sector in Figure 1) actively collaborated in the research process consisting of six major tasks:



**Figure 1.** Panel Membership by Sector

1. definition and consolidation of vignettes
2. classification of job roles and responsibilities
3. identification and prioritization of job goals
4. definition and refinement of tasks
5. development of a Job Analysis Questionnaire (JAQ)
6. deployment of the JAQ.

The process began with the identification and elaboration of vignettes (security scenarios) and definitions of job roles. The panel identified 44 job roles and mapped them to the National Initiative for Cybersecurity Education Cybersecurity Workforce Framework<sup>1</sup> in conjunction with the U.S. Department of Homeland Security to enable a common frame of reference for the smart grid cybersecurity workforce.

<sup>1</sup>NICE-National Initiative for Cybersecurity Education. 2011. *The National Cybersecurity Workforce Framework*. Accessed August 16, 2012 at: <http://csrc.nist.gov/nice/framework/documents/NICE-Cybersecurity-Workforce-Framework-printable.pdf>

From these 44 roles, the panel chose three dominant job roles on which to focus the job performance modeling effort. They include:


- Smart Grid Cybersecurity Operations
- Smart Grid Cyber Intrusion Analysis, and
- Smart Grid Cyber Incident Response.

Based on the three selected roles, the panel members arrived at a list of operational responsibilities associated with each job role. In turn, from those responsibilities the expert panel identified a comprehensive list of tasks to be performed by smart grid cybersecurity professionals as part of their typical duties. These job roles and responsibilities were the starting point for the JAQ.

The list of tasks helped define the broad functional boundaries of key smart grid cybersecurity job roles, but it provided limited insight into how the ability to perform part or all of the listed tasks is related to the expertise level of a smart grid cybersecurity professional. For greater granularity of the job role’s tasks, NBISE researchers identified three expertise-level designations: novice (apprentice), intermediate (journeyman), and expert (master). With the input from the panel, NBISE developed a JAQ, or survey, that included 516 operational tasks identified as potentially relevant for determining levels of expertise along with identifying performance levels expected for each of the three expertise levels. The JAQ survey was administered via the internet to a wide range of industry respondents through NBISE’s professional network as well as that of the panel. The respondents ranked the tasks into one of three specified skill levels as well as ranking the related frequency and importance for each level of expertise. An example survey element is shown in Figure 2.

\* Coordinate with administrators from other departments (i.e., networking, operating systems, servers) to identify strengths and weaknesses in the organization's logging implementations. (Task ID: R2-9140)

	Frequency					Importance				
	Never	Rarely	Sometimes	Often	Always	Unimportant	Low	Moderately	Very	Extremely
Novice (Apprentice)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Intermediate (Journeyman)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Expert (Master)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

 To make a comment about this task at the end of the survey click here

**Figure 2.** Example JAQ Element

The survey was sent to over 20 organizations including Pacific Gas and Electric Company (PG&E), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), the Electric Reliability Council of Texas (ERCOT) and the Tennessee Valley Authority (TVA), to name just a few. A profile of our target audience emerged from the demographic portion of the JAQ survey:

- 41–50 years of age (28%) and primarily male (83%)
- Employed by organizations with 10,000+ employees (43%)
- Identified their job function as Smart Grid Security (60%)
- Intermediate level of expertise in cybersecurity (25%)
- Intermediate level of expertise in smart grid operations (26%).

The survey results guide the definition and identification of fundamental and differentiating tasks, the performance of which have the potential to distinguish cybersecurity professionals' expertise levels and predict their related job performance. In this context, “fundamental tasks” include those tasks that are highly critical but show little differentiation across the skill levels of novice, intermediate or expert, while “differentiating tasks” refer to those tasks that exhibit both high criticality and high differentiation scores and thus can help separate smart grid cybersecurity professionals by their exhibited expertise levels. The survey results show that:

- 83 tasks were deemed fundamental to job performance across the three smart grid cybersecurity job roles selected by the panel; the JAQ respondents indicated that the competence on these tasks is essential and should be considered minimal entrance requirements for the field.
- 20 tasks were identified as differentiating the level of individual competence, progressing from novice to intermediate to master levels of expertise.

The identification of job roles, tasks, and vignettes as well as the classification of fundamental and differentiating tasks accomplished in Phase I created a solid foundation for Phase II research that will continue to utilize the panel of experts for identifying influential tasks and determining key performance indicators needed for smart grid cybersecurity workforce identification and evaluation.

Response to the idea of smart grid cybersecurity certification and validation has been overwhelmingly positive, with interest from groups such as DHS, DoD, CERT, NESCO, IEIA, the SANS Institute, NERC, along with large corporations such as PG&E. The project team is encouraged by the strong support from these agencies and industry partners, and will continue to engage and inform them in the next phases of the project.

## **Path Forward**

Phase 2 of the project will focus on critical analysis; building on work completed in Phase 1 as well as looking at similar work in the area of certifications. The first task of Phase 2 will include a gap and overlap analysis of existing related certifications. The resulting information will be used to better focus our work on tuning a certification approach. We will also build on the job skills identified in Phase 1 along with those identified in the NICE Workforce Framework and Electricity Subsector Cybersecurity Capability Maturity Model<sup>2</sup> (ES-C2M2). The resulting job skills broken out by domains, will be

---

<sup>2</sup> *The Electricity Subsector Cybersecurity Capability Maturity Model (May 2012)*. Accessed August 24, 2012 at: <http://energy.gov/oe/downloads/electricity-subsector-cybersecurity-capability-maturity-model-may-2012>

reviewed by the panel and then ultimately by a larger audience. Phase 2 will document how the SGC project fills a gap, what existing certifications would be good complements to the SGC certification along with a resulting job skillset that can be used to grow existing SGC workers, recruit new ones and help determine future needs.

## **Summary**

Proactive protection of the electric power grid entails timely and carefully coordinated efforts to recognize emerging risks and to prepare and entrust a certified workforce with the responsibility of protecting the nation's smart grid infrastructure. At the conclusion of this project, we will have gained a deeper understanding of how to effectively identify and measure the skills that are essential for addressing smart grid cybersecurity protection, and to develop and validate an approach for certifying the workforce.

Finally, the U.S. Department of Energy's foresight to begin this project has demonstrated the demand and opportunity to bring together policy makers, industry participants, and the research community to collectively strategize and prepare to transition the current electric power grid into a more secure and resilient power grid of the future.

This document is a summary overview of a longer, more detailed report titled: *Smart Grid Cybersecurity: Job Performance Model Report* August 2012, document clearance number PNNL-21639. Please contact Lori Ross O'Neil ([lro@pnnl.gov](mailto:lro@pnnl.gov)) for a copy of this report.



## Appendix – Smart Grid Cybersecurity Panel Roster

<b>Leaders</b>	
Justin Searle	UtiliSec
Scott King	Sempra
<b>Advisors</b>	
Bill Huntzman	Retired DOE
Emmanuel Hooper	Global Info intel and Harvard
Jamey Sample	PG&E
Joel Garmon	Wake Forest Baptist Medical Center
JohnAllen	IEIAForum
<b>Members</b>	
Andres Andreu	NeuroFuzz
Andy Bochman	IBM, Smart Grid Security Blog, DOD Energy Blog
Anthony David Scott	Accenture
Art Conklin	University of Houston
Balusamy Arumugam (Balu)	Infosys
Barbara Endicott Popovsky	University of Washington
Benjamin Damm	Silver Springs Network
Bjorn Frogner	Frogner Associates, Inc.
Bora Akyol	PNNL
Charles Reilly	SCADA Security & Compliance, So. Cal. Edison
Chris Blask	AlienVault
Chris Sawall	Ameren
Clay Storey	Avista
Cliff Maraschino	Southern California Edison
Craig Rosen	PG&E
Dan Thanos	GE Digital Energy
Don Weber	InGuardians
Ido Dubrawsky	Itron
James Pittman	Idaho Power
Jason Christopher	FERC
Jesse Hurley	NAESB Board
Kevin Tydings	SAIC
Lee Aber	OPower
Maria Hayden	Pentagon
Michael Echols	Salt River Project
Mike Wenstrom	Mike Wenstrom Development Partners
Mital Kanabar	GE Digital Energy
Nic Ziccardi	Network & Security Technologies
Sandeep Agrawal	Neilsoft Limited
Scott Saunders	Sacramento Municipal Utility District
Steve Dougherty	IBM Global Technology Services



**Pacific Northwest**  
NATIONAL LABORATORY

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

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

[www.pnl.gov](http://www.pnl.gov)



U.S. DEPARTMENT OF  
**ENERGY**