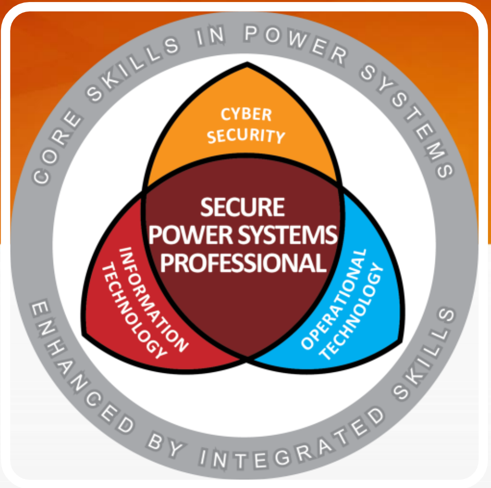
PNNL- 23583


CORE SKILLS IN POWER SYSTEMS
ENHANCED BY INTEGRATED SKILLS
CYBER SECURITY
SECURE POWER SYSTEMS PROFESSIONAL
INFORMATION TECHNOLOGY
OPERATIONAL TECHNOLOGY

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Secure Power Systems Professional Phase III Final Report: Recruiting, Selecting and Developing Secure Power Systems Professionals

August 2014

LR O'Neil	FL Greitzer
TJ Conway	AC Dalton
DH Tobey	PK Pusey

U.S. DEPARTMENT OF ENERGY

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

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
www.osti.gov
ph: (865) 576-8401
fox: (865) 576-5728
email: reports@osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
or (703) 605-6000
email: info@ntis.gov
Online ordering: http://www.ntis.gov

PNNL- 23583

Secure Power Systems Professional Phase III Final Report: Recruiting, Selecting and Developing Secure Power Systems Professionals

LR O'Neil, PNNL	FL Greitzer, PsyberAnalytix
TJ Conway, SANS	AC Dalton, PNNL
DH Tobey, VivoWorks	PK Pusey, VivoWorks

August 2014

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

Pacific Northwest National Laboratory
Richland, Washington 99352

Abstract

With significant numbers of power system experts retiring and a continuing trend of increasing complexity in modern power systems, there is a need throughout the power industry for cybersecurity awareness and competence in tasks that previously had no cyber components. To address these challenges, the U.S. Department of Energy established the Secure Power Systems Professional (SPSP) project to develop resources for job definition and competency analysis along with tools to guide assessment and curriculum design and to help identify and develop required knowledge, skills, and abilities in technical and operational power systems cybersecurity. The major accomplishments in Phase III of the project, which were built upon foundations laid in the first two phases, were (a) development and fielding of a Recruitment Guide for Human Resources and Hiring Managers and a Guide to Developing SPSPs; (b) development of psychometrically validated job profiles for identified SPSP job roles; (c) development of behavioral interview guidelines that list competencies necessary to perform each job role; and (d) development of guidelines that aid in evaluating individual and team performance and that inform strategic planning for organizations in selection, development and retention of SPSP professionals. The outcomes of the project can be immediately applied by human resources professionals, recruiters and hiring managers to assist in the recruitment, selection, and training of SPSPs, as well as to identify needed skills to grow existing employees into SPSPs.

Executive Summary

The growing deficit of electric power industry workers with sufficient cybersecurity expertise is approaching a crisis point. With significant numbers of power system experts retiring and a continuing trend of increasing complexity in modern power systems, there is a great need throughout the power industry for cybersecurity awareness and competence in tasks that previously had no cyber components. To address these challenges, the U.S. Department of Energy established the Secure Power Systems Professional (SPSP) project. The goals of the SPSP project are to

1. develop a validated model of job requirements
2. determine alignment of existing workforce development programs with these requirements
3. apply the validated model in creating resources for a holistic workforce development program grounded in current best practices.

The SPSP Project developed resources for job definition, competency analysis along with tools to guide assessment and curriculum design that will help identify and develop the required knowledge, skills, and abilities in technical and operational power systems cybersecurity. The outcomes of the project can be immediately applied by human resources personnel, recruiters and hiring managers to assist in the recruitment, selection, and training of SPSPs, as well as to identify needed skills to grow existing employees into SPSPs.

Background

The SPSP Project comprised a three-phase effort; the focus of this report is the third phase of the project. A major contribution of the first two phases of the SPSP project was to highlight the interdisciplinary nature of SPSP jobs, which require an integration of power systems engineering, information technology, and cybersecurity capabilities. This combination of skills is essential to protect the operational technology in power networks, often referred to as industrial control systems, and the supporting control system networks. The Phase I effort identified the critical, fundamental, and differentiating job responsibilities and competencies of four essential job roles: Secure Power Systems Operator, Secure Power Systems Intrusion Analyst, Secure Power Systems Incident Responder, and Secure Power Systems Engineer. An enhanced process of job task analysis was developed to address highly volatile and complex dynamic job domains in which overcoming uncertainty, ambiguity, and equivocality are key predictors of success. The result was a predictive *job performance model* that is consistent with the requirements of the U.S. Equal Employment Opportunity Commission, the International Organization for Standardization, and the American National Standards Institute guidelines for development of recruitment and selection programs. In Phase II, the competencies identified in Phase I were analyzed against current workforce development frameworks, certifications and education programs, yielding a greater understanding of how certifications, frameworks, and training/education program topics align with the job responsibilities. This allows power utilities to determine which framework approach or blending of approaches will be most appropriate for their needs. This work also highlighted the benefits of using a dynamic approach in which an organization may rotate its focus from one framework to another as ever-changing organizational needs shift over time to meet new workforce challenges.

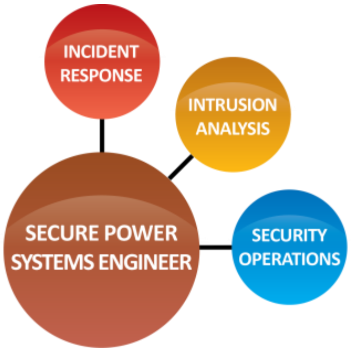
Phase III Accomplishments

Guides. The major objective of Phase III was to develop a guide to be used by human resources personnel, recruiters and hiring managers to assist in recruitment and selection of SPSPs. We applied key information gathered in Phases I and II to develop *How to Recruit Secure Power Systems Professionals – A Guide for Human Resources and Hiring Managers;* feedback received from reviewers identified another use for the information—understanding how to develop existing staff into this new role—which resulted in the creation of a second guide, *Guide to Developing Secure Power Systems Professionals*. Recruiters, hiring managers, and human resources professionals will find *How to Recruit Secure Power Systems Professionals – A Guide for Human Resources and Hiring Managers* useful for attracting and recruiting qualified SPSP job candidates. Existing staff and their line managers will find the *Guide to Developing Secure Power Systems Professionals* useful in growing existing power systems staff into SPSPs.

In producing and validating both guides, the SPSP Project team sought extensive feedback from the SPSP community, with reviews coming from three different sets of stakeholders: a panel of subject matter experts; a collection of industry professionals who evaluated the usefulness of *How to Recruit Secure Power Systems Professionals – A Guide for Human Resources and Hiring Managers* for both recruiting and hiring using a web-based survey; and a "deep dive" review with a power grid entity. These separate evaluations provided important "360-degree" feedback on anticipated use, relevance, areas for improvement, and industry/stakeholder dissemination approaches. Feedback from each review was incorporated into successive versions of the guides. The results demonstrated broad agreement among experts and industry professionals that the guides would be useful educational tools to explain the requirements for the SPSP job roles studied, as well as to help educate recruiters, or to better inform stakeholders, in the development of the SPSP workforce.

Job Profiles. A second objective of Phase III was to produce psychometrically validated job profiles that meet the U.S. Equal Employment Opportunity Commission (EEOC) and American National Standards Institute (ANSI) requirements. This was done by integrating the results of Phases I and II to capture the relevant requirements of a job that would be necessary to accurately predict performance. There are four job profiles, one for each job role identified in Phase I:

- Secure Power Systems Engineer
- Secure Power Systems Intrusion Analyst
- Secure Power Systems Incident Responder
- Secure Power Systems Operator



Each job profile begins with a list of the major responsibility areas identified in Phase I. The four workforce frameworks from Phase II are discrete sections in the job profile. The job profiles were mapped to the appropriate major job responsibilities, and each job profile has four distinct sections:

1. Major Responsibilities
2. National Initiative for Cybersecurity Education National Cybersecurity Workforce Framework Tasks
3. Electricity Sector Cybersecurity Competency Maturity Model (ES-C2M2) Objectives to Determine Maturity Level
4. Applicable Certifications

In addition, to supplement the job profiles, we developed behavioral interview guidelines that list competencies (i.e., knowledge, skills, and abilities) necessary to perform each job role. The behavioral interview guide provides a checklist for hiring managers and human resources professionals to use in tailoring selection criteria to the competency mix that is appropriate to meet specific organizational missions and goals; it can also serve as the basis for career development planning for existing staff that have interest in developing into SPSPs.

Individual and Team Performance Guidelines. A consideration in designing and developing new job profiles is to facilitate the conversion of the validated job profiles into a selection instrument and interview questions to aid hiring managers and human resources professionals. These considerations supported the third objective of Phase III, which was to produce guidelines for individual and team performance that aid in evaluating individual and team performance and that inform strategic planning for organizations in selection, development and retention of SPSPs. The primary objectives in developing the Individual/Team Performance Guidelines was to provide a resource for recruiting and interviewing candidates for new position openings and support the evaluation of individual and team performance. The Guidelines may also be used in part or in whole to align workforce capabilities with the strategic goals and tactical focus of an organization.

Implications

The SPSP project was developed to address a pervasive skills gap constraining effective response to the growing threat posed by cybersecurity vulnerabilities in critical infrastructure. A lack of experienced talent presents an increasing risk to critical infrastructure industries dependent upon technical human capital, as cited in reports of a widening skills gap threatening our nation. Traditional methods of competency modeling that require months or years to produce high-level descriptions of job requirements are ill suited to meet the constantly shifting demands and dynamic nature of the cybersecurity threat. Consequently, researchers increasingly recognize the need to adapt methods of modeling and measuring the gaps that exist in workforce readiness across professions. The SPSP project methods and findings have influenced a number of programs seeking to enhance the cybersecurity workforce and to improve the tools available to workforce planners, assessment developers, instructional designers, and personnel credentialing programs. The project’s innovative methods and detailed findings have had major impacts on workforce development, selection, credentialing, and training programs; in particular, the results

- informed workforce plans for the federal workforce, including the U.S. Department of Homeland Security

- guided re-engineering of the Defense Information Systems Agency's military schoolhouse programs intended to accelerate the proficiency of cyber operations and defense
- influenced the design of exercises and simulations that seek to engage talented youth in the science, technology, engineering and math professions (National Cyber League)
- informed certification objective development for credentialing personnel across industrial control systems disciplines, including the Global Industrial Cyber Security Professional.

Conclusions and Next Steps

The Phase III effort has identified a series of short-term tactical and longer-term strategic actions that electric power entities can take in addressing the workforce challenges that they are facing. In addition, the Phase III effort provides a call to action for leadership within the electric power sector to begin implementing some of the recommendations provided throughout the SPSP effort. The growing need and continuing skills gap is clear, and strong leaders will be needed to respond with equally increasing efforts to implement necessary programs and corrective actions. When the electric power sector once faced a similar challenge with skilled power system operators, actions were taken by entities and regulators to require the necessary staffing, development, training and credentialing programs to provide for continued reliability. The time has come for the entities and regulators to address the staffing, development, training, and credentialing needs of the cyber operators that support all of the tools and technology used to maintain a reliable electricity system.

Acknowledgments

The SPSP project would like to personally acknowledge and thank Michael Assante, Karl Perman and Josh Sandler for their contributions and support of this work.

Acronyms and Abbreviations

AMI	advanced metering infrastructure
ANSI	American National Standards Institute
C2M2	Cybersecurity Competency Maturity Model
CEH	certified ethical hacking
CIP	critical infrastructure protection
CISA	Certified Information Systems Auditor
CISM	Certified Information Security Manager
CISSP	Certified Information Systems Security Professional
CRISC	Certified in Risk and Information Systems Control
DHS	U.S. Department of Homeland Security
DOE	U.S. Department of Energy
EEOC	United States Equal Employment Opportunity Commission
ES-C2M2	Electricity Subsector Cybersecurity Capability Maturity Model
GCIA	GIAC Certified Intrusion Analyst Certification
GCIH	GIAC Certified Incident Handler Certification
GIAC	Global Information Assurance Certification
GPEN	GIAC Penetration Testing Certification
GWAPT	GIAC Web Application Penetration Tester
HR	human resources
IA	information assurance
ICS	industrial control systems
IDS	intrusion detection system
IPS	intrusion prevention system
IR	incident response
IRT	Incident Response Teams
IT	information technology
NERC	North American Electric Reliability Corporation
NICE	National Initiative for Cybersecurity Education
NTP	Network Time Protocol
OT	operational technology
SHRM	Strategic Human Resource Management
SIEM	Security Information and Event Management
SME	subject matter expert
SOC	System Operator Certification
SPSP	Secure Power Systems Professional

Contents

Figures

Tables

Report at a Glance

The Secure Power Systems Professional (SPSP) project was developed to address a pervasive skills gap constraining effective response to the growing threat posed by cybersecurity vulnerabilities in critical infrastructure. The U.S. Department of Energy responded to this call for action to secure and protect critical infrastructure by establishing the SPSP project, which has applied a holistic approach to workforce development that continuously adapts to the latest tactics, techniques and protocols—the ground truth expertise that determines competence. In this report, we review the findings of this three-year project. The third phase of this important effort establishes the framework to develop important tool sets and capabilities for selecting best-fit candidates for specific SPSP roles. This remains a challenge for electric power entities, as most lack an adequate candidate selection tool that can map behavioral interview questions to the identified SPSP roles. All three phases of the SPSP project have provided much-needed strategic findings to aid entities in addressing workforce issues; in addition, each phase has provided immediate tactical tools, data, and approaches to help solve the problems of today. Phase III is no different in this aspect, as it has provided the foundation for the industry to begin strategic work on selecting the most qualified individual for a specific SPSP role, as well as providing a tactical resource to help identify and train the SPSP employees that the industry needs now.

Below is a brief synopsis of each major section of the report. Click the graphic on the left to proceed directly to that section.

Workforce Lifecycle

Each phase of the SPSP project contributed to different processes within the SPSP workforce life cycle. A major contribution of the first two phases of the SPSP project was to highlight the interdisciplinary nature of SPSP jobs, which merge control systems engineering, information technology, and cybersecurity. The Phase III work focused on developing SPSP job profiles and new tools to support workforce development.

Guides

The Guides for Recruitment and Career Development were developed based on results of Phases I and II, and validated through three carefully designed reviews, to yield feedback from diverse perspectives: meetings with recognized experts in the field, surveying the broader operational community, and conducting onsite “deep dive” interviews on their use and effectiveness with expected users and stakeholders.

Job Profiles

The Job Profiles will facilitate the use of more accurate performance evaluations and identify gaps in proficiencies; these inform education/training and personnel-acquisition needs to support individual and team professional development.

Performance Guidelines

The SPSP Phase III effort provides an innovation in workforce development that identifies needs and gaps in the coordination of individual and team performance to reveal organization-level requirements.

Broader Impacts

The SPSP project broadly impacts workforce development programs in the many professions experiencing a severe skills gap through its innovation of a holistic approach to the expertise development life cycle.

1.0 Introduction

1.1 Impetus for Work

Government and industry now largely agree that the deficit of electric power industry workers with sufficient cybersecurity expertise is approaching a crisis point. Power system complexity is increasing and large numbers of power system security experts are retiring (O'Neil et al. 2012). Throughout the power industry, increased awareness and competence in cybersecurity is required in the performance of tasks that previously did not have cyber components. A pervasive demand for cybersecurity competence is being driven by the rapid migration of traditional field devices to digital assets. Throughout recent years, the number of new digital automation and control components that have been introduced to the market has sharply increased. There has also been a consistent trend to cyber-enable existing industrial control systems (ICS) technologies, including relay protection, sensors, actuators, breaker control, switching, and meters. This parallel increase in digital technology combined with an effort to cyber-enable existing ICS technology has resulted in a demand for cyber-aware operators, technicians, and support personnel that did not previously exist.

To address these challenges, the U.S. Department of Energy (DOE) established the Secure Power Systems Professional (SPSP) project to

1. develop a validated model of job requirements
2. determine alignment of existing workforce development programs with these requirements
3. apply the validated model in creating resources that are required as a critical first step in developing a holistic workforce development program grounded in current best practices (Assante and Tobey 2011).

To this end, the SPSP Project developed job definition and competency analysis resources and tools to guide assessment and curriculum design and to help identify and develop required knowledge, skills, and abilities in technical and operational power systems cybersecurity. The outcomes of the project can be immediately applied by human resources (HR) professionals, recruiters and hiring managers to assist in recruiting, selecting, and training SPSPs.

The SPSP Project is a three-phase effort (see Figure 1.1). The first phase began by identifying the critical, fundamental, and differentiating job responsibilities and competencies of four essential job roles (O'Neil et al. 2012). The SPSP project team applied an enhanced process of job task analysis developed specifically to address highly volatile and complex dynamic job domains in which overcoming uncertainty, ambiguity, and equivocality are key predictors of professional success (Tobey and Pusey 2014; Tobey et al. 2012; Tobey 2011d). The result is a predictive *job performance model* (JPM) that is shown to be consistent with the requirements of the U.S. Equal Employment Opportunity Commission, the International Organization for Standardization, and the American National Standards Institute (ANSI) guidelines for development of recruitment and selection programs. During the second phase of the project, we mapped the JPM elements (mission, goals, responsibilities, and tasks) to a competency model (National Initiative for Cybersecurity Education [NICE]), a maturity assessment (Electricity Sector Cybersecurity Competency Maturity Model [ES-C2M2]), learning objectives (training and education), and certification programs (O'Neil et al. 2013). In the third phase of the project (reported here), we developed guides for recruiting, selecting, and evaluating individuals and teams performing SPSP job roles. Results of this phase also provide the necessary linkages from these SPSP job roles to performance criteria for development of selection criteria for job candidates, as well as the development of guidance resources for recruiting SPSPs.

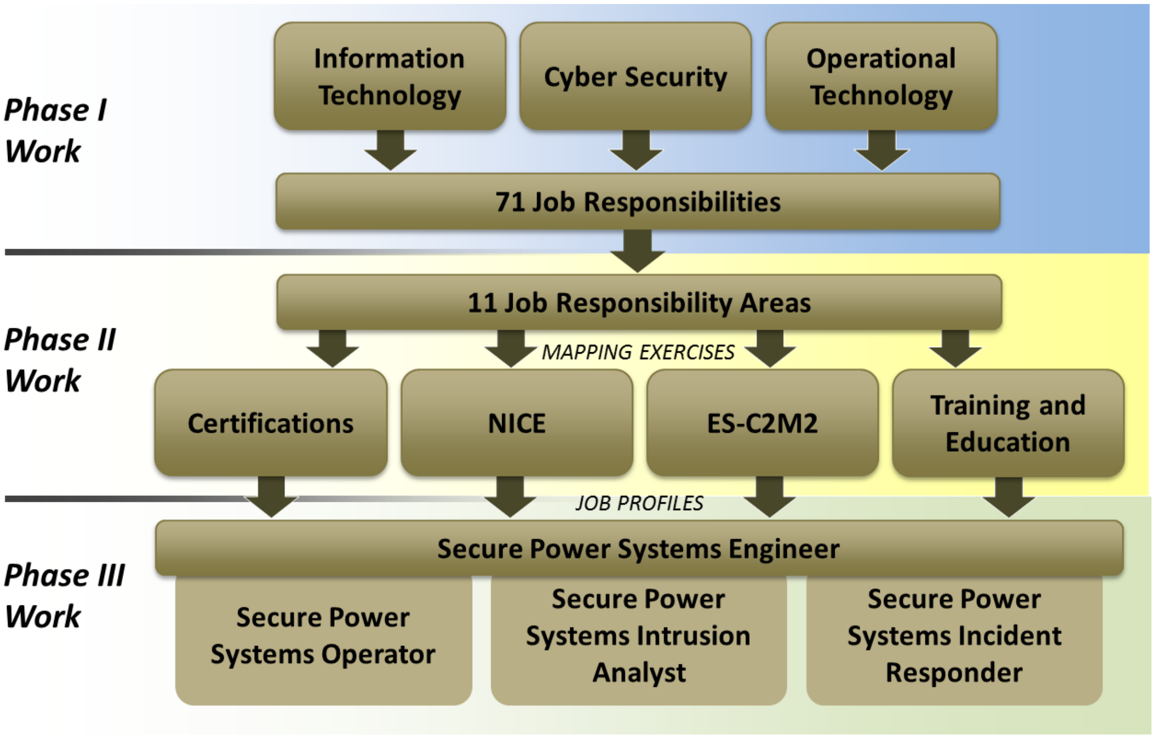


Figure 1.1. Overview of Activities in Phases I, II, and III

Figure 1.2 shows an emerging life cycle for the SPSP position that is typical for power industry employees. The overall cycle begins with workforce planning, including justifying the need for the new position within an organization and budgeting for recruitment and hiring. Justifying the need for a position represents a crucial initial step in the workforce planning cycle. Just as was the case in the cybersecurity community fifteen years ago, most organizations today do not yet realize they have a need to secure their control systems. Therefore, raising management’s awareness of the need for hiring SPSPs through case studies and supporting documentation helps establish the basis and secure organizational commitment to a budget allocation to support the identification of the gap in skills and staffing for this new position.

The next step in the life cycle may vary somewhat, depending on the existing capabilities in the organization. If current staff capabilities can extend into this position, career planning can be done to determine how to advance their capabilities to the desired level by training, gaining experience in related areas, or other professional development activities. This step is identified in Figure 1.2 as “Career Growth (I),” where the “I” indicates internal staff development. An ideal internal candidate would be someone with substantial floor or power engineering experience and a desire to learn more about cybersecurity. The other option occurs if there is a lack of existing capability or potential in the organizational staff, leading to the decision to recruit a candidate externally. This is shown as “Recruiting (E)” in the figure; “E” indicates an external search for a candidate. In this case, the search is for individuals with experience in cybersecurity of power systems, which is currently a very small pool.

The next step in the life cycle occurs when a qualified candidate is identified for the position—this occurs through external hiring or internal promotion (Hiring or Promoting). In either event, additional training and career development ("Training and Developing") will be needed for the individual to learn specific organizational details for this new position, as each site is unique.

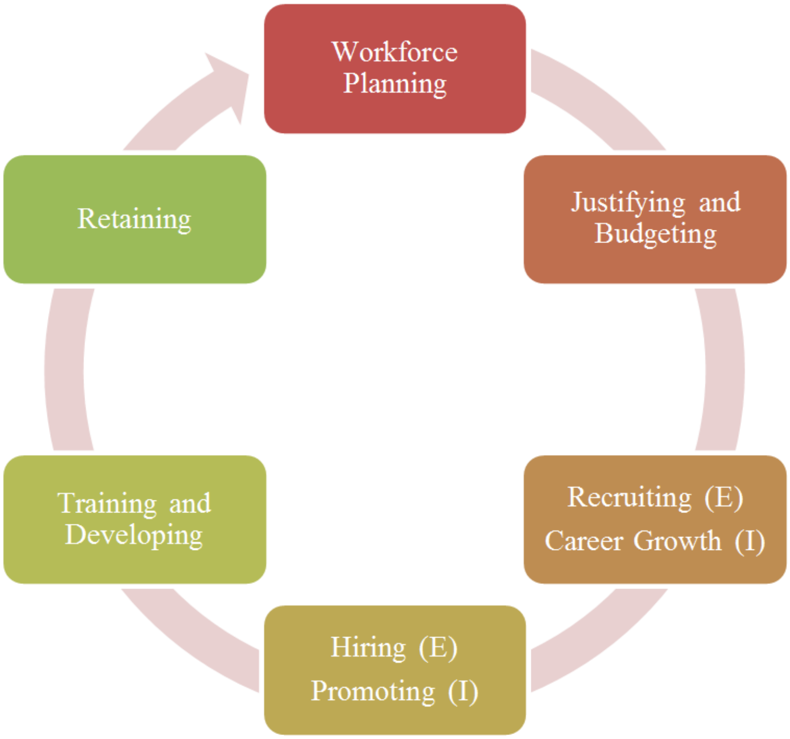


Figure 1.2. SPSP Recruiting, Hiring, and Development Lifecycle

After the organization has invested in and trained these employees, these experienced professionals become valuable to competitors, vendors, system integrators and other outside entities. Thus, "Retaining" is an important step in the life cycle: finding ways to keep job satisfaction high will help the organization retain its valuable personnel resources.

The SPSP project design wraps organically around the life cycle depicted in Figure 1.2, and each phase of the SPSP project contributed to different processes within the SPSP workforce life cycle. The processes of budgeting, recruiting, developing, and retaining correspond directly to the Pillars of Strategic Human Resource Management (SHRM) that are critical to creating resource-based competitive advantage (Lado and Wilson 1994). During each phase, expert opinions were elicited (see Panel Roster in Appendix A and Panel Demographics in Appendix B) to form a 360-degree perspective of the job role, mission, responsibilities, tasks, and competencies required to secure power systems. The psychometric rigor of the job performance modeling and workforce program mapping process in the first two phases was intended to support design of legally defensible, holistic tools for the entire SPSP life cycle during the third phase of the project.

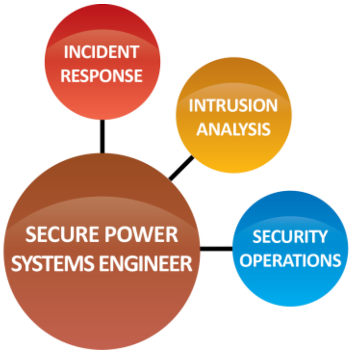
1.2 Summary of Phase I and Phase II Accomplishments

1.2.1 Identifying Job Roles and Competencies

In Phase I, an expert panel of secure power engineers identified four secure power systems job roles to be studied and discussed by the panel:

- Secure Power Systems Operator
- Secure Power Systems Intrusion Analyst
- Secure Power Systems Incident Responder
- Secure Power Systems Engineer.

A major contribution of the first two phases of the SPSP project was to highlight the interdisciplinary nature of SPSP jobs, which merge control systems engineering, information technology and cybersecurity. This union of skills is essential to protect the operational technology in power networks and advanced energy control systems.



The panel defined *goals*, *responsibility areas*, *vignette-based job responsibilities*, and *tasks* that are (a) fundamental to these job roles and (b) clearly differentiated across SPSP job activities. This information was used to develop a comprehensive set of cybersecurity competencies needed for SPSPs to do their job effectively. The competencies in this list were mapped to job roles. This provided power utilities with information that could be integrated directly into job descriptions for appropriate role definitions, competency evaluation criteria for selecting candidates, and objectives for assessing training development offerings. Mapping exercises for the identified job roles led to specification of eleven "job responsibility areas," as shown in Figure 1.3. These job responsibility areas had varying numbers of associated job responsibilities (shown in parentheses in Figure 1.3). The Phase II work continued mapping exercises, and identified existing applicable competency models, training courses and certification programs that contribute to developing the necessary knowledge, skills, and abilities required of this highly specialized workforce.

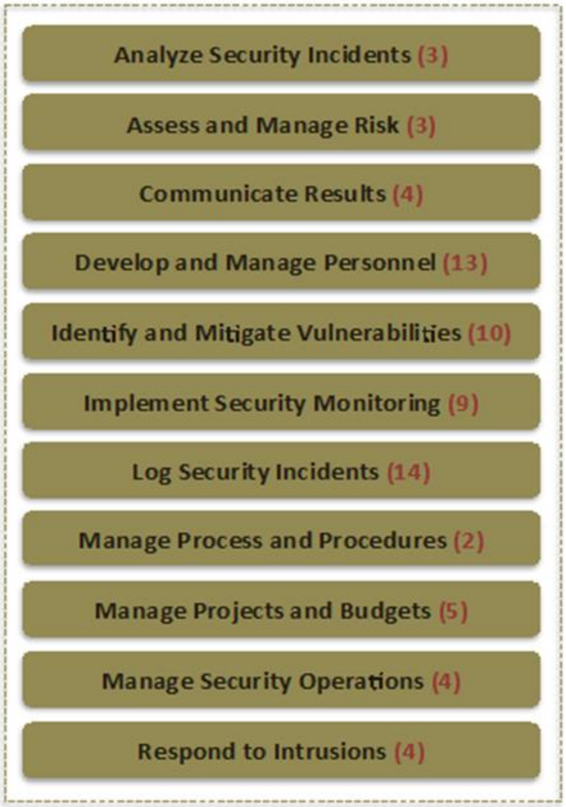

Analyze Security Incidents (3)
Assess and Manage Risk (3)
Communicate Results (4)
Develop and Manage Personnel (13)
Identify and Mitigate Vulnerabilities (10)
Implement Security Monitoring (9)
Log Security Incidents (14)
Manage Process and Procedures (2)
Manage Projects and Budgets (5)
Manage Security Operations (4)
Respond to Intrusions (4)

Figure 1.3. Mapping Job Roles to Responsibility Areas

1.2.2 Mapping Responsibility Areas to Workforce Development Frameworks

In Phase II, the competencies identified in Phase I were analyzed against current workforce development frameworks, certifications and education programs to determine how well these fulfill the current workforce needs. This provides a greater understanding of how certifications, NICE framework, ES-C2M2 framework, and training/education program topics surveyed during Phase II aligned with the job responsibilities. By identifying the competencies that are the focus of existing industry training programs, certification offerings, and capability assessment frameworks, power utilities can determine which framework approach or blending of approaches is most appropriate for their current needs. In addition to providing this guidance on certification and workforce development frameworks, the Phase II effort highlighted the benefits of using a dynamic approach, in which an organization may rotate its focus from one framework to another as ever-changing organizational needs shift over time to meet new workforce challenges.

1.2.3 Recognizing Key Activities in Developing and Maintaining Effective Secure Power Systems Environments

As illustrated in Figure 1.4, *process*, *technology*, and *people* are the three pillars of effective secure power systems environments. Performing work in highly complex and dynamic secure power systems requires

- *process knowledge and skills*—a deep understanding of both power systems and control systems environments
- programming and configuration of *technologies* that bridge cyber technology to the physical world—a diverse set of roles and competencies in operational and technical disciplines
- *recognizing people assets*—identifying and organizing the required, overlapping skills and human capital. This also requires recognition of team performance factors: a manager faced with the complicated task of locating a candidate or developing staff with the necessary mix of cybersecurity, ICS technology, and operations experience must also consider the overall strengths and weaknesses of the team and make sure that the candidate is being pursued or developed in a manner that will have a positive impact on the overall team capability.

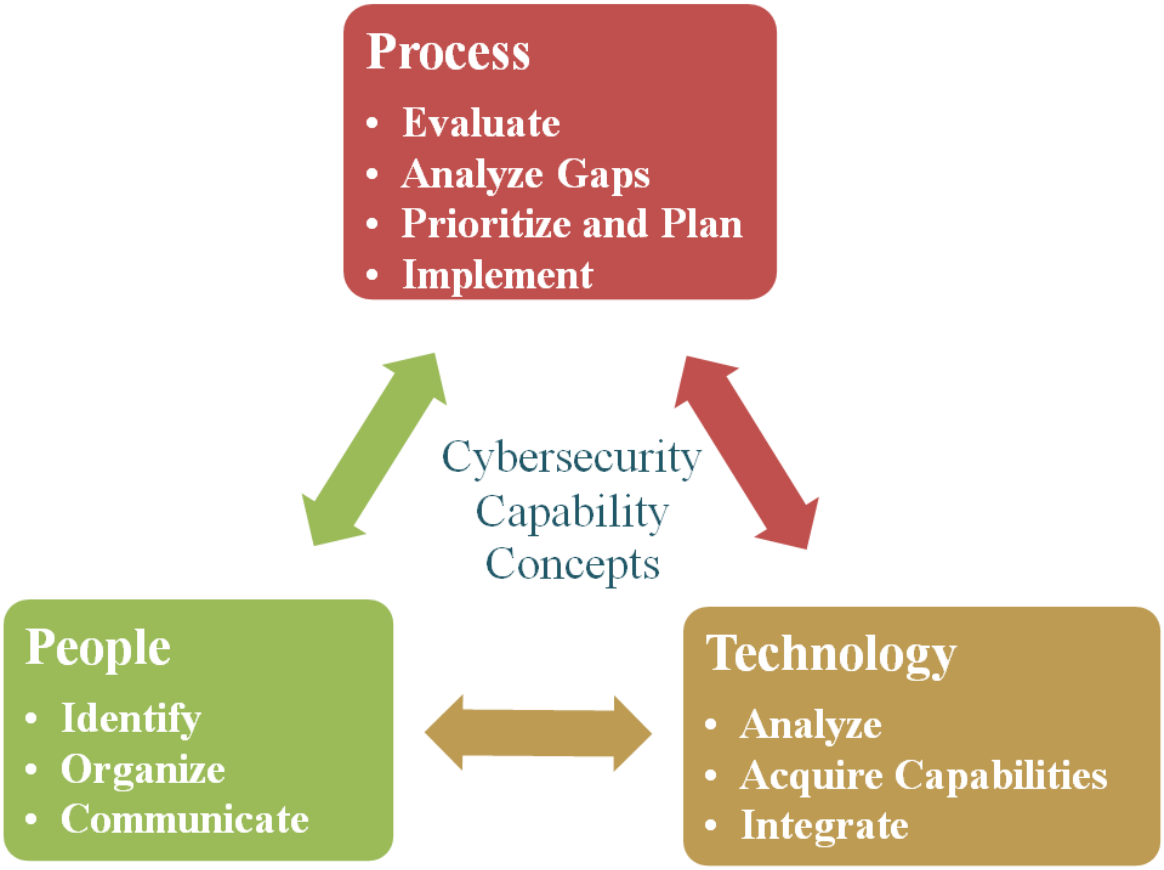
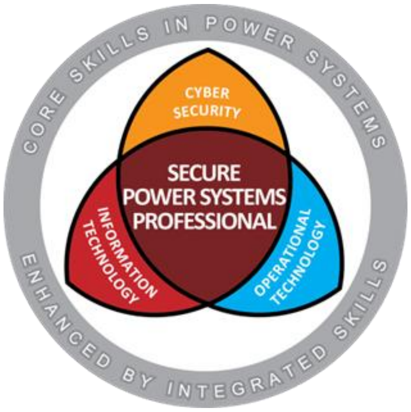


Figure 1.4. Three Pillars of Effective Secure Power Systems Environments

1.3 Phase III Purpose and Contribution

The SPSP Phase III activities extended and refined the results of the first two phases to provide a foundation for the three pillars of effective secure power systems environments depicted in Figure 1.4. This resulted in the identification of major secure power systems engineer job profiles and the development of new tools to use in the recruiting, selection, and development processes for these SPSP positions.


CORE SKILLS IN POWER SYSTEMS
ENHANCED BY INTEGRATED SKILLS
CYBER SECURITY
SECURE POWER SYSTEMS PROFESSIONAL
INFORMATION TECHNOLOGY
OPERATIONAL TECHNOLOGY

The SPSP effort focuses on the primary question: How do we help entities achieve a more reliable electric power system? We believe the key answer to this question is the development of an integrated cyber workforce that has the knowledge, skill, and ability to support and defend the electric power system operational assets.

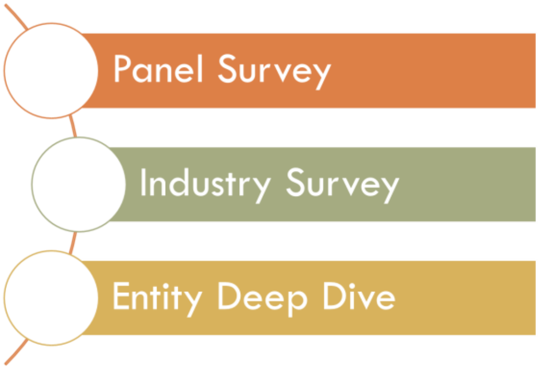
A major objective of Phase III was to develop a product that could immediately be used by industry. Two-page guides for use by HR professionals, recruiters and hiring managers to assist in recruitment and selection of SPSPs as well as career development of existing staff, were developed. The development of these guides is reported in Section 2 of this report (additional details are provided in Appendix C).

A second objective was to produce psychometrically validated job profiles that meet the Equal Employment Opportunity Commission (EEOC) and ANSI requirements. This was accomplished by grounding the profiles in detailed lists of competencies to achieve a consensus among subject matter experts (SMEs) and industry experts who would confirm the profiles' relevancy and criticality to job performance. Section 3 reports on the methods and results of developing these job profiles (additional details are provided in Appendix D. A consideration in designing and developing new job profiles is to facilitate the conversion of the validated job profiles into a selection instrument and interview questions to aid hiring managers and HR professionals. In Section 3.2, we discuss the competencies that form valid guidelines for legally defensible behavioral interviews used in recruiting SPSP professionals (details on behavioral interviews are in Appendix E). These considerations supported the third objective of Phase III, which is described in Section 4 (with details in Appendix F). This objective was to produce guidelines for individual and team performance that aid in evaluating individual and team performance, and to inform strategic planning for organizations in selection, development and retention of SPSPs.

2.0 Recruitment and Career Development Guides

Phase III of the project was intended to bring together work done in Phases I and II in the form of a final report (this document), as well as a product that the power industry can use immediately. During discussions with utilities in prior phases of the project, we observed a growing acknowledgment of the need for staff proficient in protecting the operational technology (OT) infrastructure from cyber attacks; however, stakeholders did not always know what qualifications to look for, or even how to convince management that this position was needed. Discussions with key panel members revealed a critical need for, and the value of, a guide to help recruiters and hiring managers identify skills and find candidates for this emerging SPSP job role. Design, development, and vetting of such a guide became a major objective of the project. During most of the associated design and validation activities, there was one version (originally referred to as a "recruitment guide" and referred to here as the *Guide*), but ultimately the product evolved into two complementary *Guides*:

- *How to Recruit Secure Power Systems Professionals – A Guide for Human Resources and Hiring Managers*, aimed at recruiters, hiring managers, and HR professionals, who will find the *Guide* useful for attracting and recruiting qualified SPSP job candidates;
- a *Guide to Developing Secure Power Systems Professionals*, aimed at current technical and power professionals (and their management), who can grow into SPSP job roles by developing the cybersecurity skill set.



The Guides were developed based on results of Phases I and II, and validated through three carefully designed reviews to yield feedback from diverse perspectives: meeting with recognized experts in the field, surveying the broader operational community, and conducting onsite "deep dive" interviews on their use and effectiveness with expected users and stakeholders.

The design and development of the *Guides* included extensive feedback from the SPSP community, with reviews coming from three different sets of stakeholders. First, we discussed the document with a panel of SMEs and received detailed feedback. Next, we solicited and obtained feedback from industry professionals using a web-based survey that sought to evaluate the usefulness of the *Guide* for both recruiting and hiring. Following the industry review, we conducted a "deep dive" review of the *Guide* with a power grid entity, obtaining feedback from its OT leadership, recruiting department, and HR department. These separate evaluations provided important feedback on anticipated use, relevance, areas for improvement, and industry/stakeholder dissemination approaches. Feedback from each review was incorporated into successive versions of the *Guide*. This section of the report documents the methods and results obtained in the design and development of the *Guide*.

2.1 Method

The project team created an initial draft of the *Guide* based on the findings of Phase I and Phase II. We then planned and conducted three separate reviews to support incremental improvements in its design and contents. In the first review, the *Guide* was presented to a panel of SMEs as an online survey. The *Guide* and the survey were then revised based on the feedback from the panelists. Next, an online survey was used to support evaluation of the revised *Guide* by industry professionals engaged in SPSP workforce development and related activities. Finally, after incorporating the industry feedback in the *Guide*, a "deep dive" interview was conducted with a power grid entity. The *Guide to Developing Secure Power Systems Professionals* was not created until after *How to Recruit Secure Power Systems Professionals – A Guide for Human Resources and Hiring Managers* was reviewed by the panel and industry. For this reason, all data presented in the Method section of this report referring to the *Guide* refers only to *How to Recruit Secure Power Systems Professionals – A Guide for Human Resources and Hiring Managers*.

2.1.1 SME Panel Survey Instrument

An online survey instrument was developed to solicit feedback from the SPSP expert panel. The panel was composed of senior leaders representing multiple stakeholders in secure power systems: industry, consultants, government agencies, and vendors (see Appendix A for the Phase III roster of 17 SME panel participants and the distribution of panel members by stakeholder group). Selection of panelists involved a multistep nomination and credential review process led initially by the SPSP Project Board of Advisors and subsequently by chairs and vice-chairs of the panel. Candidates were selected based on their areas of expertise and years of experience to make sure the panel comprised a broadly representative, highly qualified team of experts in secure power systems. Further information on the panel selection process may be found in the Phase I report (O'Neil et al. 2012).

Invitations to participate were sent the participants on the SME panel. The survey was administered online between February 27, 2014 and March 6, 2014. We received 10 responses; seven of those respondents answered all items in the survey and these seven were included in the subsequent analysis. While the sample was small, it served the intended function of collecting detailed feedback on the initial draft of the *Guide* from SPSP experts.

The survey was divided into five sections: a demographics section was first, followed by sections for rating of content fragments,[1] ranking of topical themes, suggesting keywords, and providing optional free-text comments.

Rankings by Topical Themes

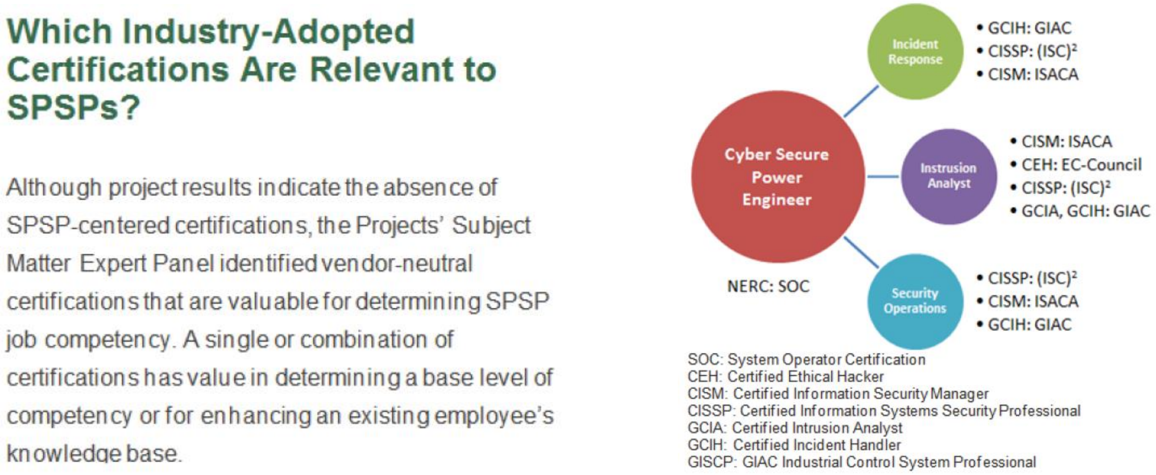
To facilitate ranking, the *Guide* was divided into ten topical themes that could include one or more content fragments. The ten topical themes are:

- Overview Information
- SPSP Job Functions

[1] A content fragment is text with or without accompanying illustrative graphics.

- Challenge: Accelerate Development of SPSPs
- What Does an SPSP Do?
- How are Skills Acquired?
- Which Industry-Adopted Certifications are Relevant?
- Profile of an Ideal Candidate
- Where to Find Candidates
- Keywords to Use in Job Postings
- DOE SPSP Project Overview

Figure 2.1 is an example of a topical theme that contains a content fragment with a graphic.



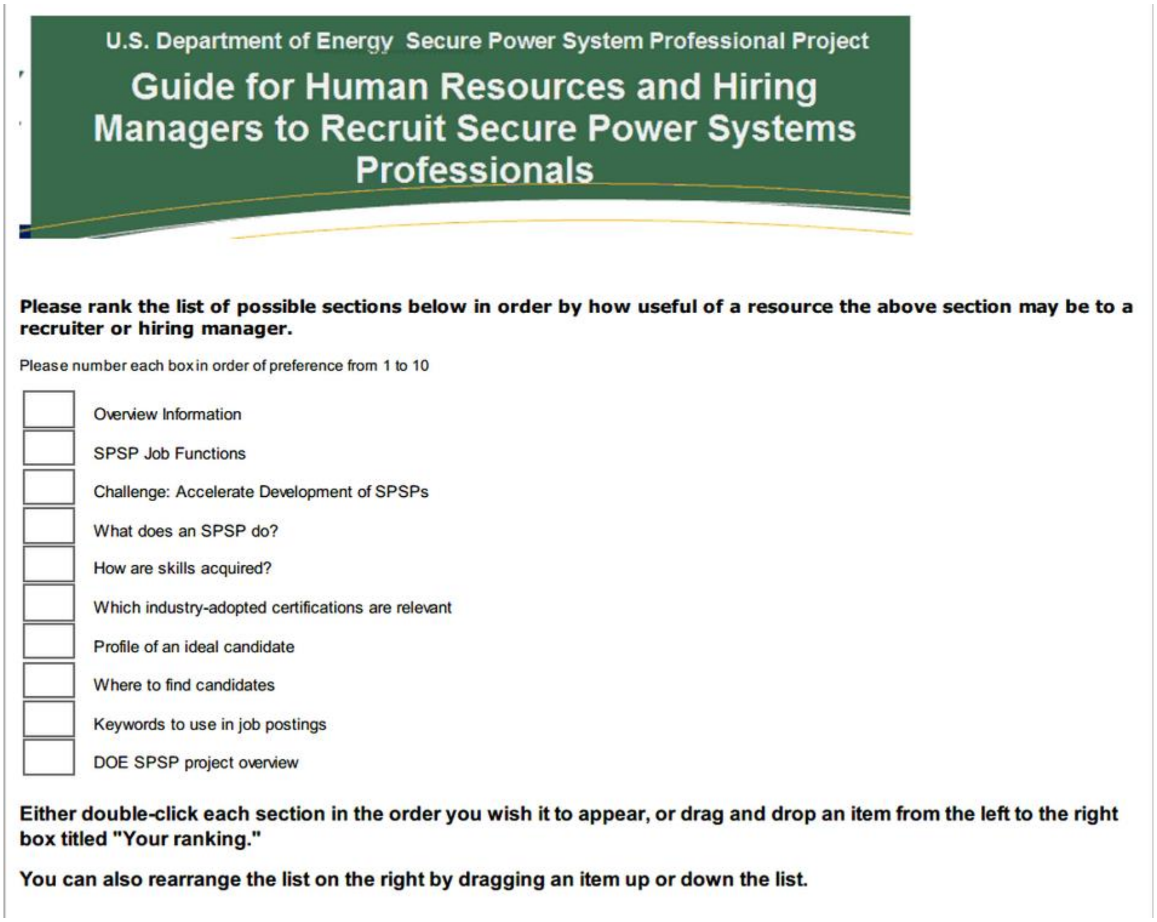
Which Industry-Adopted Certifications Are Relevant to SPSPs?

Although project results indicate the absence of SPSP-centered certifications, the Projects' Subject Matter Expert Panel identified vendor-neutral certifications that are valuable for determining SPSP job competency. A single or combination of certifications has value in determining a base level of competency or for enhancing an existing employee's knowledge base.

SOC: System Operator Certification
CEH: Certified Ethical Hacker
CISM: Certified Information Security Manager
CISSP: Certified Information Systems Security Professional
GCIA: Certified Intrusion Analyst
GCIH: Certified Incident Handler
GISCP: GIAC Industrial Control System Professional

Figure 2.1. Example of Topical Theme

For the ranking section of the web-based survey, the SPSP SMEs ranked the ten topical themes by order of importance. This was done by dragging a topical theme to its desired rank/position in the list, as shown in Figure 2.2; therefore, ties were not possible. For scoring purposes, the ten topical themes were assigned ranks from 1 to 10, where 1 = most important and 10 = least important.


U.S. Department of Energy Secure Power System Professional Project

Guide for Human Resources and Hiring Managers to Recruit Secure Power Systems Professionals

Please rank the list of possible sections below in order by how useful of a resource the above section may be to a recruiter or hiring manager.

Please number each box in order of preference from 1 to 10

□ Overview Information

□ SPSP Job Functions

□ Challenge: Accelerate Development of SPSPs

□ What does an SPSP do?

□ How are skills acquired?

□ Which industry-adopted certifications are relevant

□ Profile of an ideal candidate

□ Where to find candidates

□ Keywords to use in job postings

□ DOE SPSP project overview

Either double-click each section in the order you wish it to appear, or drag and drop an item from the left to the right box titled "Your ranking."

You can also rearrange the list on the right by dragging an item up or down the list.

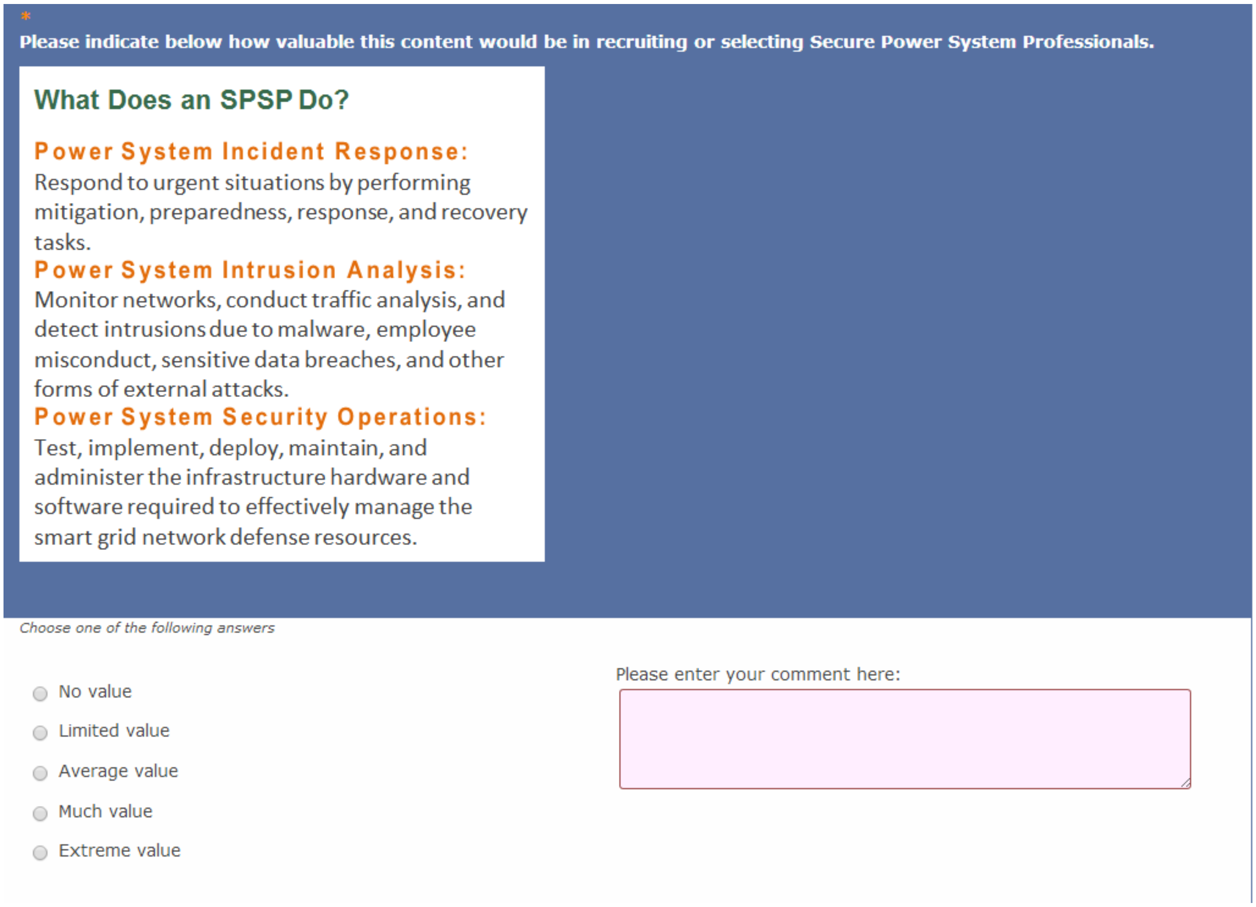
Figure 2.2. Ranking in the Online Survey

Rating of Content Fragments

For the rating section, the survey exhibited 15 content fragments taken directly from the draft *Guide*. As explained above, a content fragment is associated with a topical theme (some topical themes comprise more than one content fragment). Table 2.1 lists the content fragment titles and descriptions in the order they appeared on the panel survey. As shown in Figure 2.3, respondents were asked to rate how valuable a content fragment would be to a recruiter in the power industry, using a Likert-type scale from “Low Value” to “Extreme Value.”

Table 2.1. Content Fragment Name and Description

Content Fragment Title	Description
Overview of the Grid	Explains the North American Power Grid
Overview of Emerging Modern Power Systems	Lists the complexity and vulnerabilities of the current system
Voices from Our Expert Panel	Quotes from the expert panelists about the SPSP project
Purpose Statement	Describes need to recruit and develop SPSPs
Challenge	Identifies the challenges to accelerating the development of SPSPs
SPSP Job Functions	Lists the 11 responsibilities associated with one or more of the job roles
Venn Diagram	Demonstrates the overlapping skills (secure power systems, information technology, and OT power systems) required for an SPSP
What Does an SPSP Do?	Describes the three key job roles Secure Power Systems Professional Cybersecurity Operator, Secure Power Systems Professional Intrusion Analyst, and Secure Power Systems Professional Incident Responder
SPSP Project Overview	Lists the goals of the SPSP project
Locating Talent	Enumerates sources for finding SPSP candidates
How are Skills Acquired?	Outlines how skills are acquired, including experience, education and training, and certifications
Profile of an Ideal Candidate	Describes the qualifications, preferred skills and professional attributes of an SPSP candidate
Which Industry-Adopted Certifications are Relevant to SPSPs?	Describes the need for overlapping industry-adopted certifications to make sure the SPSP has the necessary knowledge
Certification Graphic	Lists the relevant industry-adopted certifications that are needed for each of the three SPSP job roles



*
Please indicate below how valuable this content would be in recruiting or selecting Secure Power System Professionals.

What Does an SPSP Do?

Power System Incident Response: Respond to urgent situations by performing mitigation, preparedness, response, and recovery tasks.

Power System Intrusion Analysis: Monitor networks, conduct traffic analysis, and detect intrusions due to malware, employee misconduct, sensitive data breaches, and other forms of external attacks.

Power System Security Operations: Test, implement, deploy, maintain, and administer the infrastructure hardware and software required to effectively manage the smart grid network defense resources.

Choose one of the following answers

○ No value
○ Limited value
○ Average value
○ Much value
○ Extreme value

Please enter your comment here:

Figure 2.3. An Example of the "What Does an SPSP Do?" Content Fragment

Keywords

The SME panelist survey provided a text box for respondents to list keywords to be used in job postings. The following keywords were listed by the expert panelists:

- industrial control
- CIP (critical infrastructure protection)
- NERC (North American Electric Reliability Corporation)
- energy
- cybersecurity
- critical infrastructure
- mission critical
- team player

It should be noted that the Keywords section is unique in this survey for two reasons. First, it is the only open-ended section in the survey, requiring direct keyword input from the survey respondents. Second, because it was ranked by the SME panel as the least important topical theme (scoring a 10, i.e., not highly valuable to recruiting and selecting SPSPs), it was excluded from the analysis of the industry survey, thus reducing the number of analyzed topical themes from ten (10) to nine (9).

2.1.2 Industry Survey Instrument

Minor revisions were made to the *Guide* based on feedback obtained from the SME panel (some changes are described below in Section 2.2; details are provided in Appendix C). An online survey instrument was then created to solicit feedback from industry professionals and to compare their responses with those of the SPSP expert panel. This revised survey was administered online between March10th and March 23rd, 2014. Participants were solicited from power systems industry groups and SANS Industrial Control Systems students by the project team via email and in person. Additionally, SPSP reviewers were encouraged to ask their recruiting and HR professionals to participate. A total of 42 industry professionals participated in the survey.

Table 2.2 shows the breakdown of job functions and levels of expertise for this sample: nearly two-thirds of the respondents classified themselves as technical staff, and 43% considered themselves to be at an intermediate level of expertise. Additional details on Phase III demographics are provided in Appendix B; (Appendix B also provides summary data on Phase I and Phase II demographics).

Table 2.2. Phase III Survey Respondent Job Functions and Expertise Levels

Job Function	Number	%
Human Resources Staff	7	17%
Power Systems Staff	9	21%
Technical Staff	26	62%
Total	**42**	100%

Expertise Level	Number	%
Beginner	16	38%
Intermediate	18	43%
Expert	8	19%
Total	**42**	100%

The organization of the survey was similar to that of the SME panel review: after the demographics section there were additional sections for rating of content fragments, ranking of content fragments, providing an overall value of the *Guide*, and free-text comments.

Using the same procedure that was employed in the SME panel review, the survey asked participants to evaluate topical themes of the *Guide* (same procedure as the panel review). Because of changes made to the content of the *Guide* following the SME panel review, the topical themes used for the industry review were similar, but not identical, to the topical themes described in the SME panel review:

- Job Functions
- What Does an SPSP Do?
- Candidate Profile
- Overview of Emerging Modern Power Systems
- Quotes from the Expert Panelists about the SPSP Project
- SPSP Skills

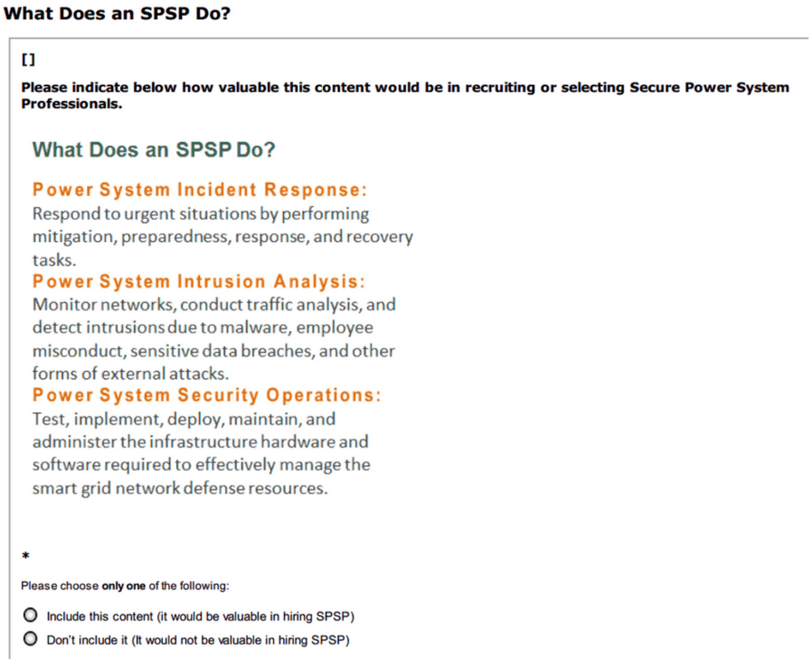
- Project Overview
- Certifications
- Locating Talent
- Keywords to Use in Job Postings (this topical theme was not analyzed).

Rating of Content Fragments

The industry survey design was altered based on an analysis of the SME panel responses and an analysis of the time required to complete the survey. To reduce the time required to complete the survey, the 23-item survey was restructured and the content fragment questions were changed from a rating scale to a binary response, i.e.:

○ Include this content (it would be valuable in hiring SPSPs) or
○ Don't include it (It would not be valuable in hiring SPSPs).

Figure 2.4 shows the content-fragment rating question for "What Does an SPSP Do?"



What Does an SPSP Do?

[]

Please indicate below how valuable this content would be in recruiting or selecting Secure Power System Professionals.

What Does an SPSP Do?

Power System Incident Response: Respond to urgent situations by performing mitigation, preparedness, response, and recovery tasks.
Power System Intrusion Analysis: Monitor networks, conduct traffic analysis, and detect intrusions due to malware, employee misconduct, sensitive data breaches, and other forms of external attacks.
Power System Security Operations: Test, implement, deploy, maintain, and administer the infrastructure hardware and software required to effectively manage the smart grid network defense resources.

*

Please choose **only one** of the following:

○ Include this content (it would be valuable in hiring SPSP)
○ Don't include it (It would not be valuable in hiring SPSP)

Figure 2.4. Content Fragment "What Does an SPSP Do?"

Unlike the panel survey, which provided space for comments for each content fragment, the industry survey respondents were prompted to provide comments only at the very end of the survey.

Rankings by Topical Themes

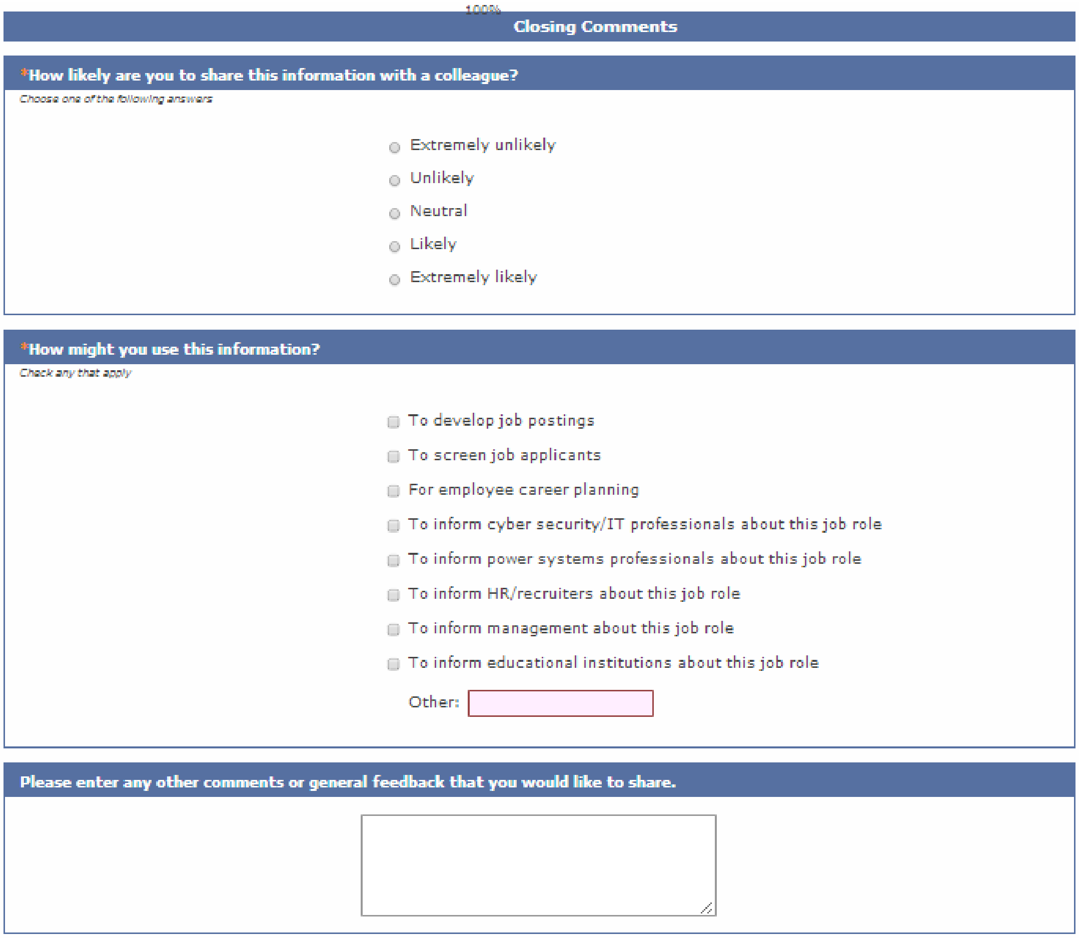
Similar to the participants in the SME panel survey, industry participants were also asked to rank order the ten sections of the *Guide*. The format of the ranking was identical to that included in the SME panel survey (see Figure 2.2).

Overall Value of the Guide

While the SME panel survey included ratings of the value of each content fragment, the industry survey only asked respondents to rate the overall value of the *Guide* by answering the question, “Please indicate below how valuable this Guide would be in recruiting or selecting Secure Power Systems Professionals.” Consistent with the rating sections of the survey, respondents were asked to rate how valuable the overall *Guide* would be to a recruiter in the power industry using a Likert-type scale from “Low Value” to “Extreme Value.”

Comments

Finally, industry respondents were asked to provide closing comments indicating how likely they were to share this information with a colleague, how they might use the information, and any other comments or general feedback they would like to share (see Figure 2.5).



100%

Closing Comments

*How likely are you to share this information with a colleague?

Choose one of the following answers

○ Extremely unlikely
○ Unlikely
○ Neutral
○ Likely
○ Extremely likely

*How might you use this information?

Check any that apply

□ To develop job postings
□ To screen job applicants
□ For employee career planning
□ To inform cyber security/IT professionals about this job role
□ To inform power systems professionals about this job role
□ To inform HR/recruiters about this job role
□ To inform management about this job role
□ To inform educational institutions about this job role

Other:

Please enter any other comments or general feedback that you would like to share.

Figure 2.5. Closing Comments

2.1.3 Deep-Dive Review

An onsite analysis was conducted with an energy company with responsibility over control center operation, generation resources, transmission resources, distribution resources, and energy trading. The SPSP panel chair performed an in person *Guide* analysis exercise with representatives from the entity after the panel and industry surveys were complete. The onsite analysis was pursued to gain an increased understanding of how the *Guide* would likely be used, how it could be improved, and the best approach to socialize the *Guide* across the various stakeholder communities. The entity provided representatives from the OT leadership team, the recruiting personnel, and the HR personnel that are directly responsible for supporting the SPSP-related positions. The representatives provided direct feedback on a number of specific areas, and overall affirmed the relevance of the effort, found the resource guide valuable, and believed they would make routine use of the material, depending on the dynamic nature of where they may be in the workforce development life cycle at any given time.

2.2 Results

2.2.1 Survey Instrument

For the SME panel, the median time required to complete the survey was 16 minutes and 29 seconds. The distribution of completion times was highly skewed by two respondents who required 81.5 and 145.5 minutes to complete the survey, respectively. If we remove the completion times for these two respondents, the mean response time was 5 minutes and 35 seconds and the median time to complete the survey was 7 minutes and 54 seconds. Since the SME panelists are volunteers who are critical employees in their organizations, we suspect that the two respondents who required substantially more time to complete the survey may have been interrupted and left the survey active on their computer screen until they returned to complete it.

Based on this result, we modified the survey instrument to reduce the required time to complete the review. The survey was revised to make it better fit the interests and schedules (time availability) of the intended industry experts, whose feedback was solicited to provide verification and validation for the *Guide*. For example, changing the responses to binary answers served to decrease the length of time required to complete the survey.

2.2.2 Analysis of Survey Feedback

Detailed results of analyses of the SME panel survey and the industry survey are provided in Appendix C. Because the results were similar, here we provide an overview and discuss a few notable differences in feedback obtained from these two cohorts.

A primary objective in obtaining feedback from industry was to determine whether additional changes were needed beyond the changes that were made based on the SME panel survey. The analysis would also take into account any possible differences in the results of the panel survey versus the industry survey. At the outset, we established a criterion "threshold" for retaining a content fragment of 33% favorable ratings of the value of the fragment—i.e., if at least one-third (33%, inclusive) of all respondents from each survey considered the content to have value, it would be retained. We were also interested in comparing the rankings of different sections or topical themes of the *Guide*.

A summary of the topical-themes ranking results for the SME panel survey and the industry survey is provided in Table 2.3, which allows a comparison of the rankings by these two cohorts of the nine topical themes that were analyzed (as noted previously, the tenth topical theme, *keywords*, was not analyzed for the industry survey). As a general observation, the results from the industry survey were consistent with those of the SME panel survey, i.e., there was a high level of consensus regarding the value of the topical themes between these two cohorts, despite potential differences in their job functions. The only notable discrepancies are the rankings of the Project Overview (9 for SME panel, 6 for Industry) and Locating Talent (4 for SME panel, 8 for Industry). Nevertheless, these topical themes received greater than 33% support by both cohorts, so this result did not suggest that these sections be removed.

Table 2.3. Comparison of Guide Section Ranks Assigned by SME Panel Versus Industry Participants*

Thematic Area of *Guide*	**SME Panel Ranking**	**Industry Ranking**
Job Functions	1	1
What Does an SPSP Do?	2	2
Candidate Profile	3	3
North American Power Grid Overview	5	4
How are Skills Acquired?	6	5
Project Overview	9	6
Which Industry-Adopted Certifications are Relevant to SPSPs?	7	7
Locating Talent	4	8
Challenge: Accelerate Development of SPSPs	8	9

* Rankings based on nine topical themes of the *Guide*

Because of some variations in rankings and ratings between the SME panel and industry respondents, we also analyzed the responses in more detail. One detailed analysis of interest was to compare SME panel versus industry ratings of the value of specific content fragments (a thematic area or section of the Guide could comprise one or more such content fragments). For the industry survey, the “value” was a binary variable (include content—has value, versus do not include content—has no value), while the SME panel survey acquired these responses using a five-point Likert scale (no value, limited value, average value, much value, extreme value). This scale was converted into a rating from 1 to 5 for each content fragment. Any content fragment with a mean rating of 2.5 or greater was considered to be rated as valuable by panel respondents. Similarly, the industry binary choice was converted to a score of 1 or 0 and any item receiving a “1” from at least 50% of the respondents was considered valuable. Based on these analyses of ratings by the SME and industry participants, we found that all but one of the content fragments received at least 33% support from both cohorts: the exception was the *Expert Voices* content fragment (this content fragment contained quotes from the expert panel; it was part of the North American Power Grid topical theme). Because of its low ratings, it was identified as a candidate for removal from the *Guide*.

A second detailed analysis of interest was focused on further delineating the responses of industry participants based on their job functions (specifically, Human Resources versus Technical/Power Engineer respondents). The responses of Human Resources professionals were compared with the combined responses of technical and power engineers. While all of these industry respondents agreed that three topical themes (*SPSP Job Functions*, *What Does an SPSP Do*?, and *Candidate Profiles*) are paramount, the HR professionals rated some constituent content fragments somewhat differently than the participants in the technical job functions group. These content fragments are shown in Figure 2.6, which plots the percentage of value ratings of each content fragment as rated by Human Resources versus Technical/Power Engineer participants. Even though there are differences in absolute ratings, the plot shows that the relative ratings of these five content fragments are similar within these two groups of participants.

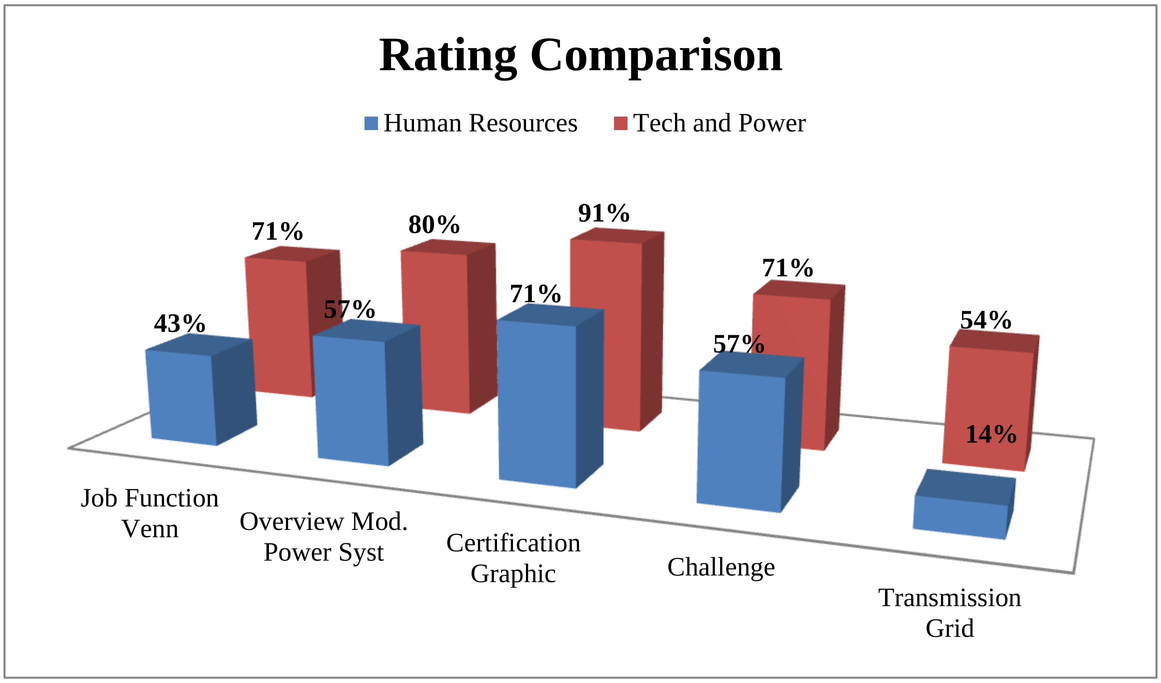


Figure 2.6. Comparison of Ratings by Human Resources and by Technical and Power Professionals on Five Content Fragments

In summary, there was substantial agreement between SME panel participants and industry participants (as well as different subsets of the industry participants representing Human Resources versus technical job functions). The *Guide* overall was generally viewed as a very valuable resource. For example, six of the seven panelists said they saw value in sharing the document within their organization. However, the presence of subtle differences in rankings for some sections of the *Guide* suggested the possible value of creating different versions of the *Guide* attuned to the specific needs and preferences of each audience. At a minimum, the *Guide* could be made significantly more useful by highlighting the three most important sections (*SPSP Job Functions*, *What Does an SPSP Do*?, and *Candidate Profiles*).

2.2.3 Results of Interviews

As noted above, the onsite review of the *Guide* was conducted with an electric utility with responsibility over control center operation, generation resources, transmission resources, distribution resources, and energy trading. The purpose of the onsite analysis was to gain an increased understanding of how the guide is likely to be used, how it could be improved, and the best approach to socialize the guide across the various stakeholder communities. The findings are summarized as follows:

1. **Relevance.** The interview examined the relevance of a proposed section within the *Guide*. This section would focus on useful keywords for organizations to use in job postings that would be likely to attract strong SPSP candidates. There was not a strong response from the panel or industry to the keyword section of the *Guide* and the entity interview affirmed that this proposed section of the guide would have little to no value for industry implementation. Rather, they felt that each entity would find greater success in implementing job-specific filtering questions for prospective candidates to answer within the application process.

2. **Specificity.** The entity identified a number of the *Guide* components that provided guidance on programs or resources that organizations could use in finding or selecting candidates. However, the entity felt that the *Guide* would be more useful if more specific information were provided directly in the *Guide*. The SPSP project team felt this would be a useful approach and would provide direct guidance for an entity. However, a potential disadvantage of this approach is that it would require an ongoing industry effort to evaluate and refresh the *Guide* to keep the content up to date.

3. **Use.** Feedback was provided by the entity to make sure that the format of the resource guide would be easily disseminated by the various stakeholders making use of the document. Guidance was provided to make sure the *Guide* would be available for organizations to download electronically, print in a variety of formats and layouts, and remain as selectable images and text so they could be repurposed in awareness and education campaigns. While the original goal was to produce a tool for recruiters, the feedback identified another use, namely understanding how to develop existing staff into this new role, resulting in the creation of the second guide, the *Guide to Developing Secure Power Systems Professionals.*

4. **Distribution/Dissemination.** The *Guide* should be made available to power utilities with distribution capability to education institutions, third party recruiters, SHRM, regional HR utility associations, utility commissions, and other relevant critical-infrastructure-sector industry associations.

2.3 Guides: Conclusions

In conclusion, the SME panel and industry professionals responding to the survey as well as on-site interviews felt the *Guide* would also be a useful educational tool to explain the requirements for the SPSP job roles. For this reason, a second guide was created, the *Guide to Developing Secure Power Systems Professionals*. Existing staff and their line managers will find the *Guide to Developing Secure Power Systems Professionals* useful in growing existing power systems staff into SPSPs. Qualitative feedback, collected from panel and industry respondents, further indicates that the respondents felt the *Guide* will be useful to help educate recruiters, and to better inform stakeholders, in the development of the SPSP workforce. Finally, several of the qualitative comments suggested that the respondents found value in the process and work product and indicated the desire to participate in future phases of the SPSP program.

Guides

The Guides are a valuable resource to identify SPSP job roles and requirements that will aid in the development of the SPSP workforce.

Analysis of the feedback from the SME panel and the industry survey revealed a high level of consensus about the usefulness of the topical themes, despite important differences in professional backgrounds between these two cohorts. Broadly speaking, the panel and industry survey analyses suggested that all but two topical themes of the *Guide* should be retained; the two topical themes that were considered least useful, and therefore candidates to be deleted, were (a) the *Expert Voices* and (b) the *Keywords*. The low rating for the *Expert Voices* remains unexplained. A possible explanation for the *Keywords* section being rated as the least valuable came from a discussion of the SME panel survey results with stakeholders at the deep-dive onsite review. This discussion revealed that keywords should be specific to each power entity, and therefore it is difficult to find meaningful terms that are useful for all entities.

As noted, the *Guide* went through several designs and substantive iterations based on feedback obtained in the panel, survey, and interview phases. The analysis of survey responses suggested some differences in ratings between HR professionals and technical respondents. These differences could indicate a disparity in knowledge between the HR and technical respondents; therefore, the *Guide* could be a useful educational tool to explain the complexities of SPSP job roles to people who are unfamiliar with these emerging job roles. This conclusion is supported by qualitative feedback received during interviews by Tim Conway, the SME panel chair. The feedback indicated that the respondents felt the *Guide* would be useful to help educate recruiters.

Some of the subtle differences in ratings or rankings of different sections of the *Guide* suggested the value of creating versions of the *Guide* attuned to the specific needs and preferences of each audience—e.g., one for HR professionals and another for the technical and power professionals. At a minimum, it was suggested that the *Guide* could be made significantly more useful by highlighting the three most important sections, as determined by the survey analyses, in the published version of the *Guide*. Given these considerations, the project team decided to develop two distinct versions of the *Guide* to maximize its impact and usefulness for different stakeholders/users. The final, published forms of both *Guides* are provided in Appendix G.

3.0 Job Profiles

Corresponding to the job roles identified in Phase I, four job profiles were created in Phase III: Secure Power Systems Security Engineer, Secure Power Systems Intrusion Analyst, Secure Power Systems Incident Responder, and Secure Power Systems Operator.

3.1 Method

The four job profiles created in SPSP Phase III capture the relevant requirements of a job that are necessary to accurately predict performance. In SPSP Phase I, a statistically valid sample of SMEs participated in a process that created a nomological network of factor relationships, which identified critical tasks related to job performance of the four job roles. Phase II of this project enabled the identification of appropriate NICE National Cybersecurity Workforce Framework Tasks and ES-C2M2 Objectives to Determine Maturity Level and relevant certifications for each job role. This work was completed using online questionnaires and a review and comment system. Agreement analyses were completed and resulted in the final lists of job goals, responsibilities and tasks stored in a database that also contained the mapping of the these elements to the NICE tasks, ES-C2M2 objectives and relevant certifications. The complete descriptions of the Phase I and II methodologies can be found in the final Phase I and Phase 2 reports (O'Neil et al. 2012, 2013). Phase III merged the results of Phases I and II to create the four job profiles found in Appendix D.

3.2 Outcomes

3.2.1 Job Profiles

The job profiles reported in Appendix D derive from the work of Phases I and II. They are presented in a format that meets the EEOC and ANSI requirements of psychometrically validated job profiles (Arvey 1979; 43 FR 38290–38315 1978; Kesselman and Lopez 1979; Pursell et al. 1980). There are four job profiles, one for each job role identified in Phase I.

- Secure Power Systems Engineer (Appendix D.1)
- Secure Power Systems Incident Responder (Appendix D.2)
- D.3 Secure Power Systems Intrusion Analyst (Appendix D.3)
- Secure Power Systems Security Operator (Appendix D.4)

Each job profile begins with a list of the major responsibility area identified in Phase I. The four next-step workforce frameworks from Phase II are discrete sections in the job profile. The job profiles were mapped to the appropriate major job responsibilities, and each job profile has four distinct sections:

1. Major Responsibilities
2. NICE National Cybersecurity Workforce Framework Tasks
3. ES-C2M2 Objectives to Determine Maturity Level
4. Applicable Certifications

3.2.2 Behavioral Interview Guidelines

The behavioral interview guidelines provide lists of competencies (i.e., knowledge, skills, and abilities) necessary to perform each job role to guide interview or other selection processes. The list of competencies for each job role can be found in Appendix E. Table 3.1 is a brief excerpt showing that the lists serve as guidelines or a checklist for hiring managers and HR professionals to aid the selection of the competency mix determined as appropriate to meet the organizational mission and goals. A complete description of how to use the Competency-Based Behavioral Interview Guidelines is provided in Appendix E.

Table 3.1. Excerpt from Section E.2, Behavioral Interview Guideline Items: Secure Power Intrusion Analyst

X	**Knowledge** ***The understanding of a concept, strategy, or procedure; knowledge is measured by depth of understanding, from shallow to deep***
	Collect a sequence of events and continue to add information based on the investigation process
	Subscribe to vulnerability feeds and maintain information-sharing subscriptions
	Train Incident Response Team on the usage of an attack technique table
	Understand NERC CIP and audit requirements

X	**Skill** ***The reliable application of knowledge to achieve desired outcomes; skill is measured by the degree of reliability, from inconsistent to consistent***
	Configure rules for Security Information and Event Management (SIEM) tools to capture and flag events known to be intrusion indicators
	Coordinate reactive and proactive responses
	Develop a schedule for testing elements of the incident response plan and organizations involved in the process
	Develop attack scenarios that might be used to intrude upon systems and networks and use tabletop exercises to gauge how personnel might respond in these situations
	Escalate analysis findings in accordance with defined plan
	Maintain a current list of stakeholders' contact information and cross-listing with respect to notification requirements
	Maintain chain of custody and integrity of log files if they are to be used by law enforcement at a later date
	Test implementation with a testing regime to include events that should trigger alerts based on how the monitor has been configured
	Update database of device configurations upon changes to configurations

X	**Ability** ***The application of skills to new domains; ability is measured by the extent of skill transfer, from narrow to broad***
	Analyze monitoring technique to determine whether newer technology better accomplishes the mission
	Update database of device configurations upon changes to configurations
	Analyze test results to make sure systems are functioning nominally

X	**Ability** ***The application of skills to new domains; ability is measured by the extent of skill transfer, from narrow to broad***
	Report what was analyzed and the list of flagged events, key findings, issues, and actions taken
	Review “healthy” log collection metrics to understand baseline from which to measure normal performance
	Select a team of internal experts that should be consulted

The behavioral interview questions support three other important HR tasks relating to talent development. These interview questions are designed to

- structure gap analyses of critical and fundamental employee knowledge, skills, and abilities
- support individual and team development plans
- help HR professionals understand the quality/capabilities of the individual employees/job candidates

The contents of the job profile can be used by any HR or testing entity to develop a selection tool that would be EEOC compliant.

3.3 Implications for Developers of Workforce Development Programs

The job profiles created by the SPSP project may be applied to determine alignment of recruitment and selection programs with various workforce programs. The workforce framework objectives of the NICE and ES-C2M2 differentiated by job role can be used to align job descriptions with workforce requirements of government and industry. The certifications section of the *Guide to Developing Secure Power Systems Professionals* provides HR professionals with information relating to the qualification of personnel for specific task domains within each job role.

The alignment of these workforce programs with staff development can be accomplished by using the behavioral interview guidelines. First, managers or HR specialists may rate the performance or capability of a job incumbent or a new hire for each competency listed in the behavioral interview guidelines. Second, personal development plans may be constructed by creating separate checklists of competencies that indicate areas of strength, weakness, opportunities, or threats for an individual or team. Third, these checklists may be used to determine the appropriate intervention necessary to increase competence (Tobey and Pusey 2014). Knowledge may be developed by selecting training courses with learning objectives aligned with the target competency; skill may be developed by providing access to experiential assignments or simulation exercises; and job rotation or systematic variation of simulations may be used to develop ability. Finally, the checklists may be used to guide assessment development or evaluation of training program effectiveness to make sure competence improvements are meeting organizational objectives.

Job Profiles

The Job Profiles will facilitate the use of more accurate performance evaluations and identify gaps in proficiencies, which informs education/training and personnel acquisition needs to support individual and team professional development.

The detailed specification of job responsibilities, job descriptions, applicable certifications, and competencies enumerated in the job profiles and behavioral interview guidelines will be useful in answering the following questions that are important for workforce development:

- To what degree does an individual or team feel they can perform the responsibilities of the NICE functional roles?
- How mature are staff capabilities to meet the objectives identified by the ES-C2M2?
- What certifications are likely to best inform independent analysis of proficiency based on job role or organization-specific responsibility assignments?
- What education and training programs should be given priority in an individual- or team-based development plan?
- What competencies (knowledge, skills, or abilities) should be included in queries requesting examples of prior experience or work history of a candidate during an interview or other selection process?

The Phase II outcomes yielded important implications for developers of workforce development programs:

1. Education, training and certification programs should document how their curriculum's learning objectives align with the job responsibilities emphasized in the competency frameworks. This would include stating explicitly the job role(s) and/or the specific responsibilities of that job that the program is targeted to improve or assess.
2. Second, development programs should align their outcomes with these same responsibilities. For instance, exam items would be developed and validated to measure knowledge, skill, and ability defined in the behavioral interview guidelines as required for task performance within a responsibility area. Further, rather than providing the student with a summative score—a grade or a pass/fail based on an overall cutoff score—a student should receive a profile report indicating areas of strength and weakness in executing the tasks necessary to fulfill the target responsibility. This competency profile would enable both individuals and their organizations to better map and align future development with those programs designed to address gaps shown through these formative assessments.
3. Third, program descriptions and outcome results should specify the program's level of expertise (Benner 2004; Dreyfus and Dreyfus 1980). Programs designed for beginners should demonstrate that they are covering the fundamental responsibilities and tasks. Likewise, programs designed for development of competent or expert practitioners should demonstrate that they are emphasizing those differentiating responsibilities and tasks.
4. Finally, program effectiveness evaluation should be based on a demonstration of either breadth or depth of competency profile improvement according to how the program is aligned with the JPM for the targeted job role.

In future phases of this project, the competencies listed in the behavioral interview guideline items may be converted into a valid, legally defensible selection instrument, and a corresponding interview protocol based on the guideline items may be developed. The composition of the behavioral interview guideline items is grounded in foundational work by Pursell et al. (1980). The behavioral interview has been adopted by most HR professionals as it provides a reliable and defensible process for selecting job candidates. Adler (2013) concludes that the behavioral interview is a tool that helps HR professionals comply with U.S. labor law. There are key elements of behavioral interviews that can be developed from the behavioral interview guideline items in the job profiles. These include

- fair, nondiscriminatory process for selection
- job relevant
- connects critical tasks to job roles and workforce frameworks
- consistent assessment for interview teams
- accommodates thorough documentation

4.0 Individual and Team Guidelines

The primary objectives in developing the Individual/Team Performance Guidelines was to provide a resource for recruiting and interviewing candidates for new position openings and support the evaluation of individual and team performance. The Guidelines may also be used in part or in whole to align workforce capabilities with the strategic goals and tactical focus of an organization. We applied methods described below in creating these Guidelines, provided in Appendix F. This tool supports performance evaluation of individuals and teams engaged in the following types of tasks:

- Vignette: Advanced Metering Infrastructure Attacks (Appendix F.1)
- Vignette: Data Leakage and Related Attacks (Appendix F.2)
- Vignette: Encryption and Phishing Incidents (Appendix F.3)
- Vignette: Incident Response Process and Log Management (Appendix F.4)

4.1 Method

Phase I and Phase II SMEs mapped tasks and responsibilities for each job role to critical incidents, called vignettes. Traditionally, in order to meet EEOC and ANSI requirements of psychometrically validated job profiles, critical tasks are mapped to a single job role. By mapping the tasks to vignettes, it is possible to understand which tasks overlap between job roles and to facilitate fair evaluation of individuals who are working as part of a team.

4.2 Outcome

The team performance guidelines created in Phase III can be used to evaluate individual/team performance and address strategic planning for organizations, including identification of training needs and recruitment of individuals who are a good fit for an organization’s needs. The Guidelines may be applied to develop performance reviews or to produce individual development programs for existing staff. The Guidelines may assist in specifying learning objectives for a training or education program. In addition, they may be easily incorporated into most human capital software to facilitate development of job descriptions that comply with guidelines established by the SHRM.

The SPSP Phase III effort provides an innovation in workforce development that identifies needs and gaps in the coordination of individual and team performance to reveal organizational level requirements.

The specific development of Team Performance Guidelines represents an important contribution of the SPSP project: it is an innovation for the workforce development field. The EEOC and ANSI require SMEs to map critical tasks to a job role to produce a validated job profile. Traditionally, in order to meet EEOC and ANSI requirements of psychometrically validated job profiles, critical tasks are mapped to a single job role. Phase I and Phase II SMEs completed this mapping in accordance with the established methods of the EEOC and ANSI. Clearly, organizational capability is the synergy of individual capabilities. While some critical tasks can be carried out by individuals, some tasks require the coordination and collaboration of a group of individuals working together on the same issue. This mapping can illustrate potential human resource gaps on the organizational level.

To illustrate how the Guideline is used, in Table 4.1 we provide an excerpt of the Team Performance Guidelines from Appendix F.4 for the Incident Response Process and Log Management vignette. This detailed list of goals, responsibilities, and tasks was drawn from the JPMs for the four job roles developed during Phase I. Items that are shaded gray indicate overlapping or team tasks. To use the Guidelines, key individuals—including management and HR professionals—review the vignettes and identify the unique set of priorities for their organization. With the vignettes identified, human resource professionals survey the current employees using the team performance guidelines to identify capabilities among existing personnel. This process will highlight gaps in the capability of individuals to address the identified organizational priorities. Knowledge of the gaps informs strategic decisions. For example, current staff could be trained to address the gaps, or the identified gaps can be used to focus recruitment and hiring processes. Furthermore, once overlapping tasks have been identified, the tasks unique to each job role are highlighted. Consequently, this mapping facilitates the fair evaluation of individuals who are working as part of a team.

Table 4.1. Excerpt from Incident Response Process and Log Management Vignette

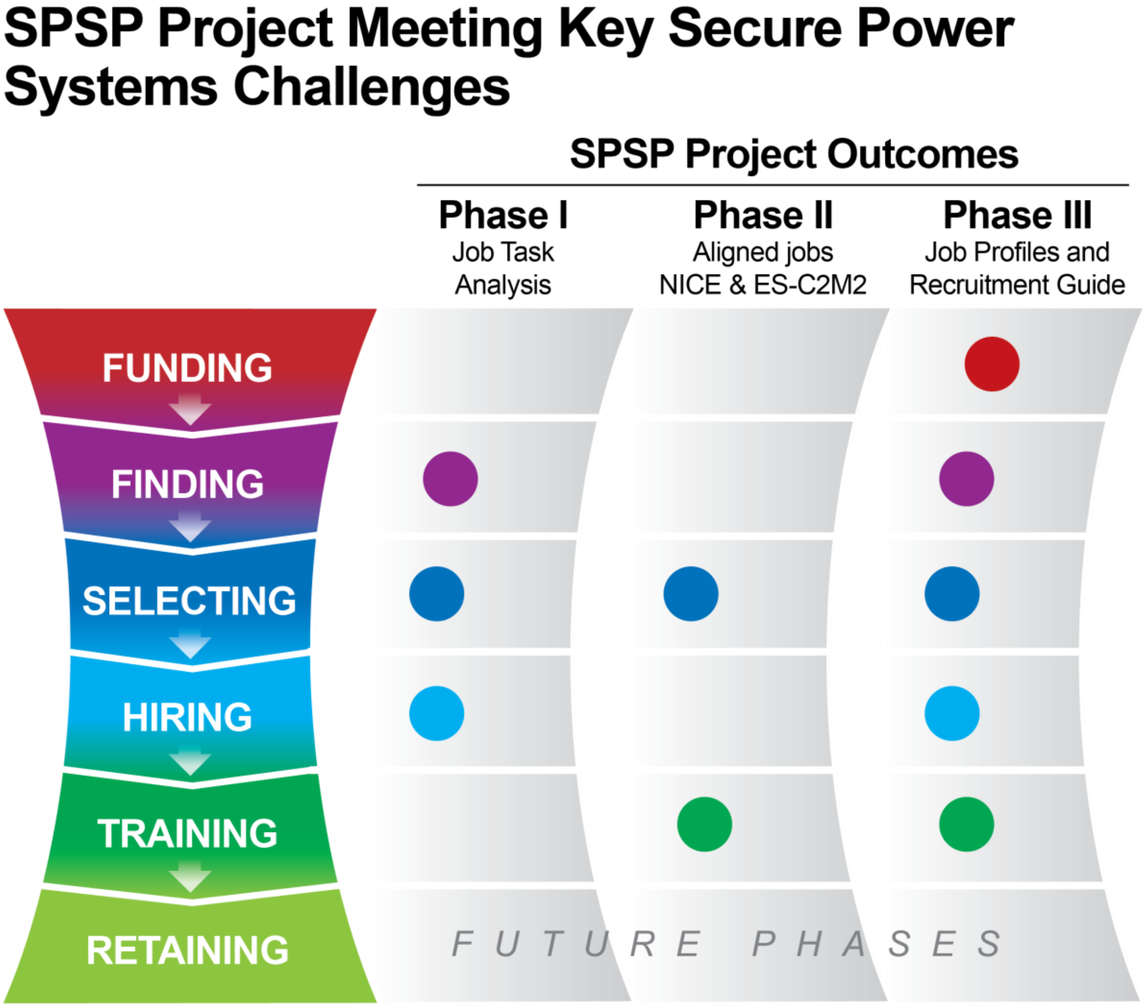
Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
GOAL: Install security monitoring solutions			
RESPONSIBILITY: Make sure adequate budget has been apportioned for monitoring solution			
Access an up-to-date power systems inventory and asset list	Alert end users of potential risks and vulnerabilities that they may be able to mitigate	Alert operators to events occurring so that they may increase system logging or retain logs, where normally such logs might be simply lost due to system storage constraints	Alert operators to events occurring so that they may increase system logging or retain logs, where normally such logs might be simply lost due to system storage constraints
Develop a prioritized list of critical resources	Develop a prioritized list of critical resources		Develop a prioritized list of critical resources
		Review “healthy” log collection metrics to understand baseline from which to measure normal performance	Review “healthy” log collection metrics to understand baseline from which to measure normal performance

We envision that key individuals, including management and HR professionals, would use the team performance guidelines as follows. First, they should review the vignettes and identify which of the vignette(s) represent the unique set of priorities for their organization. With the vignettes identified, HR professionals use the information provided in the Guideline to conduct a survey of the current employees to confirm whether their current staff has the knowledge, skill, or ability to complete the required tasks. This will identify existing capabilities among current personnel. Knowledge of the gaps will inform strategic decisions such as hiring, professional training, and workforce development. For example, current staff could be trained to address the gaps. Alternatively, the identified gaps can be used to focus recruitment and hiring processes. Thus, selection of specific vignettes and/or responsibilities for an open position may be made by a hiring manager based on the strategic focus and/or workforce competency gaps in their organization. A hiring manager can easily highlight areas of focus to include in their strategic or recruitment plan. The completed form may then be sent to an HR professional or recruiter for development of existing recruitment and selection programs, enabling application of current organizational practices to the competency requirements necessary for successful job performance by SPSPs.

5.0 Implications

5.1 Implications for Electric Power Sector Entities

Each phase of the SPSP effort has focused on specific deliverables. In addition, there has been a continuous discussion about the broader workforce development challenges faced by the power sector and the members of the panel. Over time, a number of themes emerged in the conversations on workforce development, and in Phase III the project team defined these life cycle themes: Funding, Finding, Selecting, Hiring, Training, and Retaining. These life cycle stages have been mapped across the three phases of the SPSP effort, as depicted in Figure 5.1.



	Phase I Job Task Analysis	Phase II Aligned jobs NICE & ES-C2M2	Phase III Job Profiles and Recruitment Guide
FUNDING			●
FINDING	●		●
SELECTING	●	●	●
HIRING	●		●
TRAINING		●	●
RETAINING	FUTURE PHASES		

Figure 5.1. Major Outcomes and Impacts of the SPSP Project

Organizations naturally move through these life cycle stages over time as the organization matures and develops programs to improve their overall workforce management capability. For example, an organization that is just starting to identify a need for cybersecurity professionals within their operating environments may be faced with funding challenges as they work to justify and prioritize the need for the SPSP positions. Once an organization gains approval for additional staff, they may face a very difficult challenge to find and select the best-fit candidate, often experiencing open unfilled positions for nine months or longer. Many panel members also conveyed challenges in hiring individuals whose salary requirements exceed the approved ranges for a position, or cases where the hiring manager has to decide whether to hire an individual who possesses some but not all of the hybrid skills required in the SPSP job positions. Most, if not all, individuals who are hired will need fully developed training programs in Cybersecurity, Operational Technology, Information Technology, or electric power system operations. When an organization has succeeded in developing an integrated, trained, and capable team, it will ultimately face retention issues as the workforce becomes marketable and mobile. As individuals exit the team or the responsibilities of the team grow, the organization will move throughout the workforce life cycle phases again. This natural movement through the life cycle challenges many organizations and requires continuous engagement by management, HR, recruiting, and Organizational Development personnel to foster success. When looking at assessment frameworks like the Cybersecurity Competency Maturity Model (C2M2), the organization needs to consider this natural movement and the impact it will have on the overall capability and maturity. Within the C2M2 Workforce Management Domain focus areas (Assign Cybersecurity Responsibilities, Control the Workforce Lifecycle, Develop Cybersecurity Workforce, Increase Cybersecurity Awareness, Manage Workforce Activities), there will likely be organization capability changes that could result in movement from one Maturity Indicator Level to another as events occur within the organization (staffing changes, budgetary changes, leadership changes, organization mergers, acquisitions, divestitures, restructuring, etc.).

The SPSP project deliverables, provided in reports from its various phases, include both tactical and strategic resources to assist organizations in dealing with these challenges.

Tactical resources:

- The Phase I report includes job titles and job tasks performed that can be integrated into job postings prepared by hiring organizations.
- The Phase I report includes an analysis of relevant certifications to specific job roles that can be used to assist hiring organizations in identifying qualified candidates for a position, can be used as job posting requirements, and can be utilized in shaping current employees' training development programs.
- The Phase I project identified a mix of SPSP roles involved in responding to cyber vignettes—over 40 unique roles were identified.
- The Phase II report mapped job tasks to responsibility areas and then further mapped these to existing frameworks, certifications, and educational programs. An organization can look at the responsibility areas and determine which framework aligns with the needs of their teams based on the tasks performed. Identifying the framework or development area that aligns with a team's specific needs allows the organization to quickly implement a necessary component of a framework or development approach. This provides for needed agility in addressing a specific area rather than taking the time to implement an entire program that may not align with a workgroup's need. This focus on workgroup capabilities is essential in assessing how well a team's diverse skill sets have integrated to provide the necessary coverage for SPSP responsibility areas.
- The Phase III effort provided quick guides for recruiting and development that will assist organizations in educating stakeholders on the workforce challenges within the SPSP area, as well as provide resources for finding and training individuals for SPSP positions.

Strategic resources:

- The Phase I report identified job tasks required for the Phase II responsibility area and framework mappings. This enables an organization to look more strategically at personnel who perform the various required tasks and responsibilities. Using the developed team mapping, the organization can assess and identify areas in which they are currently strong, but where they may struggle if personnel events occur. This information can be used in employee succession and continuity planning.
- The Phase II report mapped responsibility areas across a number of frameworks that an organization can use to identify the areas of greatest opportunity. Based on the assessment outcomes, organizations can develop an integrated capital and expense funding approach that addresses the areas of greatest risk. These mappings can also assist an organization in selecting a framework or development tool that best aligns with their areas of maturity and greatest need.
- The Phase III effort has further defined role-based behavioral assessment criteria that will be essential in the development of tools used in the selection of personnel for a specific role.

The SPSP project outcomes inform and support industry stakeholders as well as industry professionals. The results of all three SPSP Project phases can be consulted by the industry to assist in development of existing frameworks, credentialing, and educational programs to address current gaps in each of these areas. This can be seen in the growing interest in training programs and credentialing programs that focus on blended training offerings that cover the various domains relevant for an SPSP. In addition, individuals considering entry to this field can examine the SPSP project reports to identify possible focus areas to further pursue based on their individual strengths and interests. In this way, the individual self-identifies areas of improvement/development to increase marketability, rather than the less-efficient alternative where an organization hires an individual strong in one domain and then attempts to train staff in the other areas. This promotes an integral organizational training approach that provides foundational knowledge, demonstration of ability, and use of role-specific training to develop a focused area of expertise.

5.2 Broader Impacts

The SPSP project was developed to address a pervasive skills gap constraining effective response to the growing threat posed by cybersecurity vulnerabilities in critical infrastructure. Just a week prior to submission of the project proposal, a call to action was issued to address the mounting workforce crisis (see the insert, "Developing Ground Truth Expertise"). A lack of experienced talent presents an increasing risk to critical infrastructure industries dependent upon technical human capital as cited in reports of the "widening skills gap" threatening our nation (Brown and Barry 2008; Cappelli 2012; Hein 2013; TEK Systems 2012). Traditional methods of competency modeling that require months or years to produce high-level descriptions of job requirements are ill-suited to meet the constantly shifting demands and dynamic nature of the cybersecurity threat (Tobey 2011a, 2011d). Consequently, researchers are increasingly recognizing the need to adapt methods of modeling and measuring the gaps that exist in workforce readiness across professions (Campion et al. 2011; Clark 2013). The SPSP project methods and findings have influenced a number of programs seeking to enhance the cybersecurity workforce and to improve the tools available to workforce planners, assessment developers, instructional designers, and personnel credentialing programs.

Developing Ground Truth Expertise:
A holistic approach to workforce development

> *The Office of Personnel Management and those involved with the National Initiative for Cybersecurity Education say a shortage of talent and resource constraints are affecting agencies' cybersecurity workforce… We want to do something that reflects a workforce that is trained and qualified with actual capabilities and competencies and not just a rote exam.* – John Mills, OSD/NII special assistant for the National Cybersecurity Initiative (August 16, 2010)

The U.S. Department of Energy responded to this call for action to secure and protect critical infrastructure by establishing the Secure Power Systems Professional project in response to a proposal (Tobey et al. 2010, p. 5) that outlined a holistic approach to workforce development that continuously adapts to the latest tactics, techniques and protocols—the ground truth expertise that determines competence. A Ground Truth Expertise Development cycle (Assante and Tobey 2011) was proposed to address four gaps in existing secure power systems workforce development programs:

- Competency measurement gap (What competencies do we need to test for?)
- Assessment gap (How should we conduct tests so they are holistic and accurate, differentiating between simple understanding of concepts and skilled performance of actions?)
- Training gap (How do we prepare professionals for the tests and the real world?)
- Certification gap (What is the best framework for security certifications that integrate both knowledge and skill while predicting constraints of innate abilities on performance?)

In this section, we briefly review the impact that the SPSP project is having in addressing gaps in each of these areas. Throughout the development of the project, the innovative methods and detailed findings have informed workforce plans for the entire federal workforce; guided re-engineering of military schoolhouse programs intended to accelerate the proficiency of cyber operations and defense; influenced the design of serious games and simulations that seek to engage talented youth in the science, technology, engineering, and math professions; and reformulated objectives for credentialing personnel across many disciplines.

The SPSP project broadly impacts workforce development programs in the many professions experiencing a severe skills gap through its innovation of a holistic approach to the expertise development life cycle.

5.2.1 Competency Measurement Gap

In 2011, the second annual workshop for the NICE was held at the National Institute of Standards and Technology in Gaithersburg, Maryland. The purpose of the event was raising awareness among the American public about the growing cybersecurity risk, broadening the skilled workforce capable of securing and protecting the nation's critical infrastructure, and developing and maintaining the United States' premier position in the cybersecurity profession. Consistent with the workshop theme of "Shaping the Future of Cybersecurity Education," the SPSP research team made two presentations based on early findings from Phase I of the project and the findings from development of two other JPMs for operational security testing and advanced threat response.

The first presentation (Tobey 2011b) discussed the potential for using the JPMs to determine alignment between the newly introduced NICE National Cybersecurity Workforce Framework and the collection of training and certification programs from the newly formed Cybersecurity Credentialing Collaborative organization. This was the first time any organization had presented a method for determining how the varying credentials indicated foundational, specialist (differentiating), or related (team responsibility) expertise that aligned with the functional cybersecurity roles and specialty areas being proposed by NICE as a standard for federal workforce planning. The presentation showed how the JPM produced in Phase I could specify the correspondence of credentialing programs with the NICE information assurance framework by comparing certification domains with detailed the job performance competencies underlying NICE functional job roles.

The second presentation (Tobey 2011d) discussed how job performance modeling addressed the recent call for new methods for modeling and measuring gaps in workforce performance and development programs (Campion et al. 2011). The presentation described the innovations introduced by predictive job performance modeling and addressed deficiencies in competency modeling programs. The job-performance-model process was able to construct a comprehensive, predictive model of job performance that enabled translation of competencies into specific workforce development programs based on targeted development of knowledge, skill, or ability. This presentation also showed how to construct formative assessments based on a job model that indicates future potential of workforce capability, which could replace or augment existing summative assessments of past experience used by existing credentialing programs. Both of these presentations were well received by the attendees at the workshop. Accordingly, applying the JPM developed in Phase I to determine alignment across workforce programs became a core focus of Phase II.

Similarly, the application of JPMs to assessment-driven competency development established the foundation for broader impact of the SPSP project on workforce development programs offed by military schoolhouses, colleges, and universities around the country (discussed further in Sections 5.2.2 and 5.2.3 below). In addition, development of these JPM-based training and performance management programs is consistent with the Ground Truth Expertise Development model proposed to guide the long-term development of the SPSP project (Assante and Tobey 2011; Tobey et al. 2010). This means the SPSP project established a strong foundation for development of future credentialing programs, specifically for energy infrastructure applications as discussed in Section 5.2.4 below.

5.2.2 Assessment Gap

By discretely analyzing the relative strengths and weaknesses of an individual’s (or team’s) competence, a competency profile assessment can be generated that would indicate where interventions are needed to improve performance. Competency profile assessments are holistic measures of competence. They differentiate between simple understanding of concepts and skilled performance of actions. Furthermore, they offer formative guidance to the type (instruction, practice, or scenario simulation) and focus (foundational or differentiating tasks) of training needed to increase competence and job performance.

A presentation of the competency profile assessment approach was made at the NICE workshop. This led to a request to present the method and findings from the SPSP project at a workshops hosted by the National Defense University (Tobey 2011c). This approach to assessment and assessment-driven learning is currently being adopted by Defense Information Systems Agency. They plan to use competency profile assessments to both determine aptitude and to accelerate development of cybersecurity professionals by personalizing training programs. Despite the focus on secure power systems, the SPSP Job Profiles and Individual and Team Performance Guidelines could provide a strong foundation for this Department of Defense initiative by providing job profiles and behavioral interview guidelines for security operations, incident analysts, and intrusion responders. The mappings done in Phase II of the SPSP project could also assist in aligning the Department of Defense competency profiles with the NICE Framework and training and certification courses. In the next section, we will describe how a similar leveraging of the SPSP JPM is improving training and competition-based learning in community colleges and universities around the country.

5.2.3 Training Gap

Key training challenges concern questions like, “How can we better prepare professionals for the continually changing and increasingly sophisticated cyber threats? How can we shorten the time required to become an expert or master in the field so that the skills gap can be reduced or closed?”

Through the impact that the SPSP project has had on related workforce development programs, this training gap has begun to be addressed. For example, the National Cyber League has recently adopted the job performance modeling technique and virtual mapping technology that supported the SPSP project in producing a mapping of their cyber competitions to certifications, training courses, lab exercises, and competency models, such as the NICE Framework. A similar process is beginning with the Collegiate Cybersecurity Defense Competition. These recent adoptions of SPSP project resources have shown that JPMs may provide the foundation for establishing balance in game-based learning necessary to foster student engagement in the learning activities and the profession overall (Tobey et al. 2014).

5.2.4 Certification Gap

The formative approach to assessment described in Section 5.2.2 differs significantly from traditional credentialing exams that lack developmental feedback. Numerous presentations at the National Defense University workshop reported a need to augment credentialing exams with new techniques that could identify an individual's potential to develop the competencies required to succeed in the cybersecurity profession. A similar need exists in the secure power systems market.

Accordingly, a competency profile assessment based on the SPSP JPM was presented at a seminar simulcast by the University of Illinois (Assante and Tobey 2012). This model could create broad impact in power systems industries in future phases of the SPSP project (see Figure 5.2). Future phases of the SPSP project, or other organizations interested in providing assessment tools, could apply the SPSP Job Profiles, Behavioral Interview Guidelines, and Individual and Team Performance Guidelines to produce competency profile assessments. This is best achieved using the cyclical process of Design, Pilot, and Deploy that was followed during the first three phases of the SPSP project. During the design phase, a self-assessment of self-efficacy could be used in lieu of more time-intensive situational judgment and performance-based tests to assess relative competence. The array of relative task efficacies across the fundamental and differentiating tasks identified in the SPSP JPM could provide a very quick appraisal of workforce readiness on an individual, team, organizational, or even industry-wide basis. Finally, this assessment model could then be piloted in a few organizations before being deployed as a virtual or downloadable assessment center to support workforce planning, training, and program evaluation.

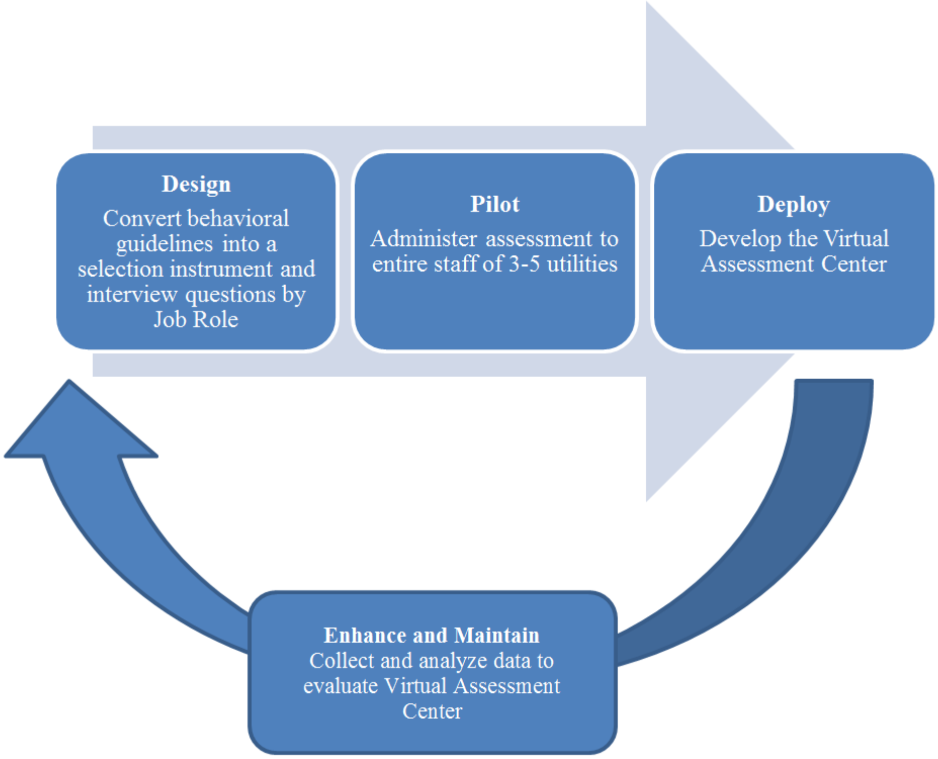

Design
Convert behavioral guidelines into a selection instrument and interview questions by Job Role
Pilot
Administer assessment to entire staff of 3-5 utilities
Deploy
Develop the Virtual Assessment Center
Enhance and Maintain
Collect and analyze data to evaluate Virtual Assessment Center

Figure 5.2. Application of a Competency Profile Assessment Model for Secure Power Systems Professionals

The SPSP project resources have also recently been used to address a related certification challenge—how to accredit education programs as being aligned with competency models, e.g., the NICE information assurance framework and the Centers for Academic Excellence program operated by the National Security Agency and the U.S. Department of Homeland Security. The analytical techniques used to develop and validate the SPSP JPM have informed the assessment of alignment of the NICE Framework list of knowledge, skills and abilities with the Centers for Academic Excellence list of knowledge units. Some members of the SPSP project team also assisted in the C2M2 development for the Workforce Management domain of the model. Thus, the SPSP project has the potential to affect not only individual, team, and organizational assessment, but it can guide future accreditation programs within the energy sector and across multiple industries. The SPSP project has been presented to the electric power sector through a variety of channels, including NERC Critical Infrastructure Protection Committee meetings, DOE Google Hangout information sessions, SANS ICS industry Summits both domestic and international (Spain), Industrial Control System Information Sharing and Analysis Center webinars, and Industrial Control Systems Joint Working Group conferences as well as a number of regional industry conferences.

6.0 Conclusions and Next Steps

A key component to the success of the SPSP project efforts is in the socialization and adoption of these findings. Efforts are underway to socialize these findings through ICS, the electric power sector, and HR industry-specific conferences and distribution lists. The findings are detailed in Section 5 of this report and a number of tactical and strategic recommendations have been outlined within Section 4 of this report. Given the findings and recommendations of the three phases of the SPSP project, it is incumbent on the organizational leaders and the industry at large to assimilate and understand these results and to develop methods to implement corrective action. These recommendations and findings should be evaluated for the variety of roles involved in SPSP tasks; a diverse team of individuals should be assembled to use the SPSP project results to improve the design of security, security monitoring processes, and the response to security incidents. Leveraging the recommendations in Section 4 and the approaches identified throughout the first three phases of the SPSP effort, we present the following call to action:

1. **Gain Awareness.** Asset owners and operators, you have the responsibility to provide a safe and reliable operating environment. Assess your organization's ability to detect and defend the ICS assets that are critical to your mission.
2. **Assess Workforce.** Evaluate SPSP team capabilities, maturity, competence diversity, current staffing levels, future staffing levels, and funding plans.
3. **Educate Leadership.** Provide the assessment results to leadership and ask for help to address those areas of greatest risk.
4. **Initiate Programmatic Change.** Develop and implement programs supported by leadership to fund needed capability development, recruiting, training, and retaining of essential personnel.
5. **Give Back.** Participate in industry efforts to develop additional tools, lessons learned, and best practice approaches to the challenges we all share in the operation of our critical infrastructure.

The electric power sector has long discussed the critical workforce challenges, and the SPSP initiative has many more steps before the development of necessary tools and approaches is complete. However, much has been done, and stakeholders now have the knowledge, insights, and tools provided by the SPSP project to achieve success in meeting these challenges.

We envision four ways in which the job profiles can be used in future phases of the SPSP project. These future phases will ultimately develop the necessary components for industry to perform appropriate position-selection decisions with a recommended training development plan that uses credentials and reassessment criteria to shape the individual and team capabilities.

- ***Convert the job profile, including the behavioral interview guidelines, into a validated selection instrument and interview questions.*** Phases I and II employed an expert panel to identify the critical elements of a job role. This process generated a validated list of skill areas and responsibilities necessary for a selection tool to be EEOC compliant. Therefore, any HR or testing entity can use the job profile to develop a selection tool that is EEOC compliant.
- ***Convert the behavioral interview guidelines into a self-efficacy instrument.*** SPSP industry experts have requested that a future project be created to convert the behavioral interview guidelines into a self-efficacy instrument that can be used by HR professionals, recruiters, and SPSP professionals to

inform professional development. The next step includes engaging power-systems HR and legal professionals to create a candidate-evaluation scoring tool that can be validated and certified.

- ***Create a Query Engine and Customized Reporting*****.** There are requests that future phases of the SPSP Project create a query engine of the collected data to provide customized reports that may be used by recruiting and HR professionals to guide talent development and to address workforce gaps.
- ***Develop a Learning Platform.*** The findings and recommendations of SPSP Phases I–III can be used to design and develop a learning platform that will build capabilities among current SPSPs. This can be accomplished by developing a simulation-based learning platform that uses pre-assessments to identify skill gaps, provides effective practice through learning modules that address the gaps, and applies appropriate assessments to demonstrate learning.

7.0 References

43 FR 38290–38315. 1978. “Equal Employment Opportunity Commission, Civil Service Commission, Department of Labor and Department of Justice; Adoption by four agencies of Uniform Guidelines on Employee Selection Procedures.” U.S. Department of Energy, *Federal Register*.

Adler, L. 2013. *The Essential Guide for Hiring & Getting Hired*. Workbench Media.

Arvey, RD. 1979. “Unfair discrimination in the employment interview: Legal and psychological aspects.” *Psychological Bulletin*, 86(4):736–765.

Assante, MJ and DH Tobey. 2011. “Enhancing the cybersecurity workforce.” *IEEE IT Professional*, 13:12–15.

Assante, MJ and DH Tobey. 2012. *Ground truth competency assessment for smart grid cyber security*. Seminar presentation presented at the Trustworthy Cyber Infrastructure for the Power Grid Seminar Series, University of Illinois, Champaign-Urbana, IL. Retrieved from http://tcipg.org/news/TCIPG-Seminar-2012-May-4-Assante

Benner, PE. 2004. “Using the Dreyfus model of skill acquisition to describe and interpret skill acquisition and clinical judgment in nursing practice and education.” *Bulletin of Science, Technology and Society*, 24:188–199.

Brown, J and L Barry. 2008. Retiring workforce, widening skills gap, exodus of “critical talent” threaten companies: Deloitte survey. Press release. Retrieved from http://www.deloitte.com/view/en_au/au/03a55139fb1fb110VgnVCM100000ba42f00aRCRD.htm

Campion, MA, AA Fink, BJ Ruggenberg, L Carr, GM Phillips, and RB Odman. 2011. “Doing competencies well: Best practices in competency modeling.” *Personnel Psychology*, 64:225–262.

Cappelli, P. 2012. “The skills gap myth: Why companies can’t find good people.” *Time Business*. Retrieved July 27, 2012, from http://business.time.com/2012/06/04/the-skills-gap-myth-why-companies-cant-find-good-people/?t-find-good-people/

Clark, H. 2013. “A comprehensive framework for measuring skills gaps and determining work readiness.” *Employment Relations Today*, 40(3):1–11.

Dreyfus, SE and HL Dreyfus. 1980. *A five-stage model of the mental activities involved in directed skill acquisition*. Berkeley, CA: Air Force Office of Scientific Research.

Hein, R. 2013. “How to Close the IT Talent Gap.” *CIO Magazine*. Retrieved May 21, 2014, from http://www.cio.com/article/735464/How_to_Close_the_IT_Talent_Gap

Kesselman, GA and FE Lopez. 1979. “The impact of job analysis on employment test validation for minority and nonminority accounting personnel.” *Personnel Psychology*, 32(1):91–108.

Lado, AA and MC Wilson. 1994. “Human resource systems and sustained competitive advantage: A competency-based perspective.” *Academy of Management Review*, 19:699–727.

O'Neil, LR, MJ Assante, and DH Tobey. 2012. *Smart Grid Cybersecurity: Job Performance Model Report* (Technical Report No. PNNL-21639). Alexandria, VA: National Technical Information Service.

O'Neil, LR, MJ Assante, DH Tobey, TJ Conway, TJ Vanderhorst, J Januszewski, R Leo, and K Perman. 2013. *Developing secure power systems professional competence: Alignment and gaps in workforce development programs* (Technical Report No. PNNL-22641). Alexandria, VA: National Technical Information Service.

Pursell, ED, MA Campion, and SR Gaylord. 1980. "Structured interviewing: Avoiding selection problems." *Personnel Journal*, 59(11):907–912.

TEK Systems. 2012, January 24. *TEKsystems Survey Reveals IT Job Seekers Crave a More Personal Touch in the Job Search Process*, http://www.teksystems.com/resources/pressroom/2012/teksystems-survey-reveals-it-job-seekers-crave-more-personal-touch

Tobey, DH and P Pusey. 2014, July 22. *Cyber defense competition design: A vignette-based method to improve cybersecurity talent management*. Conference presentation presented at the Community College Cyber Summit, Center for Systems Security and Information Assurance, Palos Hills, IL.

Tobey, DH, M Assante, S King, and K Ziegler. 2010. "Developing Ground Truth Expertise in Smart Grid Security Specialists." National Board of Information Security Examiners. August 24.

Tobey, DH, P Pusey, and D Burley. 2014. "Engaging learners in cybersecurity careers: Lessons from the launch of the National Cyber League." *ACM InRoads*, *5*(1):53–56.

Tobey, DH, R Reiter-Palmon, and A Callens. 2012. *Predictive Performance Modeling: An innovative approach to defining critical competencies that distinguish levels of performance. OST Working Group Report.* Idaho Falls, ID: National Board of Information Security Examiners.

Tobey, DH. 2011a. *A competency model of advanced threat response. ATR Working Group Report NBISE-ATR-11-02*. Idaho Falls, ID: National Board of Information Security Examiners.

Tobey, DH. 2011b, September 21. *Cybersecurity certification: The way ahead*. Conference presentation presented at the Shaping the Future of Cybersecurity Education, 2nd Annual NICE Workshop, National Institute of Standards and Technology, Gaithersburg, MD.

Tobey, DH. 2011c, October 12. *What should personnel credentialing for the cyber workforce look like*. Conference presentation at Preparing the Pipeline, National Defense University, Fort Lesley J. McNair, D.C.

Tobey, DH. 2011d, October 31. *From Cybersecurity Competencies to a Job Performance Model*. Presented at the First Annual National Initiative for Cybersecurity Education Workshop, National Institute of Standards and Technology, Gaithersburg, MD. Retrieved from https://www.academia.edu/1702967/NICE_-_From_cybersecurity_competencies_to_a_job_performance_model

Appendix A

Phase III Secure Power Systems Professional Subject Matter Expert Panel Roster

Appendix A

Phase III Secure Power Systems Professional Subject Matter Expert Panel Roster

Subject Matter Expert	Affiliation	Sector
Officer		
Conway, Tim (Chair)	SANS	Industry
Panel Members		
Aber, Lee	Opower	Industry
Agrawal, Sandeep	Neilsoft Limited	Service
Assante, Michael	NexDefense	Vendor
Damm, Benjamin	Silver Springs Networks	Vendor
Greipp, Jeff	University of Phoenix	Research
Januszewski, Joseph	Consultant	Research
Keller, Steven	Southwest Power Pool Electric Energy Network	Industry
Kersey, Karl	Schneider Electric	Vendor
Leo, Ross	Consultant	Vendor
Parker, Steven	Energy Sec	Industry
Perman, Karl	Consultant	Service
Sample, James	PG&E	Industry
Sandler, Josh	Duke Energy	Industry
Sawall, Chris	Ameren	Industry
Tydings, Kevin	Leidos	Service
Whitney, Will	Garland Power & Light	Industry
Yardley, Chris	University Of Illinois	Research

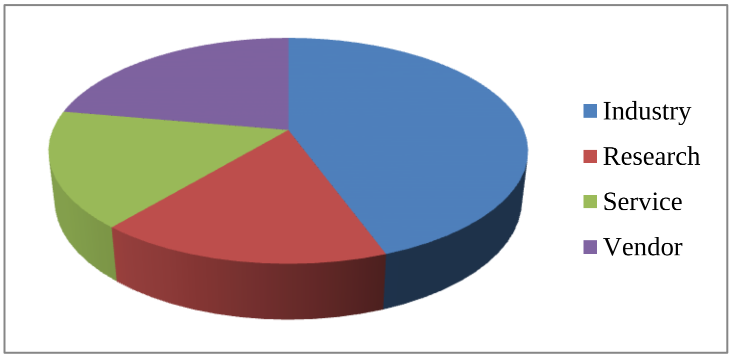


Figure A.1. Breakdown of Panel by Sector

Appendix B

Demographic Analysis

Appendix B

Demographic Analysis

This appendix has two sections. The first section provides the breakdown of demographic information gathered during each phase of the Secure Power Systems Professional (SPSP) project. The second section provides an analysis based on respondents' self-reported job functions and levels of expertise. It is important to acknowledge that in accordance with recommended practice for developing models of expert performance (Campbell et al. 1990; Patton 1990), a purposive sampling method was used in all project phases to recruit survey respondents appropriate to the job domain and content objectives. A complete analysis of respondent demographics for the first two phases can be found in the respective project phase reports (O'Neil et al. 2012, 2013).

B.1 Demographics from Each Phase of the SPSP Project

B.1.1 Phase I

Phase I was intended to elicit the competencies required to perform cybersecurity tasks within power systems affected by the deployment of smart grid components. Phase I work required expertise in information technology (IT), power systems, and cybersecurity to define four job roles and their corresponding responsibilities and tasks. Prior studies supporting development of performance models (e.g., Campbell et al. 1990) have emphasized the importance of including a balance between job incumbents and peer raters of job performance during model verification. Accordingly, while input was sought primarily from cybersecurity professionals in the energy industry, the respondent pool also included individuals in the energy sector who perform related technical roles (e.g., IT and power system professionals) as well as vendors, consultants, and government agencies involved in securing power systems. Following the guidelines of other recent studies of competency of professional expertise (Davis et al. 2008; Mylopoulos et al. 2012), a group of professionals with suitable expertise was obtained using a purposive, snowball sampling technique to support both Phase I and subsequent Phase II analyses. The Phase I survey collected more detailed demographic information about the survey respondents than the other two Phases.

In total, 289 responses to the Job Analysis Questionnaire (O'Neil et al. 2012) were received from individuals performing IT, cybersecurity, and power systems functions. Cybersecurity professionals in the energy industry often have a background in either IT or power systems prior to identifying with or being assigned to a cybersecurity-specific job function. Accordingly, some respondents indicated they performed multiple job functions. Because the objective of this phase was to identify discrete cybersecurity job tasks in the energy sector, the cybersecurity job category was assigned only to respondents who indicated their sole job function was cybersecurity.

The resulting job function distribution for Phase I respondents is shown in Table B.1. The respondents comprised 91 individuals performing IT job functions, 140 cybersecurity professionals, and 58 power systems professionals. As shown in the table, the intended targeting of dedicated cybersecurity professionals was achieved, ensuring that the survey response represented a focus on cybersecurity job functions while balancing this input with feedback from supporting job functions.

Table B.1. Categorization of Phase I Survey Respondent Job Functions

Category	Number	%
IT	91	32%
Cybersecurity	140	48%
Power Systems	58	20%
Total	**289**	**100%**

In sum, the demographic analysis above supports a conclusion that the respondent sample captures a broad range of the cybersecurity job function. The primary targeting of job incumbents performing cybersecurity staff duties was achieved. Moreover, the robustness of the job performance model (JPM) was enhanced by including the input from all related job functions.

B.1.2 Phase II

The goal of Phase II was to apply the JPM developed in Phase I to determine the relative emphasis, alignment, and gaps in workforce programs supporting the development of a Secure Power Systems Professional workforce. Accordingly, an industry survey was conducted to verify the Subject Matter Expert (SME) panel assessment of workforce programs for securing power systems developed by the National Initiative for Cybersecurity Education, the Electricity Sector Cybersecurity Competency Maturity Model (ES-C2M2), and highly relevant certification and education programs available from various institutions. The emphasis on applying cybersecurity job performance within a secure power systems framework required that Phase II include a more balanced representation of power systems and cybersecurity perspectives, with related input from the supporting IT job function. This section will report the composition of Phase II public survey respondents selected to assess the adequacy of the workforce development program gap-and-overlap analysis produced during this phase.

A total of 127 people accessed the survey home page and completed the demographic section of the survey. Phase II respondents were asked to select from the same set of jobs as in the Phase I survey. These jobs are classified in Table B.2 into the three job functions: IT, Cybersecurity, and Power Systems. The intended targeting of a balanced group of power systems and cybersecurity professionals was achieved, with the focal group representing 87% of all respondents. A limited number of IT workers provided peer review.

Table B.2. Categorization of Phase II Survey Respondent Job Functions

Category	Number	%
IT	17	13%
Cybersecurity	53	42%
Power Systems	57	45%
Total	**127**	**100%**

As this phase was focused on application of the JPM to improving workforce development, it was important to gain a greater understanding of the perspective of power systems professionals and cybersecurity management. As mentioned above, the sample was nearly evenly split between individuals performing cybersecurity and power systems job functions.

B.1.3 Phase III

The goal of Phase III was to apply the JPM developed in Phase I and the lessons learned from the gap-and-overlap analysis in Phase II to develop useful tools for human capital planning, recruitment, selection, and performance evaluation, as well as staff development and retention. Accordingly, an industry survey was conducted to verify the value and relevance of components to be included in a draft of *How to Recruit Secure Power Systems Professionals – A Guide for Human Resources and Hiring Managers* (Dalton and O'Neil 2014; also available in Appendix G). This guide was developed in focus group sessions with a panel of SME. This section will report the composition of Phase III industry survey respondents selected to evaluate the components to be included in the published guide.

Secure power systems personnel are typically recruited from a pool of IT and cybersecurity workers, with some coming from power systems engineering. Consequently, an emphasis was placed on locating respondents who had experience in IT and Cybersecurity. The perspectives of individuals performing power system jobs or recruiting duties (i.e., human resources staff and hiring managers) were also sought for peer ratings of the guide components.

The Phase III industry survey was accessed by 61 individuals and 42 surveys were completed. In the demographic section of the survey, the respondents were asked to select one or more of the following job functions that they currently perform:

1. Human Resources
2. Hiring Manager
3. Information Technology/Network Engineer (IT)
4. Power Systems Engineer
5. Cybersecurity
6. Other (please explain).

To assess the presence of the target technical job function (Cybersecurity and IT) in the respondent pool, and to analyze differences in ratings between respondent groups, we further classified these job functions into three categories. This categorization was consistent with the findings from Phase I. The reclassification scheme is shown in Table B.3.

Table B.3. Reclassification of Phase III Survey Respondent Job Functions

Job Function	Category
Human Resources Hiring Manager	Human Resources Staff
Power Systems Engineer	Power Systems Staff
Information Technology/Network Engineer (IT) Cybersecurity	Technical Staff

For those respondents who reported performing only one job function (excluding the "other" group), a one-to-one mapping was used. Eight individuals who reported dual job functions were classified as shown in Table B.4. Finally, categorization of individuals performing "Other" job functions is shown in Table B.5.

Table B.4. Categorization of Dual Roles

Dual Roles	Category
Hiring Manager and Technical Staff (1)	Human Resources Staff
Power Systems and Technical Roles (1)	Power Systems Staff
IT and Cybersecurity (6)	Technical Staff

Table B.5. Reclassification of Individuals Performing "Other" Job Functions

Other	Category
Project Manager (1) Quality Representative (1)	Power Systems Staff
Software Quality Management (1) Consultant(1)	Technical Staff

Table B.6 shows the respondents broken down by reclassified categories. This detailed analysis of job functions shows, as intended, that technical staff represented nearly two-thirds (62%) of the responses.

Table B.6. Categorization of Phase III Survey Respondent Job Functions

Category	Number	%
Human Resources Staff	7	17%
Power Systems Staff	9	21%
Technical Staff	26	62%
Total	**42**	**100%**

B.2 Analysis by Job Functions and Expertise Levels

Respondents of each phase were also asked to report their levels of expertise in cybersecurity and power systems. For ease of analysis and understanding, the expertise levels were reclassified according to Table B.7.

Table B.7. Mapping of Expertise Levels in Phases I and II to Phase III

Phases I and II	Reclassification in Phase III
Beginner: working knowledge of key aspects of practice Novice: minimal knowledge, no connection to practice	Beginner
Proficient: good working and background knowledge of the area Competent: depth of understanding of discipline and area of practice	Intermediate
Expert: authoritative knowledge of discipline and deep tacit understanding across area of practice	Expert

Table B.8 provides the breakdown of the respondents by level of expertise and domain.

Table B.8. Breakdown of Respondents by Level of Expertise

Phase	Level of Expertise	Cybersecurity	%	Power Systems	%
I	Beginner	43	16.86%	58	45.67%
	Intermediate	139	54.51%	58	45.67%
	Expert	73	28.63%	11	8.66%
	Total	**255**	**100.00%**	**127**	**100.00%**
II	Beginner	64	50.39%	115	44.57%
	Intermediate	55	43.31%	124	48.06%
	Expert	8	6.30%	19	7.36%
	Total	**127**	**100.00%**	**258**	**100.00%**
III	Beginner	7	16.67%	16	38.10%
	Intermediate	14	33.33%	18	42.86%
	Expert	21	50.00%	8	19.05%
	Total	**42**	**100.00%**	**42**	**100.00%**

Table B.8 shows that there was a similar distribution pattern of power system expertise for all three Phases of the SPSP project. As described in sections B.1 to B.3 above, this was the desired outcome of recruiting efforts prescribed by the research plan. Furthermore, the distribution of participants with cybersecurity expertise is also consistent with the research plan. Phase I required a greater proportion of experienced cybersecurity experts to elicit the competencies required to support the deployment of smart grid components. The focus of Phase II work applied cybersecurity job performance within a secure power systems framework and required representatives from all three levels of cybersecurity expertise. Finally, Phase III required an emphasis on individuals with a high degree of cybersecurity expertise to verify the relevance of the components to be included in the *Guide*. The purposive sampling strategy supported the recommended practice for developing models of expert performance for Phases I and II. Furthermore, the respondents' expertise supported the job domain and content objectives of Phase III outcomes.

B.3 References

Campbell, CH, P Ford, MG Rumsey, ED Pulakos, ED Borman, DB Felker, MV De Vera, and BJ Reigelhaupt. 1990. "Development of Multiple Job Performance Measures in a Representative Sample of Jobs." *Personnel Psychology*, 43:277-300.

Davis, R, E Turner, D Hicks, and M Tipson. 2008. "Developing an integrated career and competency framework for diabetes nursing." *Journal of Clinical Nursing*, 17:168-174.

Mylopoulos, M, L Lohfeld, GR Norman, G Dhaliwal, and KW Eva. 2012. "Renowned physicians' perceptions of expert diagnostic practice." *Academic Medicine*, 87(10):1413-1417.

O'Neil, LR, MJ Assante, and DH Tobey. 2012. *Smart Grid Cybersecurity: Job Performance Model Report* (Technical Report No. PNNL-21639). Alexandria, VA: National Technical Information Service. http://energy.gov/oe/downloads/smart-grid-cybersecurity-job-performance-model-report-and-phase-1-overview-august-2012.

O'Neil, LR, MJ Assante, DH Tobey, TJ Conway, TJ Vanderhorst, J Januszewski, R Leo, and K Perman. 2013. *Developing secure power systems professional competence: Alignment and gaps in workforce development programs* (Technical Report No. PNNL-22641). Alexandria, VA: National Technical Information Service. http://energy.gov/oe/downloads/developing-secure-power-systems-professional-competence-alignment-and-gaps-workforce.

Dalton, AC and LR O'Neil. 2014. *How to Recruit Secure Power Systems Professionals – A Guide for Human Resources and Hiring Managers.* PNNL-SA-103184, Pacific Northwest National Laboratory, Richland, WA. https://www.controlsystemsroadmap.net/ieRoadmap%20Documents/SPSPRecruitmentGuideFlyer.pdf.

Patton, MQ. 1990. *Qualitative evaluations and research methods, 2nd Edition*. Sage Publications, Newbury Park, CA.

Appendix C

Combined Analysis of Subject Matter Expert Panel and Industry Survey Responses

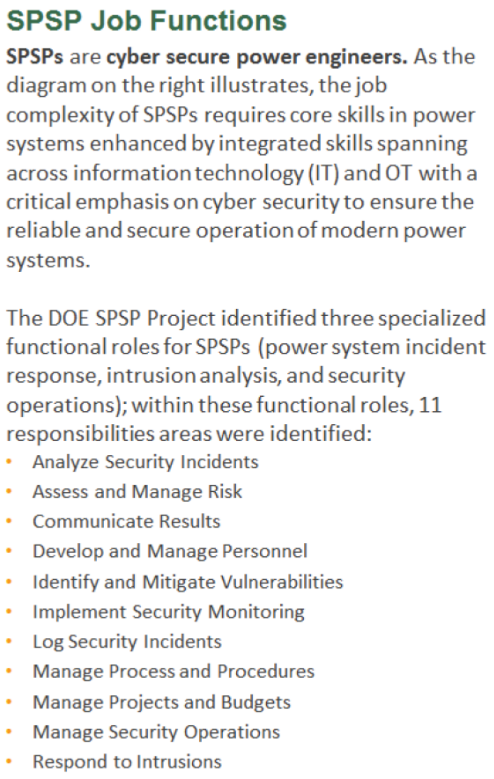
Appendix C

Combined Analysis of Subject Matter Expert Panel and Industry Survey Responses

This appendix reports the combined analysis of panel and industry survey responses. Each section represents the section of the *Guide* presented to the respondents and includes the following:

- an image of the section of the *Guide* content evaluated by the respondent
- the ranking of the content by industry and the panel
- the mean rating of the content by the panel on a scale from 1 (low value) to 5 (extreme value)
- the combined rating of the content by the number and percentage of industry respondents by job function category (recall that the criterion for retaining a content fragment in the *Guide* was that at least one-third of respondents supported the inclusion of the content fragment)

C.1 Job Functions



SPSP Job Functions

SPSPs are **cyber secure power engineers.** As the diagram on the right illustrates, the job complexity of SPSPs requires core skills in power systems enhanced by integrated skills spanning across information technology (IT) and OT with a critical emphasis on cyber security to ensure the reliable and secure operation of modern power systems.

The DOE SPSP Project identified three specialized functional roles for SPSPs (power system incident response, intrusion analysis, and security operations); within these functional roles, 11 responsibilities areas were identified:

- Analyze Security Incidents
- Assess and Manage Risk
- Communicate Results
- Develop and Manage Personnel
- Identify and Mitigate Vulnerabilities
- Implement Security Monitoring
- Log Security Incidents
- Manage Process and Procedures
- Manage Projects and Budgets
- Manage Security Operations
- Respond to Intrusions

Ranking out of 9 thematic areas of the *Guide*

Industry Ranking: 1
Panel Ranking: 1

Subject Matter Expert Panel Mean (n = 7)
[Ratings from 1 (low value) to 5 (extreme value)]

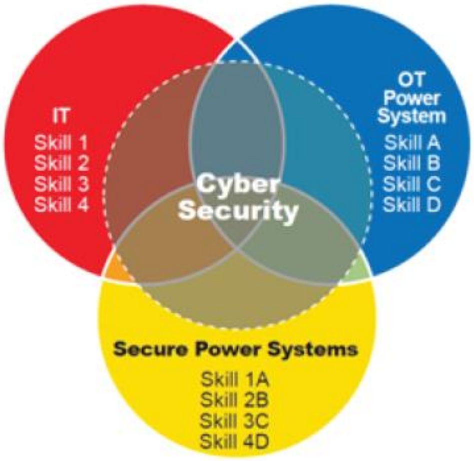
Panel Mean
4.5

Job Functions: Industry Survey Response on Value in Secure Power Systems Professional (SPSP) Recruiting

Total No. of Respondents by Job Category	No. of Respondents Saying Content is Valuable	*Percent* Saying Content is Valuable	Meets Inclusion Criterion?*
Human Resources (HR) (n = 7)	6	*86%*	Yes
Technical (n = 26)	26	*100%*	Yes
Power Staff (n = 9)	8	*89%*	Yes
Total across all industry respondents (n = 42)	**40**	***95%***	Yes

*Criterion: More than 1/3 of respondents consider the content valuable

C.2 Venn Diagram (Part of the Job Responsibilities Topical Theme)



Subject Matter Expert Panel Mean (n = 7)
[Ratings from 1 (low value) to 5 (extreme value)]

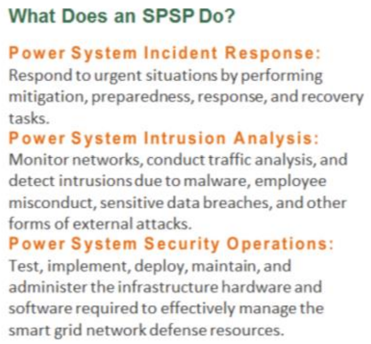
Panel Mean
2.67

Venn Diagram: Industry Survey Response on Value in SPSP Recruiting

Total No. of Respondents by Job Category	No. Respondents Saying Content is Valuable	*Percent* Saying Content is Valuable	Meets Inclusion Criterion?*
HR (n = 7)	3	*43%*	Yes
Technical (n = 26)	18	*69%*	Yes
Power Staff (n = 9)	7	*78%*	Yes
Total across all industry respondents (n = 42)	**28**	***67%***	Yes

*Criterion: More than 1/3 of respondents consider the content valuable

C.3 What Does an SPSP Do?



What Does an SPSP Do?

Power System Incident Response: Respond to urgent situations by performing mitigation, preparedness, response, and recovery tasks.

Power System Intrusion Analysis: Monitor networks, conduct traffic analysis, and detect intrusions due to malware, employee misconduct, sensitive data breaches, and other forms of external attacks.

Power System Security Operations: Test, implement, deploy, maintain, and administer the infrastructure hardware and software required to effectively manage the smart grid network defense resources.

Ranking out of 9 thematic areas of the *Guide*

Industry Ranking:	2
Panel Ranking:	2

Subject Matter Expert Panel Mean (n = 7)
[Ratings from 1 (low value) to 5 (extreme value)]

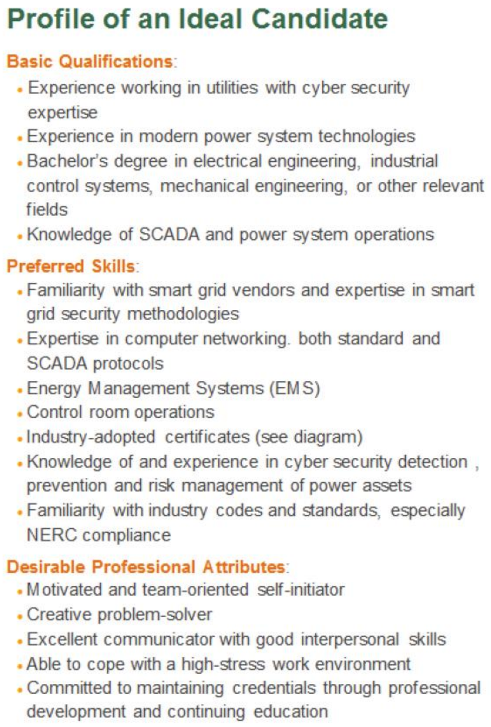
Panel Mean
4.0

What Does an SPSP Do? Industry Survey Response on Value in SPSP Recruiting

Total No. of Respondents by Job Category	No. Respondents Saying Content is Valuable	*Percent* Saying Content is Valuable	Meets Inclusion Criterion?*
HR (n = 7)	6	*86%*	Yes
Technical (n = 26)	26	*100%*	Yes
Power Staff (n = 9)	8	*89%*	Yes
Total across all industry respondents (n = 42)	**40**	***95%***	Yes

*Criterion: More than 1/3 of respondents consider the content valuable

C.4 Candidate Profile



Profile of an Ideal Candidate

Basic Qualifications:

- Experience working in utilities with cyber security expertise
- Experience in modern power system technologies
- Bachelor's degree in electrical engineering, industrial control systems, mechanical engineering, or other relevant fields
- Knowledge of SCADA and power system operations

Preferred Skills:

- Familiarity with smart grid vendors and expertise in smart grid security methodologies
- Expertise in computer networking. both standard and SCADA protocols
- Energy Management Systems (EMS)
- Control room operations
- Industry-adopted certificates (see diagram)
- Knowledge of and experience in cyber security detection , prevention and risk management of power assets
- Familiarity with industry codes and standards, especially NERC compliance

Desirable Professional Attributes:

- Motivated and team-oriented self-initiator
- Creative problem-solver
- Excellent communicator with good interpersonal skills
- Able to cope with a high-stress work environment
- Committed to maintaining credentials through professional development and continuing education

Ranking out of 9 thematic areas of the *Guide*

Industry Ranking:	3
Panel Ranking:	3

Subject Matter Expert Panel Mean (n = 7)
[Ratings from 1 (low value) to 5 (extreme value)]

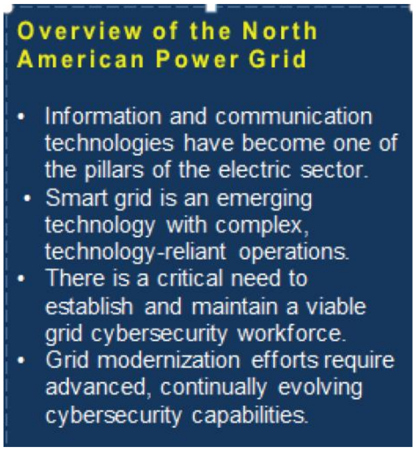
Panel Mean
4.33

Candidate Profile: Industry Survey Response on Value in SPSP Recruiting

Total No. of Respondents by Job Category	No. Respondents Saying Content is Valuable	*Percent* Saying Content is Valuable	Meets Inclusion Criterion?*
HR (n = 7)	6	*86%*	Yes
Technical (n = 26)	26	*100%*	Yes
Power Staff (n = 9)	8	*89%*	Yes
Total across all industry respondents (n = 42)	**40**	***95%***	Yes

*Criterion: More than 1/3 of respondents consider the content valuable

C.5 North American Power Grid Overview



Overview of the North American Power Grid

- Information and communication technologies have become one of the pillars of the electric sector.
- Smart grid is an emerging technology with complex, technology-reliant operations.
- There is a critical need to establish and maintain a viable grid cybersecurity workforce.
- Grid modernization efforts require advanced, continually evolving cybersecurity capabilities.

Ranking out of 9 thematic areas of the *Guide*

Industry Ranking:	4
Panel Ranking:	5

Subject Matter Expert Panel Mean (n = 7)
[Ratings from 1 (low value) to 5 (extreme value)]

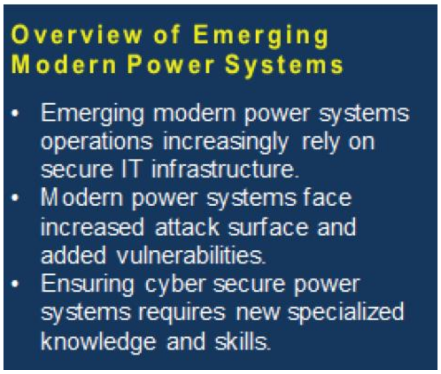
Panel Mean
2.67

North American Power Grid Overview: Industry Survey Response on Value in SPSP Recruiting

Total No. of Respondents by Job Category	No. Respondents Saying Content is Valuable	*Percent* Saying Content is Valuable	Meets Inclusion Criterion?*
HR (n = 7)	5	*71%*	Yes
Technical (n = 26)	19	*73%*	Yes
Power Staff (n = 9)	9	*100%*	Yes
Total across all industry respondents (n = 42)	**33**	***79%***	Yes

*Criterion: More than 1/3 of respondents consider the content valuable

C.6 Overview (Part of the North American Power Grid Topical Theme)



Overview of Emerging Modern Power Systems

- Emerging modern power systems operations increasingly rely on secure IT infrastructure.
- Modern power systems face increased attack surface and added vulnerabilities.
- Ensuring cyber secure power systems requires new specialized knowledge and skills.

Subject Matter Expert Panel Mean (n = 7)
[Ratings from 1 (low value) to 5 (extreme value)]

Panel Mean
3.0

Overview: Industry Survey Response on Value in SPSP Recruiting

Total No. of Respondents by Job Category	No. Respondents Saying Content is Valuable	*Percent* Saying Content is Valuable	Meets Inclusion Criterion?*
HR (n = 7)	4	*57%*	Yes
Technical (n = 26)	20	*77%*	Yes
Power Staff (n = 9)	8	*89%*	Yes
Total across all industry respondents (n = 42)	**32**	***76%***	Yes

*Criterion: More than 1/3 of respondents consider the content valuable

C.7 Voices (Part of the North American Power Grid Topical Theme)

Voices from Our Experts Panel

"I believe [the DOE study] 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, Technical Director, SANS ICS and SCADA programs

"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 Januszewski, Expert on Smart Grid Infrastructure and Security

Subject Matter Expert Panel Mean (n = 7)
[Ratings from 1 (low value) to 5 (extreme value)]

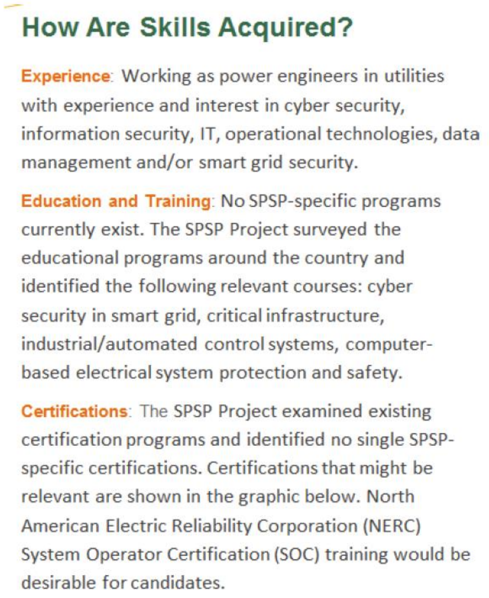
Panel Mean
2.33

Voices: Industry Survey Response on Value in SPSP Recruiting

Total No. of Respondents by Job Category	No. Respondents Saying Content is Valuable	*Percent* Saying Content is Valuable	Meets Inclusion Criterion?*
HR (n = 7)	3	*43%*	Yes
Technical (n = 26)	11	*42%*	Yes
Power Staff (n = 9)	4	*44%*	Yes
Total across all industry respondents (n = 42)	**18**	***43%***	Yes

*Criterion: More than 1/3 of respondents consider the content valuable

C.8 How are Skills Acquired?



How Are Skills Acquired?

Experience: Working as power engineers in utilities with experience and interest in cyber security, information security, IT, operational technologies, data management and/or smart grid security.

Education and Training: No SPSP-specific programs currently exist. The SPSP Project surveyed the educational programs around the country and identified the following relevant courses: cyber security in smart grid, critical infrastructure, industrial/automated control systems, computer-based electrical system protection and safety.

Certifications: The SPSP Project examined existing certification programs and identified no single SPSP-specific certifications. Certifications that might be relevant are shown in the graphic below. North American Electric Reliability Corporation (NERC) System Operator Certification (SOC) training would be desirable for candidates.

Ranking out of 9 thematic areas of the *Guide*

Industry Ranking:	5
Panel Ranking:	6

Subject Matter Expert Panel Mean (n = 7)
[Ratings from 1 (low value) to 5 (extreme value)]

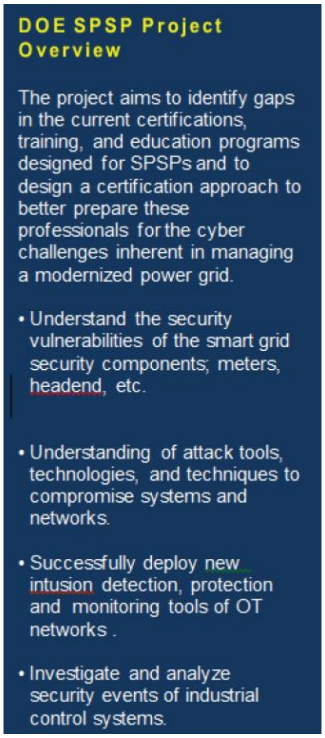
Panel Mean
3.17

How are Skills Acquired? Industry Survey Response on Value in SPSP Recruiting

Total No. of Respondents by Job Category	No. Respondents Saying Content is Valuable	*Percent* Saying Content is Valuable	Meets Inclusion Criterion?*
HR (n = 7)	5	*71%*	Yes
Technical (n = 26)	19	*73%*	Yes
Power Staff (n = 9)	5	*56%*	Yes
Total across all industry respondents (n = 42)	**29**	***69%***	Yes

*Criterion: More than 1/3 of respondents consider the content valuable

C.9 Project Overview



DOE SPSP Project Overview

The project aims to identify gaps in the current certifications, training, and education programs designed for SPSPs and to design a certification approach to better prepare these professionals for the cyber challenges inherent in managing a modernized power grid.

- Understand the security vulnerabilities of the smart grid security components; meters, headend, etc.
- Understanding of attack tools, technologies, and techniques to compromise systems and networks.
- Successfully deploy new intusion detection, protection and monitoring tools of OT networks .
- Investigate and analyze security events of industrial control systems.

Ranking out of 9 thematic areas of the *Guide*

Industry Ranking:	6
Panel Ranking:	9

Subject Matter Expert Panel Mean (n = 7)
[Ratings from 1 (low value) to 5 (extreme value)]

Panel Mean
2.33[1]

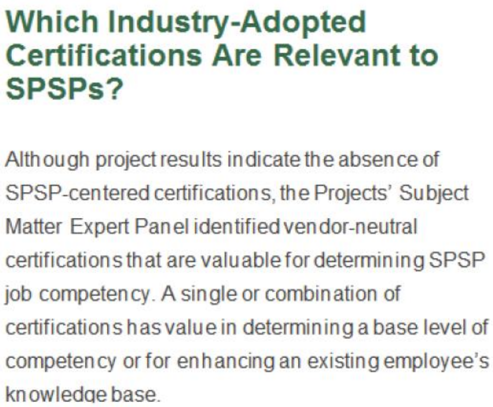
Project Overview: Industry Survey Response on Value in SPSP Recruiting

Total No. of Respondents by Job Category	No. Respondents Saying Content is Valuable	*Percent* Saying Content is Valuable	Meets Inclusion Criterion?*
HR (n = 7)	6	*86%*	Yes
Technical (n = 26)	19	*73%*	Yes
Power Staff (n = 9)	8	*89%*	Yes
Total across all industry respondents (n = 42)	**33**	***79%***	Yes

*Criterion: More than 1/3 of respondents consider the content valuable

[1] According to our criterion, a mean less than 2.5 suggests that the expert panel did not find the content useful.

C.10 Which Industry-Adopted Certifications are Relevant to SPSPs?



Which Industry-Adopted Certifications Are Relevant to SPSPs?

Although project results indicate the absence of SPSP-centered certifications, the Projects' Subject Matter Expert Panel identified vendor-neutral certifications that are valuable for determining SPSP job competency. A single or combination of certifications has value in determining a base level of competency or for enhancing an existing employee's knowledge base.

Ranking out of 9 thematic areas of the *Guide*

Industry Ranking:	7
Panel Ranking:	7

Subject Matter Expert Panel Mean (n = 7)
[Ratings from 1 (low value) to 5 (extreme value)]

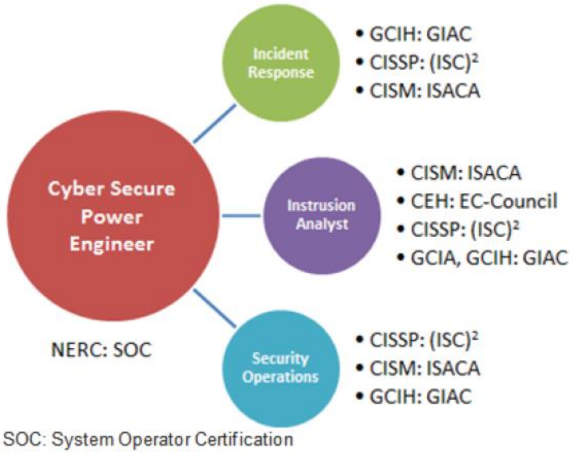
Panel Mean
3

Certifications: Industry Survey Response on value in SPSP recruiting

Total No. of Respondents by Job Category	No. Respondents Saying Content is Valuable	*Percent* Saying Content is Valuable	Meets Inclusion Criterion?*
HR (n = 7)	4	*57%*	Yes
Technical (n = 26)	14	*54%*	Yes
Power Staff (n = 9)	5	*56%*	Yes
Total across all industry respondents (n = 42)	**23**	***55%***	Yes

*Criterion: More than 1/3 of respondents consider the content valuable

C.11 Certification Diagram (Part of the Certifications Topical Theme)



SOC: System Operator Certification
CEH: Certified Ethical Hacker
CISM: Certified Information Security Manager
CISSP: Certified Information Systems Security Professional
GCIA: Certified Intrusion Analyst
GCIH: Certified Incident Handler
GISCP: GIAC Industrial Control System Professional

Subject Matter Expert Panel Mean (n = 7)
[Ratings from 1 (low value) to 5 (extreme value)]

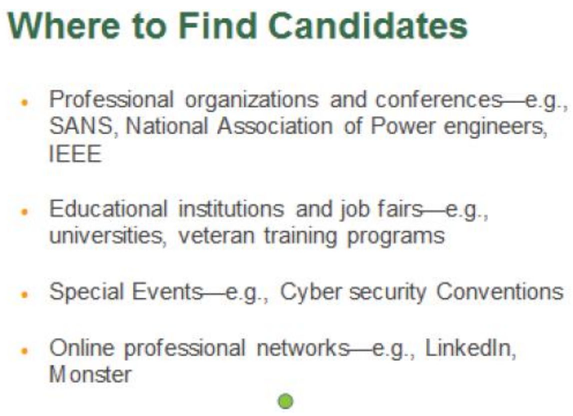
Panel Mean
3.5

Certification Diagram: Industry Survey Response on Value in SPSP Recruiting

Total No. of Respondents by Job Category	No. Respondents Saying Content is Valuable	*Percent* Saying Content is Valuable	Meets Inclusion Criterion?*
HR (n = 7)	5	*71%*	Yes
Technical (n = 26)	25	*96%*	Yes
Power Staff (n = 9)	7	*78%*	Yes
Total Across all industry respondents (n = 42)	**37**	***88%***	Yes

*Criterion: More than 1/3 of respondents consider the content valuable

C.12 Locating Talent



Where to Find Candidates

- Professional organizations and conferences—e.g., SANS, National Association of Power engineers, IEEE
- Educational institutions and job fairs—e.g., universities, veteran training programs
- Special Events—e.g., Cyber security Conventions
- Online professional networks—e.g., LinkedIn, Monster

Ranking out of 9 thematic areas of the *Guide*

Industry Ranking:	8
Panel Ranking:	4

Subject Matter Expert Panel Mean (n = 7)
[Ratings from 1 (low value) to 5 (extreme value)]

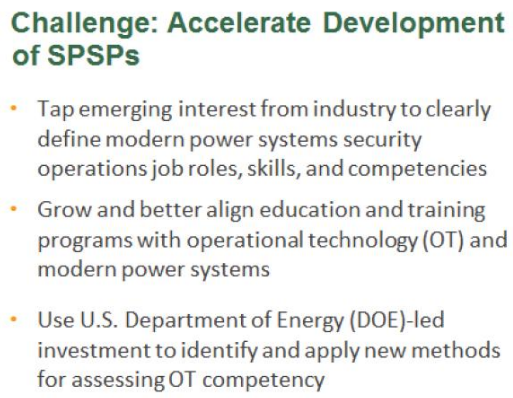
Panel Mean
3.14

Locating Talent: Industry Survey Response on Value in SPSP Recruiting

Total No. of Respondents by Job Category	No. Respondents Saying Content is Valuable	*Percent* Saying Content is Valuable	Meets Inclusion Criterion?*
HR (n = 7)	6	*86%*	Yes
Technical (n = 26)	19	*73%*	Yes
Power Staff (n = 9)	4	*44%*	Yes
Total across all industry respondents (n = 42)	**29**	***69%***	Yes

*Criterion: More than 1/3 of respondents consider the content valuable

C.13 Challenge



Challenge: Accelerate Development of SPSPs

- Tap emerging interest from industry to clearly define modern power systems security operations job roles, skills, and competencies
- Grow and better align education and training programs with operational technology (OT) and modern power systems
- Use U.S. Department of Energy (DOE)-led investment to identify and apply new methods for assessing OT competency

Ranking out of 9 thematic areas of the *Guide*

Industry Ranking:	9
Panel Ranking:	8

Subject Matter Expert Panel Mean (n = 7)
[Ratings from 1 (low value) to 5 (extreme value)]

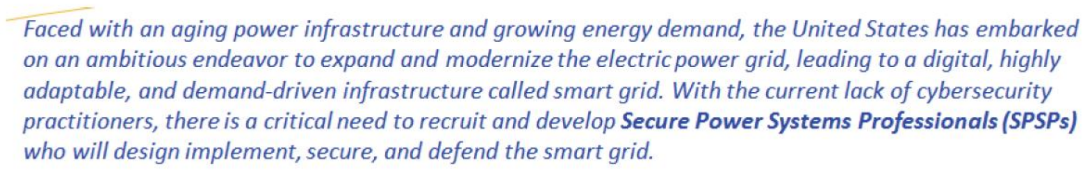
Panel Mean
3.17

Challenge: Industry Survey Response on Value in SPSP Recruiting

Total No. of Respondents by Job Category	No. Respondents Saying Content is Valuable	*Percent* Saying Content is Valuable	Meets Inclusion Criterion?*
HR (n = 7)	4	*57%*	Yes
Technical (n = 26)	16	*62%*	Yes
Power Staff (n = 9)	9	*100%*	Yes
Total across all industry respondents (n = 42)	**29**	***69%***	Yes

*Criterion: More than 1/3 of respondents consider the content valuable

C.14 Mission Statement (Part of the Challenge Topical Theme)



Faced with an aging power infrastructure and growing energy demand, the United States has embarked on an ambitious endeavor to expand and modernize the electric power grid, leading to a digital, highly adaptable, and demand-driven infrastructure called smart grid. With the current lack of cybersecurity practitioners, there is a critical need to recruit and develop ***Secure Power Systems Professionals (SPSPs)*** *who will design implement, secure, and defend the smart grid.*

Subject Matter Expert Panel Mean (n = 7)
[Ratings from 1 (low value) to 5 (extreme value)]

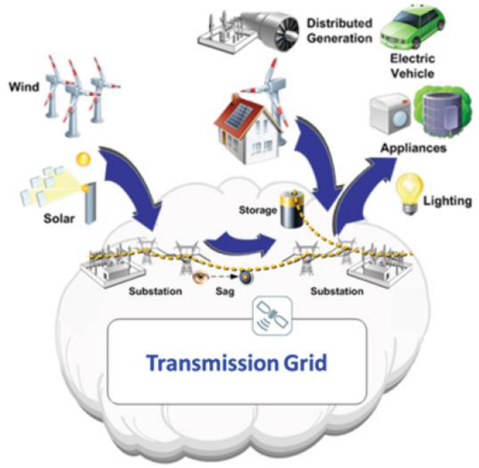
Panel Mean
2.83

Mission Statement: Industry Survey Response on Value in SPSP Recruiting

Total No. of Respondents by Job Category	No. Respondents Saying Content is Valuable	*Percent* Saying Content is Valuable	Meets Inclusion Criterion?*
HR (n = 7)	6	*86%*	Yes
Technical (n = 26)	21	*81%*	Yes
Power Staff (n = 9)	7	*78%*	Yes
Total across all industry respondents (n = 42)	**34**	***81%***	Yes

*Criterion: More than 1/3 of respondents consider the content valuable

C.15 Transmission Grid (Part of the Challenge Topical Theme)



Subject Matter Expert Panel Mean (n = 7)
[Ratings from 1 (low value) to 5 (extreme value)]

Panel Mean
3.0

Industry Survey Response Indicating Content is Valuable in Recruiting SPSPs

Total No. of Respondents by Job Category	No. Respondents Saying Content is Valuable	*Percent* Saying Content is Valuable	Meets Inclusion Criterion?*
HR (n = 7)	1	*14%*	No
Technical (n = 26)	16	*62%*	Yes
Power Staff (n = 9)	3	*33%*	No
Total across all industry respondents (n = 42)	**20**	***48%***	Yes

*Criterion: More than 1/3 of respondents consider the content valuable

Appendix D

Job Profiles

Appendix D

Job Profiles

The job profiles combine the work from Phases I and II in a format that can be used in part or in whole to align an organization's workforce capabilities with its strategic goals and tactical focus. The content of the job profiles can be incorporated into most human capital software to facilitate development of job descriptions and announcements, personnel evaluation forms, or individual development plans. Each job profile contains four distinct sections:

1. Major Responsibilities
2. National Cybersecurity Workforce Framework Tasks (n.d.)
3. Electricity Sector Cybersecurity Competency Maturity Model (ES-C2M2) Objectives to Determine Maturity Level (2014)
4. Applicable Certifications

The first subsection under each Job Profile, *Major Responsibilities*, establishes the essential job functions in accordance with the recommended practice of the Society for Human Resource Management (SHRM).[1] SHRM recommends that all job descriptions be documented using two primary sources:

- a valid job task analysis that produces a list of essential responsibilities (or functions) and a comprehensive list of knowledge, skill, and abilities required for successful job performance
- a list of related workforce requirements (e.g., the National Initiative for Cybersecurity Education functional role requirements, and the Electricity Sector Cybersecurity Capability Maturity Model [ES-C2M2] objectives), certifications, and education

Promoting Defensibility of Fair Hiring Practices

A primary goal for Phase III of the Secure Power Systems Professional project was to produce resources that can guide human resources professionals, recruiters, and technical managers in workforce planning, recruitment and selection, performance evaluation, and training and development of Secure Power Systems Professionals. The resources include:

- Recruitment and Career Development guides (see Appendix C)
- Job profiles (this Appendix)
- Behavioral interview guidelines (see Appendix E)
- Individual and team performance guidelines (see Appendix F).

Developed in accordance with current best practices for competency modeling (Campion et al. 2011), these resources will support future development of assessment, certification, selection, and development programs that will meet standards established by the U.S. Equal Employment Opportunity Commission and the American National Standards Institute. Research has shown that following these guidelines improves the legal defensibility of human resources practices (Arvey1979; 43 FR 38290-38315 1978; Kesselman and Lopez 1979; Pursell et al. 1980, Tobey 2011).

[1] http://www.shrm.org; see Insert

Phase I of this project produced the required job task analysis. The result was a predictive model of job performance that identified the major responsibilities reported in this appendix.

Phase II of this project enabled the identification of appropriate National Initiative for Cybersecurity Education (NICE) tasks and ES-C2M2 objectives, which establishes the workforce requirements for Secure Power Systems Professionals (SPSPs) in government-related and private industry organizations, respectively. These are described in the sections of this appendix on *National Cybersecurity Workforce Framework Tasks* and *ES-C2M2 Objectives to Determine Maturity Level*.

Phase II also produced a list of applicable certifications with test content that informs qualification of personnel for task domains related to each of the major responsibilities for a job. Thus, in accordance with the SHRM recommended practice, the applicable workforce requirements and related certifications are shown below the major responsibilities for each job role. These are described in the section, *Applicable Certifications*.

How to Use This Guide

This appendix contains the following sections:

(D.1) Secure Power Systems Engineer

(D.2) Secure Power Systems Incident Responder

(D.3) Secure Power Systems Intrusion Analyst

(D.4) Secure Power Systems Security Operator

The profiles may be applied to develop performance reviews or to produce individual development programs for existing staff. The workforce framework objectives of the NICE and ES-C2M2 differentiated by job role can be used to align job descriptions with workforce requirements of government and industry. The certifications section provides human resources professionals with information relating to the qualification of personnel for specific task domains within each job role.

D.1 Secure Power Systems Engineer

D.1.1 Major Responsibilities

1. Assess and manage power systems risk
2. Identify and mitigate power systems vulnerabilities
3. Implement power systems security monitoring
4. Log power systems security incidents

D.1.2 NICE - National Cybersecurity Workforce Framework Tasks

The NICE: National Cybersecurity Workforce Framework V1.0 was used in Phase II to map the Major Responsibilities.

D.1.2.1 Assess and Manage Power Systems Risk

NICE Task ID	Description
411	Analyze site/enterprise Computer Network Defense policies and configurations and evaluate compliance with regulations and enterprise directives
474	Coordinate with intelligence analysts to correlate threat assessment data
478	Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation
643	Identify potential conflicts with implementation of any Computer Network Defense tools within the Computer Network Defense service provider area of responsibility (e.g., tool/signature testing and optimization)
685	Maintain deployable Computer Network Defense audit toolkit (e.g., specialized Computer Network Defense software/hardware) to support Computer Network Defense audit missions
692	Maintain knowledge of applicable Computer Network Defense policies, regulations, and compliance documents specifically related to Computer Network Defense auditing
716	Monitor external data sources (e.g., Computer Network Defense vendor sites, Computer Emergency Response Teams, SANS, Security Focus) to maintain currency of Computer Network Defense threat condition and determine which security issues may have an impact on the enterprise
744	Perform Computer Network Defense risk assessments within the enterprise
746	Perform Computer Network Defense vulnerability assessments within the enterprise

D.1.2.2 Identify and Mitigate Power Systems Vulnerabilities

NICE Task ID	Description
427	Assist in the construction of signatures that can be implemented on Computer Network Defense network tools in response to new or observed threats within the enterprise
433	Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources
438	Collect and analyze intrusion artifacts (e.g., source code, malware, and trojans) and use discovered data to enable mitigation of potential Computer Network Defense incidents within the enterprise
448	Conduct authorized penetration testing of enterprise network assets
470	Coordinate with and provide expert technical support to enterprise-wide Computer Network Defense technicians to resolve Computer Network Defense incidents
478	Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation
685	Maintain deployable Computer Network Defense audit toolkit (e.g., specialized Computer Network Defense software/hardware) to support Computer Network Defense audit missions
743	Perform Computer Network Defense incident triage to include determining scope, urgency, and potential impact; identify the specific vulnerability and make recommendations that enable expeditious remediation
744	Perform Computer Network Defense risk assessments within the enterprise
746	Perform Computer Network Defense vulnerability assessments within the enterprise
762	Perform real-time Computer Network Defense Incident Handling tasks (e.g., forensic collections, intrusion correlation/tracking, threat analysis, and direct system remediation) to support deployable Incident Response Teams (IRTs)

D.1.2.3 Implement Power Systems Security Monitoring

NICE Task ID	Description
393	Administer Computer Network Defense test bed and test and evaluate new Computer Network Defense applications, rules/signatures, access controls, and configurations of Computer Network Defense service-provider-managed platforms
822	Purchase or build, install, configure, and test specialized hardware to be deployed at remote sites

D.1.2.4 Log Power Systems Security Incidents

NICE Task ID	Description
433	Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources
738	Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system logs) to identify possible threats to network security
750	Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack
762	Perform real-time Computer Network Defense Incident Handling tasks (e.g., forensic collections, intrusion correlation/tracking, threat analysis, and direct system remediation) to support deployable IRTs
823	Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts
861	Track and document Computer Network Defense incidents from initial detection through final resolution

D.1.3 ES-C2M2 Objectives to Determine Maturity Level

The Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) was used in Phase I.

D.1.3.1 Assess and Manage Power Systems Risk

- Establish Cybersecurity Risk Management Strategy (4.3.1 Risk Management)
- Manage Cybersecurity Risk (4.3.1 Risk Management)
- Manage Dependency Risk (4.3.8 Supply Chain and External Dependencies Management)
- Manage Risk Activities (4.3.1 Risk Management)

D.1.3.2 Identify and Mitigate Power Systems Vulnerabilities

- Identify and Respond to Threats (4.3.4 Threat and Vulnerability Management)
- Reduce Cybersecurity Vulnerabilities (4.3.4 Threat and Vulnerability Management)

D.1.3.3 Implement Power Systems Monitoring

- Detect Cybersecurity Events (4.3.7 Event and Incident Response, Continuity of Operations)

D.1.3.4 Log Power Systems Security Incidents

- Detect Cybersecurity Events (4.3.7 Event and Incident Response, Continuity of Operations)
- Perform Logging (4.3.5 Situational Awareness)

D.1.4 Applicable Certifications

The list below represents certifications available during the Phase II period; there were no certifications specific to power systems available during this period. Future work should be done to update the list of certifications.

D.1.4.1 Assess and Manage Power Systems Risk

- Risk and Program Management – Governance (Certified Information Systems Auditor [CISA], Certified Information Security Manager [CISM], Certified Information Systems Security Professional [CISSP])
- Security Analysis (CISA, CISSP, Certified in Risk and Information Systems Control [CRISC], GCIA (GIAC Certified Intrusion Analyst Certification), Security+)
- Security Design (CISA, CISSP, CRISC)

D.1.4.2 Identify and Mitigate Vulnerabilities

- Attack Techniques – Discovery (certified ethical hacking [CEH], GIAC Certified Incident Handler Certification [GCIH], GIAC Penetration Testing Certification [GPEN], GIAC Web Application Penetration Tester [GWAPT], Security+)
- Penetration Testing (CEH, GPEN, GWAPT)

D.1.4.3 Implement Power Systems Security Monitoring

- Attack Techniques – Discovery (CEH, GCIH, GPEN, GWAPT, Security+)
- Networking (CISSP, GCIA, System Operator Certification [SOC])
- Network Security (GCIA)
- Security Analysis (CISA, CISSP, CRISC, GCIA, Security+)

D.1.4.4 Log Power Systems Security Incidents

- Attack Techniques – Network (CEH, GCIH)
- Network Security (GCIA)
- Risk and Program Management – Governance (CISA, CISM, CISSP)
- Security Analysis (CISA, CISSP, CRISC, GCIA, Security+)
- Security Design (CISA, CISSP, CRISC)

D.2 Secure Power Systems Incident Responder

D.2.1 Major Responsibilities

1. Develop and manage power systems personnel
2. Log power systems security incidents
3. Manage power systems process and procedures
4. Respond to power systems intrusions

D.2.1.1 NICE - National Cybersecurity Workforce Framework Tasks

The NICE: National Cybersecurity Workforce Framework V1.0 was used in Phase II to map the Major Responsibilities.

D.2.1.2 Develop and Manage Power Systems Personnel

There are no NICE: National Cybersecurity Workforce Framework Tasks for this responsibility.

D.2.1.3 Log Power Systems Security Incidents

NICE Task ID	Description
433	Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources
738	Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system logs) to identify possible threats to network security
750	Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack
762	Perform real-time Computer Network Defense Incident Handling tasks (e.g., forensic collections, intrusion correlation/tracking, threat analysis, and direct system remediation) to support deployable IRTs
823	Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts
861	Track and document Computer Network Defense incidents from initial detection through final resolution

D.2.1.4 Manage Power Systems Process and Procedures

NICE Task ID	Description
411	Analyze site/enterprise Computer Network Defense policies and configurations and evaluate compliance with regulations and enterprise directives
654	Implement certification and accreditation requirements for specialized Computer Network Defense systems within the enterprise, and document and maintain records for them
692	Maintain knowledge of applicable Computer Network Defense policies, regulations, and compliance documents specifically related to Computer Network Defense auditing

D.2.1.5 Respond to Power Systems Intrusions

NICE Task ID	Description
438	Collect and analyze intrusion artifacts (e.g., source code, malware, and trojans) and use discovered data to enable mitigation of potential Computer Network Defense incidents within the enterprise
470	Coordinate with and provide expert technical support to enterprise-wide Computer Network Defense technicians to resolve Computer Network Defense incidents
723	Notify Computer Network Defense managers, Computer Network Defense incident responders, and other Computer Network Defense Service Provider team members of any suspected Computer Network Defense incident and articulate the event’s history, status, and potential impact for further action
741	Perform command and control functions in response to incidents
743	Perform Computer Network Defense incident triage to include determining scope, urgency, and potential impact; identify the specific vulnerability and make recommendations that enable expeditious remediation
755	Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems
762	Perform real-time Computer Network Defense Incident Handling tasks (e.g., forensic collections, intrusion correlation/tracking, threat analysis, and direct system remediation) to support deployable IRTs
823	Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts
846	Serve as technical experts and liaisons to law enforcement personnel and explain incident details, provide testimony, etc.
861	Track and document Computer Network Defense incidents from initial detection through final resolution

D.2.2 ES-C2M2 Objectives to Determine Maturity Level

The Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) was used in Phase II.

D.2.2.1 Develop and Manage Power Systems Personnel

- Control the Workforce Lifecycle (4.3.9 Workforce Management)
- Develop Cybersecurity Workforce (4.3.9 Workforce Management)
- Increase Cybersecurity Awareness (4.3.9 Workforce Management)
- Manage Workforce Activities (4.3.9 Workforce Management)

D.2.2.2 Log Power Systems Security Incidents

- Detect Cybersecurity Events (4.3.7 Event and Incident Response, Continuity of Operations)
- Perform Logging (4.3.5 Situational Awareness)

D.2.2.3 Manage Power Systems Process and Procedures

- Establish and Maintain a Common Operating Picture (4.3.5 Situational Awareness)
- Establish and Maintain Cybersecurity Architecture (4.3.10 Cybersecurity Program Management)
- Establish Cybersecurity Risk Management Strategy (4.3.1 Risk Management)
- Manage Asset Activities (4.3.2 Asset, Change, and Configuration Management)
- Manage Changes to Assets (4.3.2 Asset, Change, and Configuration Management)
- Manage Cyber Activities (4.3.10 Cybersecurity Program Management)
- Manage Dependencies Activities (4.3.8 Supply Chain and External Dependencies Management)
- Plan for Continuity (4.3.7 Event and Incident Response, Continuity of Operations)

D.2.2.4 Respond to Power Systems Intrusions

- Identify and Respond to Threats (4.3.4 Threat and Vulnerability Management)
- Manage Response Activities (4.3.7 Event and Incident Response, Continuity of Operations)
- Respond to Escalated Cybersecurity Event (4.3.7 Event and Incident Response, Continuity of Operations)

D.2.3 Applicable Certifications

The list below represents certifications available during the Phase II period; there were no certifications specific to power systems available during this period. Future work should be done to update the list of certifications.

D.2.3.1 Develop and Manage Power Systems Personnel

- Risk and Program Management – Compliance (CISM, CISSP, GPEN, Security+)
- Risk and Program Management – Governance (CISA, CISM, CISSP)
- Security Analysis (CISA, CISSP, CRISC, GCIA, Security+)

D.2.3.2 Log Power Systems Security Incidents

- Attack Techniques – Network (CEH, GCIH)
- Network Security (GCIA)
- Risk and Program Management – Governance (CISA, CISM, CISSP)
- Security Analysis (CISA, CISSP, CRISC, GCIA, Security+)
- Security Design (CISA, CISSP, CRISC)

D.2.3.3 Manage Power Systems Process and Procedures

- Power System Reliability
- Risk and Program Management – Governance (CISA, CISM, CISSP)
- Risk and Program Management – Program Management (CISA, CISM)
- Security Analysis (CISA, CISSP, CRISC, GCIA, Security+)

D.2.3.4 Respond to Power Systems Intrusions

None

D.3 Secure Power Systems Intrusion Analyst

D.3.1 Major Responsibilities

1. Analyze power systems security incidents
2. Develop and manage power systems personnel
3. Identify and mitigate power systems vulnerabilities
4. Log power systems security incidents
5. Respond to power systems intrusions

D.3.2 NICE - National Cybersecurity Workforce Framework Tasks

The NICE: National Cybersecurity Workforce Framework V1.0 was used in Phase II to map the Major Responsibilities.

D.3.2.1 Analyze Power Systems Security Incidents

NICE Task ID	Description
427	Assist in the construction of signatures that can be implemented on Computer Network Defense network tools in response to new or observed threats within the enterprise
433	Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources
438	Collect and analyze intrusion artifacts (e.g., source code, malware, and trojans) and use discovered data to enable mitigation of potential Computer Network Defense incidents within the enterprise
472	Coordinate with enterprise-wide Computer Network Defense staff to validate network alerts
478	Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation
723	Notify Computer Network Defense managers, Computer Network Defense incident responders, and other Computer Network Defense Service Provider team members of any suspected Computer Network Defense incident and articulate the event's history, status, and potential impact for further action
738	Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system logs) to identify possible threats to network security
743	Perform Computer Network Defense incident triage to include determining scope, urgency, and potential impact; identify the specific vulnerability and make recommendations that enable expeditious remediation
750	Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack
755	Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems
762	Perform real-time Computer Network Defense Incident Handling tasks (e.g., forensic collections, intrusion correlation/tracking, threat analysis, and direct system remediation) to support deployable IRTs
823	Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts
846	Serve as technical experts and liaisons to law enforcement personnel and explain incident details, provide testimony, etc.
861	Track and document Computer Network Defense incidents from initial detection through final resolution

D.3.2.2 Develop and Manage Power Systems Personnel

- There are no NICE: National Cybersecurity Workforce Framework Tasks for this responsibility.

D.3.2.3 Identify and Mitigate Power Systems Vulnerabilities

NICE Task ID	Description
427	Assist in the construction of signatures that can be implemented on Computer Network Defense network tools in response to new or observed threats within the enterprise
433	Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources
438	Collect and analyze intrusion artifacts (e.g., source code, malware, and trojans) and use discovered data to enable mitigation of potential Computer Network Defense incidents within the enterprise
448	Conduct authorized penetration testing of enterprise network assets
470	Coordinate with and provide expert technical support to enterprise-wide Computer Network Defense technicians to resolve Computer Network Defense incidents
478	Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation
685	Maintain deployable Computer Network Defense audit toolkit (e.g., specialized Computer Network Defense software/hardware) to support Computer Network Defense audit missions
743	Perform Computer Network Defense incident triage to include determining scope, urgency, and potential impact; identify the specific vulnerability and make recommendations that enable expeditious remediation
744	Perform Computer Network Defense risk assessments within the enterprise
746	Perform Computer Network Defense vulnerability assessments within the enterprise
762	Perform real-time Computer Network Defense Incident Handling tasks (e.g., forensic collections, intrusion correlation/tracking, threat analysis, and direct system remediation) to support deployable IRTs

D.3.2.4 Log Power Systems Security Incidents

NICE Task ID	Description
433	Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources
738	Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system logs) to identify possible threats to network security
750	Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack

NICE Task ID	Description
762	Perform real-time Computer Network Defense Incident Handling tasks (e.g., forensic collections, intrusion correlation/tracking, threat analysis, and direct system remediation) to support deployable IRTs
823	Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts
861	Track and document Computer Network Defense incidents from initial detection through final resolution

D.3.2.5 Respond to Power Systems Intrusions

NICE Task ID	Description
438	Collect and analyze intrusion artifacts (e.g., source code, malware, and trojans) and use discovered data to enable mitigation of potential Computer Network Defense incidents within the enterprise
470	Coordinate with and provide expert technical support to enterprise-wide Computer Network Defense technicians to resolve Computer Network Defense incidents
723	Notify Computer Network Defense managers, Computer Network Defense incident responders, and other Computer Network Defense Service Provider team members of any suspected Computer Network Defense incident and articulate the event’s history, status, and potential impact for further action
741	Perform command and control functions in response to incidents
743	Perform Computer Network Defense incident triage to include determining scope, urgency, and potential impact; identify the specific vulnerability and make recommendations that enable expeditious remediation
755	Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems
762	Perform real-time Computer Network Defense Incident Handling tasks (e.g., forensic collections, intrusion correlation/tracking, threat analysis, and direct system remediation) to support deployable IRTs
823	Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts
846	Serve as technical experts and liaisons to law enforcement personnel and explain incident details, provide testimony, etc.
861	Track and document Computer Network Defense incidents from initial detection through final resolution

D.3.3 ES-C2M2 Objectives to Determine Maturity Level

The Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) was used in Phase II.

D.3.3.1 Analyze Power Systems Security Incidents

- Detect Cybersecurity Events (4.3.7 Event and Incident Response, Continuity of Operations)
- Identify and Respond to Threats (4.3.4 Threat and Vulnerability Management)

D.3.3.2 Develop and Manage Power Systems Personnel

- Control the Workforce Lifecycle (4.3.9 Workforce Management)
- Develop Cybersecurity Workforce (4.3.9 Workforce Management)
- Increase Cybersecurity Awareness (4.3.9 Workforce Management)
- Manage Workforce Activities (4.3.9 Workforce Management)

D.3.3.3 Identify and Mitigate Power Systems Vulnerabilities

- Identify and Respond to Threats (4.3.4 Threat and Vulnerability Management)
- Reduce Cybersecurity Vulnerabilities (4.3.4 Threat and Vulnerability Management)

D.3.3.4 Log Power Systems Security Incidents

- Detect Cybersecurity Events (4.3.7 Event and Incident Response, Continuity of Operations)
- Perform Logging (4.3.5 Situational Awareness)

D.3.3.5 Respond to Power Systems Intrusions

- Identify and Respond to Threats (4.3.4 Threat and Vulnerability Management)
- Manage Response Activities (4.3.7 Event and Incident Response, Continuity of Operations)
- Respond to Escalated Cybersecurity Event (4.3.7 Event and Incident Response, Continuity of Operations)

D.3.4 Applicable Certifications

The list below represents certifications available during the Phase II period; there were no certifications specific to power systems available during this period. Future work should be done to update the list of certifications.

D.3.4.1 Analyze Security Incidents

- Attack Techniques – Discovery (CEH, GCIH, GPEN, GWAPT, Security+)
- Incident Handling (CISM, GCIH)

- Network Security (GCIA)
- Networking (CISSP, GCIA, SOC)
- Risk and Program Management – Business Continuity and Recovery (CISSP)
- Risk and Program Management – Compliance (CISM, CISSP, GPEN, Security+)
- Risk and Program Management – Governance (CISA, CISM, CISSP)
- Security Analysis (CISA, CISSP, CRISC, GCIA, Security+)
- Security Design (CISA, CISSP, CRISC)

D.3.4.2 Develop and Manage Personnel

- Risk and Program Management – Compliance (CISM, CISSP, GPEN, Security+)
- Risk and Program Management – Governance (CISA, CISM, CISSP)
- Security Analysis (CISA, CISSP, CRISC, GCIA, Security+)

D.3.4.3 Identify and Mitigate Vulnerabilities

- Attack Techniques – Discovery (CEH, GCIH, GPEN, GWAPT, Security+)
- Penetration Testing (CEH, GPEN, GWAPT)

D.3.4.4 Log Power Systems Security Incidents

- Attack Techniques – Network (CEH, GCIH)
- Network Security (GCIA)
- Risk and Program Management – Governance (CISA, CISM, CISSP)
- Security Analysis (CISA, CISSP, CRISC, GCIA, Security+)
- Security Design (CISA, CISSP, CRISC)

D.3.4.5 Respond to Power Systems Intrusions

None

D.4 Secure Power Systems Security Operator

D.4.1 Major Responsibilities

1. Analyze power systems security incidents
2. Develop and manage power systems personnel
3. Identify and mitigate power systems vulnerabilities
4. Implement power systems security monitoring

5. Log power systems security incidents
6. Manage power systems projects and budgets
7. Manage power systems security operations

D.4.2 NICE - National Cybersecurity Workforce Framework Tasks

The NICE: National Cybersecurity Workforce Framework V1.0 was used in Phase II to map the Major Responsibilities.

D.4.2.1 Analyze Power Systems Security Incidents

NICE Task ID	Description
427	Assist in the construction of signatures that can be implemented on Computer Network Defense network tools in response to new or observed threats within the enterprise
433	Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources
438	Collect and analyze intrusion artifacts (e.g., source code, malware, and trojans) and use discovered data to enable mitigation of potential Computer Network Defense incidents within the enterprise
472	Coordinate with enterprise-wide Computer Network Defense staff to validate network alerts
478	Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation
723	Notify Computer Network Defense managers, Computer Network Defense incident responders, and other Computer Network Defense Service Provider team members of any suspected Computer Network Defense incident and articulate the event’s history, status, and potential impact for further action
738	Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system logs) to identify possible threats to network security
743	Perform Computer Network Defense incident triage to include determining scope, urgency, and potential impact; identify the specific vulnerability and make recommendations that enable expeditious remediation
750	Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack
755	Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems
762	Perform real-time Computer Network Defense Incident Handling tasks (e.g., forensic collections, intrusion correlation/tracking, threat analysis, and direct system remediation) to support deployable IRTs
823	Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts

NICE Task ID	Description
846	Serve as technical experts and liaisons to law enforcement personnel and explain incident details, provide testimony, etc.
861	Track and document Computer Network Defense incidents from initial detection through final resolution

D.4.2.2 Develop and Manage Power Systems Personnel

There are no NICE: National Cybersecurity Workforce Framework Tasks for this responsibility.

D.4.2.3 Identify and Mitigate Power Systems Vulnerabilities

NICE Task ID	Description
427	Assist in the construction of signatures that can be implemented on Computer Network Defense network tools in response to new or observed threats within the enterprise
433	Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources
438	Collect and analyze intrusion artifacts (e.g., source code, malware, and trojans) and use discovered data to enable mitigation of potential Computer Network Defense incidents within the enterprise
448	Conduct authorized penetration testing of enterprise network assets
470	Coordinate with and provide expert technical support to enterprise-wide Computer Network Defense technicians to resolve Computer Network Defense incidents
478	Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation
685	Maintain deployable Computer Network Defense audit toolkit (e.g., specialized Computer Network Defense software/hardware) to support Computer Network Defense audit missions
743	Perform Computer Network Defense incident triage to include determining scope, urgency, and potential impact; identify the specific vulnerability and make recommendations that enable expeditious remediation
744	Perform Computer Network Defense risk assessments within the enterprise
746	Perform Computer Network Defense vulnerability assessments within the enterprise
762	Perform real-time Computer Network Defense Incident Handling tasks (e.g., forensic collections, intrusion correlation/tracking, threat analysis, and direct system remediation) to support deployable IRTs

D.4.2.4 Implement Power Systems Security Monitoring

NICE Task ID	Description
393	Administer Computer Network Defense test bed and test and evaluate new Computer Network Defense applications, rules/signatures, access controls, and configurations of Computer Network Defense service-provider-managed platforms
822	Purchase or build, install, configure, and test specialized hardware to be deployed at remote sites

D.4.2.5 Log Power Systems Security Incidents

NICE Task ID	Description
433	Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources
738	Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system logs) to identify possible threats to network security
750	Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack
762	Perform real-time Computer Network Defense Incident Handling tasks (e.g., forensic collections, intrusion correlation/tracking, threat analysis, and direct system remediation) to support deployable IRTs
823	Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts
861	Track and document Computer Network Defense incidents from initial detection through final resolution

D.4.2.6 Manage Power Systems Projects and Budgets

NICE Task ID	Description
822	Purchase or build, install, configure, and test specialized hardware to be deployed at remote sites

D.4.2.7 Respond to Power Systems Intrusions

NICE Task ID	Description
393	Administer Computer Network Defense test bed and test and evaluate new Computer Network Defense applications, rules/signatures, access controls, and configurations of Computer Network Defense service-provider-managed platforms
741	Perform command and control functions in response to incidents

NICE Task ID	Description
769	Perform system administration on specialized Computer Network Defense applications and systems (e.g., anti-virus, Audit/Remediation, or virtual private network devices) to include installation, configuration, maintenance, and backup/restore

D.4.3 ES-C2M2 Objectives to Determine Maturity Level

The Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) was used in Phase II.

D.4.3.1 Analyze Power Systems Security Incidents

- Detect Cybersecurity Events (4.3.7 Event and Incident Response, Continuity of Operations)
- Identify and Respond to Threats (4.3.4 Threat and Vulnerability Management)

D.4.3.2 Develop and Manage Power Systems Personnel

- Control the Workforce Lifecycle (4.3.9 Workforce Management)
- Develop Cybersecurity Workforce (4.3.9 Workforce Management)
- Increase Cybersecurity Awareness (4.3.9 Workforce Management)
- Manage Workforce Activities (4.3.9 Workforce Management)

D.4.3.3 Identify and Mitigate Power Systems Vulnerabilities

- Identify and Respond to Threats (4.3.4 Threat and Vulnerability Management)
- Reduce Cybersecurity Vulnerabilities (4.3.4 Threat and Vulnerability Management)

D.4.3.4 Implement Power Systems Security Monitoring

- Detect Cybersecurity Events (4.3.7 Event and Incident Response, Continuity of Operations)

D.4.3.5 Log Power Systems Security Incidents

- Detect Cybersecurity Events (4.3.7 Event and Incident Response, Continuity of Operations)
- Perform Logging (4.3.5 Situational Awareness)

D.4.3.6 Manage Power Systems Projects and Budgets

- Sponsor Cybersecurity Program (4.3.10 Cybersecurity Program Management)

D.4.3.7 Manage Power Systems Security Operations

- Assign Cybersecurity Responsibilities (4.3.9 Workforce Management)
- Escalate Cybersecurity Events (4.3.7 Event and Incident Response, Continuity of Operations)
- Establish and Maintain a Common Operating Picture (4.3.5 Situational Awareness)

- Establish Cybersecurity Program Strategy (4.3.10 Cybersecurity Program Management)
- Manage Cyber Activities (4.3.10 Cybersecurity Program Management)
- Manage Response Activities (4.3.7 Event and Incident Response, Continuity of Operations)
- Manage Situation Activities (4.3.5 Situational Awareness)
- Plan for Continuity (4.3.7 Event and Incident Response, Continuity of Operations)

D.4.4 Applicable Certifications

The list below represents certifications available during the Phase II period; there were no certifications specific to power systems available during this period. Future work should be done to update the list of certifications.

D.4.4.1 Analyze Security Incidents

- Attack Techniques – Discovery (CEH, GCIH, GPEN, GWAPT, Security+)
- Incident Handling (CISM, GCIH)
- Network Security (GCIA)
- Networking (CISSP, GCIA, SOC)
- Risk and Program Management – Business Continuity and Recovery (CISSP)
- Risk and Program Management – Compliance (CISM, CISSP, GPEN, Security+)
- Risk and Program Management – Governance (CISA, CISM, CISSP)
- Security Analysis (CISA, CISSP, CRISC, GCIA, Security+)
- Security Design (CISA, CISSP, CRISC)

D.4.4.2 Develop and Manage Personnel

- Risk and Program Management – Compliance (CISM, CISSP, GPEN, Security+)
- Risk and Program Management – Governance (CISA, CISM, CISSP)
- Security Analysis (CISA, CISSP, CRISC, GCIA, Security+)

D.4.4.3 Identify and Mitigate Vulnerabilities

- Attack Techniques – Discovery (CEH, GCIH, GPEN, GWAPT, Security+)
- Penetration Testing (CEH, GPEN, GWAPT)

D.4.4.4 Implement Power Systems Security Monitoring

- Attack Techniques – Discovery (CEH, GCIH, GPEN, GWAPT, Security+)
- Networking (CISSP, GCIA, SOC)

- Network Security (GCIA)
- Security Analysis (CISA, CISSP, CRISC, GCIA, Security+)

D.4.4.5 Log Power Systems Security Incidents

- Attack Techniques – Network (CEH, GCIH)
- Network Security (GCIA)
- Risk and Program Management – Governance (CISA, CISM, CISSP)
- Security Analysis (CISA, CISSP, CRISC, GCIA, Security+)
- Security Design (CISA, CISSP, CRISC)

D.4.4.6 Manage Power Systems Projects and Budgets

- Risk and Program Management – Program Management (CISA, CISM)
- Security Analysis (CISA, CISSP, CRISC, GCIA, Security+)

D.4.4.7 Manage Power Systems Security Operations

- Attack Techniques – Web and Applications (CEH, GCIH, GPEN, GWAPT)
- Incident Handling (CISM, GCIH)
- Security Analysis (CISA, CISSP, CRISC, GCIA, Security+)
- Security Design (CISA, CISSP, CRISC)

D.5 References

43 FR 38290–38315. 1978. "Equal Employment Opportunity Commission, Civil Service Commission, Department of Labor and Department of Justice. Adoption by four agencies of Uniform Guidelines on Employee Selection Procedures." U.S. Department of Energy, *Federal Register*.

Arvey, RD. 1979. "Unfair discrimination in the employment interview: Legal and psychological aspects." *Psychological Bulletin*, 86(4):736–765.

Campion, MA, AA Fink, BJ Ruggenberg, L Carr, GM Phillips, and RB Odman. 2011. "Doing competencies well: Best practices in competency modeling." *Personnel Psychology*, 64:225–262.

ES-C2M2 - Electricity Subsector Cybersecurity Capability Maturity Model. 2014. *Objectives to Determine Maturity Level*. http://energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf

Kesselman, GA and FE Lopez. 1979. "The impact of job analysis on employment test validation for minority and nonminority accounting personnel." *Personnel Psychology*, 32(1):91–108.

National CyberSecurity Workforce Framework. n.d. http://csrc.nist.gov/nice/framework/national_cybersecurity_workforce_framework_03_2013_version1_0_for_printing.pdf.

Pursell, ED, MA Campion, and SR Gaylord. 1980. “Structured interviewing: Avoiding selection problems.” *Personnel Journal*, 59(11):907–912.

Tobey, DH. 2011. *A competency model of advanced threat response. ATR Working Group Report NBISE-ATR-11-02*. Idaho Falls, ID: National Board of Information Security Examiners.

Appendix E

Behavioral Interview Guidelines by Job Role

Appendix E

Behavioral Interview Guidelines by Job Roles

The Behavioral Interview Guidelines apply the results of Phases I and II in a format that can be used in part or in whole to align workforce capabilities with the strategic goals and tactical focus of an organization. The primary objective of the Behavioral Guidelines was to provide a resource for recruiting and interviewing candidates for new position openings.

The Behavioral Guidelines have several possible uses. First, the guidelines may be applied to develop performance reviews or to produce individual development programs for existing staff. Second, the guidelines may assist in specifying learning objectives for a training or education program. Finally, the guidelines may be easily incorporated into most human capital software to facilitate development of job descriptions that comply with guidelines established by the Society of Human Resource Management. Society of Human Resource Management recommends that all job descriptions be documented using two primary sources:

- a valid job task analysis that produces a list of essential responsibilities (or functions) and a comprehensive list of knowledge, skills, and abilities required for successful job performance
- a list of related workforce requirements (e.g., the National Initiative for Cybersecurity Education, or National Initiative for Cybersecurity Education, functional role requirements and the Electricity Sector – Cybersecurity Capability Maturity Model, ES-C2M2, objectives), certifications, and education

Promoting Defensibility of Fair Hiring Practices

A primary goal for Phase III of the Secure Power Systems Professional project was to produce resources that can guide human resource professionals, recruiters, and technical managers in workforce planning, staff recruitment and selection, performance evaluation, and training and development of Secure Power Systems Professionals. The resources include:

- Recruitment and Career Development guides (see Appendix G)
- Job profiles (see Appendix D)
- Behavioral interview guidelines (this Appendix)
- Individual and team performance guidelines (see Appendix F).

Developed in accordance with current best practices for competency modeling (Campion et al. 2011), these resources will support future development of assessment, certification, selection, and development programs that will meet standards established by the U.S. Equal Employment Opportunity Commission and the American National Standards Institute. Research has shown that following these guidelines improves the legal defensibility of human resource practices (Arvey1979; 43 FR 38290-38315 1978; Kesselman and Lopez 1979; Pursell et al. 1980, Tobey 2011).

Phase I of this project produced the required job task analysis. The result was a predictive model of job performance that identified the major responsibilities reported in Appendix D. The complete list of knowledge, skills and abilities required in each of the studied job roles was assembled into the Behavioral Interview Guidelines reported below.

How to Use This Guide

This appendix contains the Behavioral Interview Guideline Items for the four job profiles in the following sections:

(E.1) Secure Power Systems Engineer

(E.2) Secure Power Systems Intrusion Analyst

(E.3) Secure Power Systems Incident Responder

(E.4) Secure Power Systems Security Operator

The guidelines may be applied to develop performance reviews or to produce individual development programs for existing staff. Human Resources professionals can use the information provided in the tables below to conduct a survey of the current employees to confirm whether their current staff has the specified knowledge, skill, or ability. Furthermore, the guidelines can be incorporated into most human capital software to facilitate development of job descriptions.

A hiring manager can use the guide to select the specific knowledge, skills, and abilities applicable to an open position based on the strategic focus and/or workforce competency gaps in their organization. The following steps should be followed:

1. A hiring manager places a checkmark in an area of knowledge, skill, or ability to include in their plan.
2. The completed form is sent to a Human Resources professional or recruiter for development of recruitment and selection programs.
3. Human Resources professionals may also add the checked items to job descriptions and performance evaluation forms.

NOTE*: By following these steps, Human Resources can apply the competency requirements necessary for successful SPSP job performance to current human capital management practices.*

E.1 Behavioral Interview Guideline Items: Secure Power Systems Engineer

X	**Knowledge** ***The understanding of a concept, strategy, or procedure; knowledge is measured by depth of understanding, from shallow to deep.***
	Access an up-to-date power systems inventory and asset list
	Collect vendor knowledge bases and testing reports generated by the U.S. Department of Energy (DOE) and U.S. Department of Homeland Security (DHS) of known vulnerabilities to specific power systems components. Supplement that information with open-source reporting and internal red teaming or tabletop assessments
	Establish a test lab where tools can be practiced and learned
	Understand the environment (culture, personnel) to create a better relationship for transmitting delicate and sometimes poorly understood information
	Understand North American Electric Reliability Corporation (NERC) critical infrastructure protection (CIP) and audit requirements
	Understand the basic components of an incident response process (Prepare, Identify, Contain, Eradicate, Recover, Lessons Learned)
	Understand the resources and processes used by the security monitoring tool; identify constraints, impacts to host or network systems, and required configurations to develop an implementation plan

X	**Skill** ***The reliable application of knowledge to achieve desired outcomes; skill is measured by the degree of reliability, from inconsistent to consistent.***
	Configure SIEM rules and alerts for unsupported devices such as those used in the power systems and Advanced Metering Infrastructure (AMI)
	Configure system against the baseline configuration manual
	Coordinate efforts with the vendor to develop an understanding of the component and security implications
	Develop a prioritized list of critical resources
	Develop configuration manuals on all custom solutions
	Develop possible attack techniques against specific technologies and implementations in your power systems deployments
	Document any changes made to the operating system, etc., for look-back opportunities should something malfunction
	Implement application (Layer 7) firewalls
	Implement penetration tests on deployed components
	Implement the multiple (layered) solution control options for mitigation
	Implement Web content filtering
	Scan for gaps in system configuration against a benchmark configuration manual
	Test the installation against the functional and performance requirements
	Verify that operating systems, services and applications are hardened in conjunction with regulatory guidance

X	**Ability** ***The application of skills to new domains; ability is measured by the extent of skill transfer, from narrow to broad.***
	Analyze vendor knowledge bases and DOE- and DHS-generated testing reports of known vulnerabilities of specific smart grid components
	Analyze vulnerabilities to determine risk based on how you have deployed the technology and the likelihood of exploitation
	Analyze vulnerability reports
	Communicate with suppliers and inventory the component supply chain
	Identify methods to detect vulnerabilities in power systems components with help from industry groups
	Monitor industry groups and forums so that you are able to obtain the latest information on security vulnerabilities related to power systems security components
	Prioritize systems within your network to determine which ones are of highest, moderate, and low impact value

E.2 Behavioral Interview Guideline Items: Secure Power Systems Intrusion Analyst

X	**Knowledge** ***The understanding of a concept, strategy, or procedure; knowledge is measured by depth of understanding, from shallow to deep.***
	Collect a sequence of events and continue to add information based on the investigation process
	Collect data from proxies and email systems to profile events involving malicious links or attachments and try to correlate to business process and assets
	Collect existing device configurations
	Collect issues to identify trends with particular vendors or manufacturers
	Review “healthy” log collection metrics to understand baseline from which to measure normal performance
	Review all internal incidents for the purposes of staying current in threats and how to best analyze them
	Review daily, weekly and monthly reports for systems that are not updating or are out of baseline with the rest of the system population
	Review logs, network captures, and traces
	Subscribe to vendor publications relevant to the product line installed
	Subscribe to vulnerability feeds and maintain information-sharing subscriptions
	Train Incident Response Team on information collection, analysis, and dissemination
	Train Incident Response Team on the usage of an attack technique table
	Train on information collection, analysis, and dissemination
	Train staff on the incident response program/plan
	Understand data classification levels and how to identify such levels with assets
	Understand how to run Wireshark and tcpdump
	Understand incident response, notification, and log handling requirements of business
	Understand NERC CIP and audit requirements

X	**Knowledge** ***The understanding of a concept, strategy, or procedure; knowledge is measured by depth of understanding, from shallow to deep.***
	Understand the basic components of an incident response process (Prepare, Identify, Contain, Eradicate, Recover, Lessons Learned)
	Understand the selected SIEM tool

X	**Skill** ***The reliable application of knowledge to achieve desired outcomes; skill is measured by the degree of reliability, from inconsistent to consistent.***
	Alert operators to events occurring so that they may increase system logging or retain logs, where normally such logs might be simply lost due to system storage constraints
	Assign significance to custom SIEM rules for unknown event types
	Configure rules for SIEM tools to capture and flag events known to be intrusion indicators
	Configure your security log management tool to sort and filter data in a manner that is best suited for the event being analyzed
	Configure your security log management tool to sort and filter data to best suit the event being analyzed
	Coordinate reactive and proactive responses
	Coordinate with administrators from other departments (i.e., networking, operating systems, servers) to identify strengths and weaknesses in the organization’s logging implementations
	Develop a prioritized list of critical resources
	Develop attack scenarios that might be used to intrude upon systems and networks and use tabletop exercises to gauge how personnel might respond in these situations
	Develop policy to determine which critical systems are to be monitored and to what level
	Escalate analysis findings in accordance with defined plan
	Maintain a current list of stakeholders’ contact information and cross-listing with respect to notification requirements
	Maintain chain of custody and integrity of log files if they are to be used by law enforcement at a later date
	Maintain documented procedures for analyzing logs and handling log archive
	Maintain professional credentials and networking relationships with professional organizations
	Maintain technical competence using industry tools for attacks (e.g., BackTrack Linux, Kali Linux)
	Test implementation with a testing regime to include events that should trigger alerts based on how the monitor has been configured
	Test incident response (IR) specialists to verify they maintain a current understanding of threats and how to analyze them
	Test the installation against the functional and performance requirements
	Update database of device configurations upon changes to configurations
	Update security tools (SIEM, intrusion detection system [IDS]/intrusion prevention systems [IPS], firewalls) with information pertinent to net tools or attacks

X	**Ability** ***The application of skills to new domains; ability is measured by the extent of skill transfer, from narrow to broad.***
	Analyze available logs and note gaps and time periods
	Analyze logs by correlating all suspect systems
	Analyze monitoring technique to determine whether newer technology better accomplishes the mission
	Analyze system configuration (for systems under attack) by correlating with the alerts generated to determine whether the alert is real or whether the IDS is "gone fishing"
	Analyze system logs for Network Time Protocol synchronization anomaly messages
	Analyze test results to make sure systems are functioning nominally
	Analyze vulnerabilities to determine risk based on how you have deployed the technology and the likelihood of exploitation
	Communicate with other analysts to "team work" larger incidents
	Identify external scanning needs that an internal scanner may not be able to adequately assess
	Identify threat actors
	Identify training material and information sources regarding cyber attacks and techniques
	Monitor for new systems installed on the network
	Monitor vulnerability reports
	Prioritize alerting after analysis into predefined buckets
	Report what was analyzed and the list of flagged events, key findings, issues, and actions taken
	Select a team of internal experts that should be consulted

E.3 Behavioral Interview Guideline Items: Secure Power Systems Incident Responder

X	**Knowledge** ***The understanding of a concept, strategy, or procedure; knowledge is measured by depth of understanding, from shallow to deep.***
	Collect a sequence of events and continue to add information based on the investigation process
	Collect issues to identify trends with particular vendors or manufacturers
	Collect necessary information for inclusion in the communications plan
	Subscribe to vendor publications relevant to the product line installed
	Subscribe to vulnerability feeds and maintain information-sharing subscriptions
	Understand how to run Wireshark and tcpdump
	Understand incident response process and initiate incident according to policies and procedures
	Understand incident response, notification, and log handling requirements of business
	Understand NERC CIP and audit requirements
	Understand the basic components of an incident response process (Prepare, Identify, Contain, Eradicate, Recover, Lessons Learned)
	Understand the selected SIEM tool
	Train Incident Response Team on information collection, analysis, and dissemination

X	**Knowledge** ***The understanding of a concept, strategy, or procedure; knowledge is measured by depth of understanding, from shallow to deep.***
	Train Incident Response Team on the usage of an attack technique table
	Train on information collection, analysis, and dissemination
	Train staff on the incident response program/plan

X	**Skill** ***The reliable application of knowledge to achieve desired outcomes; skill is measured by the degree of reliability, from inconsistent to consistent.***
	Alert operators to events occurring so that they may increase system logging or retain logs, where normally such logs might be simply lost due to system storage constraints
	Configure rules for SIEM tools to capture and flag events known to be intrusion indicators
	Coordinate notification strategies with other units, such as Compliance
	Coordinate reactive and proactive responses
	Coordinate with administrators from other departments (i.e., networking, operating systems, servers) to identify strengths and weaknesses in the organization's logging implementations
	Coordinate with other departments to make sure that routine business operations are not affected during testing
	Define security events and incidents with evaluation criteria
	Develop a prioritized list of critical resources
	Develop a schedule for testing elements of the incident response plan and organizations involved in the process
	Develop attack scenarios that might be used to intrude upon systems and networks and use tabletop exercises to gauge how personnel might respond in these situations
	Document all incident response exercises and test them
	Document call trees and reporting and coordinating procedures and supply them to all parties
	Document shortcomings and lessons learned from IR exercises and formulate action plans to make sure they are corrected as rapidly as possible
	Escalate analysis findings in accordance with defined plan
	Maintain a current list of stakeholders' contact information and cross-listing with respect to notification requirements
	Maintain a set of packaged scenarios with injects and data to exercise the response process
	Maintain chain of custody and integrity of log files if they are to be used by law enforcement at a later date
	Maintain documented procedures for analyzing logs and handling log archive
	Maintain professional credentials and networking relationships with professional organizations
	Maintain technical competence using industry tools for attacks (e.g., BackTrack Linux, Kali Linux)
	Test implementation with a testing regime to include events that should trigger alerts based on how the monitor has been configured
	Test IR specialists to verify they maintain a current understanding of threats and how to analyze them
	Update database of device configurations upon changes to configurations

X	**Ability** ***The application of skills to new domains; ability is measured by the extent of skill transfer, from narrow to broad.***
	Analyze all events and correlate to incidents if applicable
	Analyze logs by correlating all suspect systems
	Analyze monitoring technique to determine whether newer technology better accomplishes the mission
	Analyze test results to make sure systems are functioning nominally
	Assign significance to custom SIEM rules for unknown event types
	Communicate changes to user security tools and information regarding identified events and incidents
	Communicate with other analysts to “team work” larger incidents
	Identify threat actors
	Identify training material and information sources regarding cyber attacks and techniques
	Monitor all logs associated with third parties accessing your systems; this may require a manual review against historic use profiles
	Monitor vulnerability reports
	Report internal and external incident stakeholders involved during and after incident response
	Report status to management at defined stages of response per procedure
	Report what was analyzed and the list of flagged events, key findings, issues, and actions taken
	Review “healthy” log collection metrics to understand baseline from which to measure normal performance
	Review all internal incidents for the purposes of staying current in threats and how to best analyze them
	Select a team of internal experts that should be consulted

E.4 Behavioral Interview Guideline Items: Secure Power Security Operator

X	**Knowledge** ***The understanding of a concept, strategy, or procedure; knowledge is measured by depth of understanding, from shallow to deep.***
	Collect existing device configurations
	Collect issues to identify trends with particular vendors or manufacturers
	Collect vendor knowledge bases and DOE- and DHS-generated testing reports of known vulnerabilities of specific power systems components. Supplement that information with open-source reporting and internal red teaming or tabletop assessments
	Review all internal incidents for the purposes of staying current in threats and how to best analyze them
	Review checklist for implementing a device or system for necessary sign-offs
	Review daily, weekly and monthly reports for systems that are not updating or are out of baseline with the rest of the system population
	Review deployment plans and “as planned” configurations
	Review updates and version and confirm with vendor
	Subscribe to vendor publications relevant to the product line installed
	Subscribe to vulnerability feeds and maintain information-sharing subscriptions
	Understand data classification levels and how to identify such levels with assets

X	**Knowledge** ***The understanding of a concept, strategy, or procedure; knowledge is measured by depth of understanding, from shallow to deep.***
	Understand the environment (culture, personnel) to create a better relationship for transmitting delicate and sometimes poorly understood information
	Understand how to run Wireshark and tcpdump
	Understand incident response, notification, and log handling requirements of business
	Understand NERC CIP and audit requirements
	Understand the basic components of an incident response process (Prepare, Identify, Contain, Eradicate, Recover, Lessons Learned)
	Understand the resources and processes used by the security monitoring tool, identify constraints, impacts to host or network systems, and required configurations to develop an implementation plan
	Verify all devices are being submitted to SIEM for full network visibility
	Verify operating systems, services and applications are hardened in conjunction with regulatory guidance
	Verify system processes or states that are authorized for power systems components with the vendor to identify unauthorized processes
	Verify that all systems are logging to a central location

X	**Skill** ***The reliable application of knowledge to achieve desired outcomes; skill is measured by the degree of reliability, from inconsistent to consistent.***
	Alert end users of potential risks and vulnerabilities that they may be able to mitigate
	Configure rules for SIEM tools to capture and flag events known to be intrusion indicators
	Configure system against the baseline configuration manual
	Configure system technical policies that set thresholds and parameters for monitoring
	Configure your security log management tool to sort and filter data in a manner that is best suited for the event being analyzed
	Configure your security log management tool to sort and filter data to best suit the event being analyzed
	Coordinate efforts with the vendor to develop an understanding of the component and security implications
	Coordinate notification strategies with other units, such as Compliance
	Coordinate with administrators from other departments (i.e., networking, operating systems, servers) to identify strengths and weaknesses in the organization’s logging implementations
	Coordinate with network operations and system administrators to plan for the implementation and schedule required outages or notifications during the deployment
	Develop a prioritized list of critical resources
	Document deployment information in company asset management systems
	Implement penetration tests on deployed components
	Maintain a security configuration/coverage map of tools used across the enterprise
	Maintain an asset inventory of both hardware and software. Link this inventory to other security tools
	Maintain chain of custody and integrity of log files if they are to be used by law enforcement at a later date

X	**Skill** ***The reliable application of knowledge to achieve desired outcomes; skill is measured by the degree of reliability, from inconsistent to consistent.***
	Maintain documented procedures for analyzing logs and handling log archive
	Maintain professional credentials and networking relationships with professional organizations
	Maintain technical competence using industry tools for attacks (e.g., BackTrack Linux, Kali Linux)
	Scan for gaps in system configuration against a benchmark configuration manual
	Scan internal and external networks for new and unauthorized systems
	Test functionality after update to make sure system is operating
	Test implementation with a testing regime to include events that should trigger alerts based on how the monitor has been configured
	Test implementation with planned configurations to determine any deployment issues
	Test the installation against the functional and performance requirements
	Update database of device configurations upon changes to configurations
	Update security tools (SIEM, IDS/IPS, firewalls) with information pertinent to net tools or attacks

X	**Ability** ***The application of skills to new domains; ability is measured by the extent of skill transfer, from narrow to broad.***
	Analyze monitoring technique to determine whether newer technology better accomplishes the mission
	Analyze security device and application configurations for technical impacts (e.g., network congestion)
	Analyze test results to make sure systems are functioning nominally
	Analyze vulnerabilities to determine risk based on how you have deployed the technology and the likelihood of exploitation
	Analyze vulnerability reports
	Analyze which systems are being regularly scanned and which systems are being missed
	Assign significance to custom SIEM rules for unknown event types
	Communicate changes to user security tools and information regarding identified events and incidents
	Communicate with suppliers and inventory the component supply chain
	Decide on retirement of solutions that cannot handle abnormal network traffic
	Decide where to install security monitoring solutions such that the overall expense is minimized and the coverage is maximized
	Identify external scanning needs that an internal scanner may not be able to adequately assess
	Identify methods to detect vulnerabilities in power systems components with help from industry groups
	Monitor all logs associated with third parties accessing your systems; this may require a manual review against historic use profiles
	Monitor for new systems installed on the network
	Monitor industry groups and forums so that you are able to obtain the latest information on security vulnerabilities related to power systems security components
	Monitor vendor notifications for updates to software and signatures and compare against deployed

X	**Ability** ***The application of skills to new domains; ability is measured by the extent of skill transfer, from narrow to broad.***
	versions
	Monitor vulnerability reports
	Prioritize alerting after analysis into predefined buckets

E.5 References

43 FR 38290–38315. 1978. "Equal Employment Opportunity Commission, Civil Service Commission, Department of Labor and Department of Justice. Adoption by four agencies of Uniform Guidelines on Employee Selection Procedures." U.S. Department of Energy, *Federal Register*.

Arvey, RD. 1979. "Unfair discrimination in the employment interview: Legal and psychological aspects." *Psychological Bulletin*, 86(4):736–765.

Campion, MA, AA Fink, BJ Ruggenberg, L Carr, GM Phillips, and RB Odman. 2011. "Doing competencies well: Best practices in competency modeling." *Personnel Psychology*, 64:225–262.

Kesselman, GA and FE Lopez. 1979. "The impact of job analysis on employment test validation for minority and nonminority accounting personnel." *Personnel Psychology*, 32(1):91–108.

Pursell, ED, MA Campion, and SR Gaylord. 1980. "Structured interviewing: Avoiding selection problems." *Personnel Journal*, 59(11):907–912.

Tobey, DH. 2011. *A competency model of advanced threat response. ATR Working Group Report NBISE-ATR-11-02.* Idaho Falls, ID: National Board of Information Security Examiners.

Appendix F

Individual and Team Performance Guidelines

Appendix F

Individual and Team Performance Guidelines

The Individual/Team Performance Guidelines enable an “at-a-glance” view of the multidisciplinary and collaborative nature of Secure Power Systems Professional (SPSP) job roles. Phase I studied the skill sets of secure power systems operators, intrusion analysts, incident responders, and system engineers. These skill sets were mapped to stories of critical incidents (or *vignettes*); this afforded an enumeration of tasks required of each job role to effectively perform responsibilities to meet best-practice goals for that operation. Assignment of these tasks among the job roles, as either an individual responsibility or a collaborative responsibility, was validated during a job performance model analysis (O’Neil et al. 2012).

The job performance analysis identified thirteen master vignettes from the collection of critical incident stories. Many of these incidents shared a common set of job responsibilities and tasks. Therefore, the thirteen master vignettes identified in Phase I (O’Neil et al. 2012) have been reclassified into four vignette categories based on the tasks required to respond effectively to each event. The four discrete vignette groups are:

- Advanced Metering Infrastructure (AMI) Attacks
- Data Leakage and Related Attacks, including:
  - Network Attacks
  - Substation/Supervisory Control and Data Acquisition Attacks
  - Client-Side Attacks
  - Network Separation and Attack Paths
- Encryption and Phishing Incidents
- Incident Response and Log Management, including
  - Access Control Maintenance
  - Risk Management, Compliance and Audit
  - Threat and Vulnerability Management

Promoting Defensibility of Fair Hiring Practices

A primary goal for Phase III of the SPSP project was to produce resources that can guide human resources professionals, recruiters, and technical managers in workforce planning, staff recruitment and selection, performance evaluation, and training and development of SPSPs. The resources include:

- Recruitment and Career Development guides (see Appendix G)
- Job profiles (see Appendix D)
- Behavioral interview guidelines (see Appendix E).
- Individual and team performance guidelines (this appendix)

Developed in accordance with current best practices for competency modeling (Campion et al. 2011, these resources will support future development of assessment, certification, selection, and development programs that will meet standards established by the U.S. Equal Employment Opportunity Commission (EEOC) and the American National Standards Institute (ANSI). Research has shown that following these guidelines improves the legal defensibility of human resource practices (Arvey1979; 43 FR 38290-38315 1978; Kesselman and Lopez 1979; Pursell et al. 1980, Tobey 2011).

The Individual/Team Performance Guidelines may be used in part or in whole to align workforce capabilities with strategic goals and tactical focus of an organization. The primary objective of the guidelines was to provide a resource for recruiting and interviewing candidates for new position openings.

In addition, the Individual/Team Performance Guidelines have several other possible uses. First, the guidelines may be applied to develop performance reviews or to produce individual development programs for existing staff. Second, the guidelines may assist in specifying learning objectives for a training or education program. Finally, the guidelines may be easily incorporated into most human capital software to facilitate development of job descriptions that comply with guidelines established by the Society of Human Resource Management.

The team performance guidelines are an innovation of the SPSP project. The EEOC and ANSI require subject matter experts (SMEs) to map critical tasks to a job role to produce a validated job profile. Traditionally, in order to meet EEOC and ANSI requirements of psychometrically validated job profiles, critical tasks are mapped to a single job role. Phases I and II SMEs completed this mapping in accordance with the established methods at EEOC and ANSI. Clearly, organizational capability is the synergy of individual capabilities. While some critical tasks can be carried out by individuals, some tasks require the coordination and collaboration of a group of individuals working together on the same issue. Therefore, the SMEs mapped critical tasks and responsibilities for each job role to critical incidents, called vignettes. By mapping job roles to vignettes, it is possible to understand which tasks overlap between job roles, which can illustrate potential human resource gaps on the organizational level. The items shaded in gray indicate overlapping or team tasks. Furthermore, once overlapping tasks have been identified, the tasks unique to each job role are highlighted. Consequently, this mapping facilitates the fair evaluation of individuals who are working as part of a team.

How to Use This Guide

This appendix provides four team performance guidelines associated with the four vignette categories:

(F.1) AMI Attacks

(F.2) Data Leakage and Related Attacks

(F.3) Encryption and Phishing Incidents

(F.4) Incident Response Process and Log Management

Human resources professionals can use the information provided in the tables below to conduct a survey of the current employees to confirm whether their current staff has the specified knowledge, skill, or ability. Selection of specific vignettes and/or responsibilities for an open position may be made by a hiring manager based on the strategic focus and/or workforce competency gaps in their organization. A hiring manager can easily highlight areas of focus to include in their strategic or recruitment plan. The completed form may then be sent to a human resources professional or recruiter for development of existing recruitment and selection programs, enabling application of current organizational practices to the competency requirements necessary for successful job performance by Secure Power Systems Professionals.

NOTE: By distinguishing individual from collaborative tasks, a hiring process may ensure that candidate qualifications are evaluated fairly, based on tasks they will have accountability to perform, while also identifying the contributions they will need to make to team performance.

We envision that key individuals, including management and human resources professionals, would use the team performance guidelines as follows. First, they should review the vignettes and identify which of the vignette(s) represent the unique set of priorities for their organization. With the vignettes identified, human resources professionals conduct a survey of the current employees to confirm whether their current staff has the knowledge, skill, or ability to complete the task listed in the team performance guidelines. This will identify existing capabilities among current personnel. Knowledge of the gaps will inform strategic decisions such as hiring, professional training, and workforce development. For example, current staff could be trained to address the gaps, or the identified gaps can be used to focus recruitment and hiring processes.

F.6 Vignette: AMI Attacks

GOAL: Analyze log files for signs of an attack or compromise

RESPONSIBILITY: Make sure incident response and recovery procedures are tested regularly

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
Develop possible attack techniques against specific technologies and implementations in your power systems deployments	Alert end users of potential risks and vulnerabilities that they may be able to mitigate	Understand incident response process and initiate incident according to policies and procedures	
	Document deployment information in company asset management systems	Alert operators to events occurring so that they may increase system logging or retain logs, where normally such logs might be simply lost due to system storage constraints	Alert operators to events occurring so that they may increase system logging or retain logs, where normally such logs might be simply lost due to system storage constraints
	Maintain a security configuration/coverage map of tools used across the enterprise	Identify threat actors	Identify threat actors
	Understand incident response, notification, and log handling requirements of business	Understand incident response, notification, and log handling requirements of business	Understand incident response, notification, and log handling requirements of business
	Analyze test results to make sure systems are functioning nominally	Analyze test results to make sure systems are functioning nominally	Analyze test results to make sure systems are functioning nominally
	Maintain documented procedures for analyzing logs and handling log archive	Maintain documented procedures for analyzing logs and handling log archive	Maintain documented procedures for analyzing logs and handling log archive
	Maintain technical competence using industry tools for attacks (e.g., BackTrack Linux, Kali Linux)	Maintain technical competence using industry tools for attacks (e.g., BackTrack Linux, Kali Linux)	Maintain technical competence using industry tools for attacks (e.g., BackTrack Linux, Kali Linux)

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
	Test implementation with a testing regime to include events that should trigger alerts based on how the monitor has been configured	Test implementation with a testing regime to include events that should trigger alerts based on how the monitor has been configured	Test implementation with a testing regime to include events that should trigger alerts based on how the monitor has been configured
	Identify external scanning needs that an internal scanner may not be able to adequately assess	Coordinate with other departments to make sure that routine business operations are not affected during testing	Identify external scanning needs that an internal scanner may not be able to adequately assess
	Test the installation against the functional and performance requirements	Report status to management at defined stages of response per procedure	Test the installation against the functional and performance requirements
		Develop a schedule for testing elements of the incident response plan and organizations involved in the process	
		Document all incident response exercises and test them	
		Document shortcomings and lessons learned from incident response (IR) exercises and formulate action plans to make sure they are corrected as rapidly as possible	
		Escalate analysis findings in accordance with defined plan	
		Maintain a set of packaged scenarios with injects and data to exercise the response process	
		Report internal and external incident stakeholders involved during and after incident response	

RESPONSIBILITY: Make sure IR Specialist has been trained in latest threat analysis

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
		Develop attack scenarios that might be used to intrude upon systems and networks and use tabletop exercises to gauge how personnel might respond in these situations	Develop attack scenarios that might be used to intrude upon systems and networks and use tabletop exercises to gauge how personnel might respond in these situations
		Identify training material and information sources regarding cyber attacks and techniques	Identify training material and information sources regarding cyber attacks and techniques
		Review all internal incidents for the purposes of staying current in threats and how to best analyze them	Review all internal incidents for the purposes of staying current in threats and how to best analyze them
		Test IR specialists to verify they maintain a current understanding of threats and how to analyze them	Test IR specialists to verify they maintain a current understanding of threats and how to analyze them
		Train on information collection, analysis, and dissemination	Train on information collection, analysis, and dissemination
	Maintain technical competence using industry tools for attacks (e.g., BackTrack Linux, Kali Linux)	Maintain technical competence using industry tools for attacks (e.g., BackTrack Linux, Kali Linux)	Maintain technical competence using industry tools for attacks (e.g., BackTrack Linux, Kali Linux)

RESPONSIBILITY: Make sure log sources are time-synched to a local Network Time Protocol (NTP) server

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
	Configure system against the baseline configuration manual	Collect a sequence of events and continue to add information based on the investigation process	Analyze system logs for NTP synchronization anomaly messages
			Review logs, network captures, and traces

RESPONSIBILITY: Make sure Security Information and Event Management (SIEM) system is operating to expected functional and/or performance requirements

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
Configure SIEM rules and alerts for unsupported devices such as those used in power systems and AMI	Analyze security device and application configurations for technical impacts (e.g., network congestion)		
	Analyze which systems are being regularly scanned and which systems are being missed	Analyze logs by correlating all suspect systems	Analyze logs by correlating all suspect systems
	Analyze monitoring technique to determine whether newer technology better accomplishes the mission	Analyze monitoring technique to determine whether newer technology better accomplishes the mission	Analyze monitoring technique to determine whether newer technology better accomplishes the mission
	Assign significance to custom SIEM rules for unknown event types	Assign significance to custom SIEM rules for unknown event types	Assign significance to custom SIEM rules for unknown event types
	Configure system against the baseline configuration manual	Configure rules for SIEM tools to capture and flag events known to be intrusion indicators	Configure rules for SIEM tools to capture and flag events known to be intrusion indicators
	Configure system technical policies that set thresholds and parameters for monitoring	Review "healthy" log collection metrics to understand baseline from which to measure normal performance	Review "healthy" log collection metrics to understand baseline from which to measure normal performance
	Verify all devices are being submitted to SIEM for full network visibility	Understand the selected SIEM tool	Understand the selected SIEM tool
	Maintain an asset inventory of both hardware and software. Link this inventory to other security tools		
	Coordinate with network operations and system administrators to plan for the implementation and schedule required outages or notifications during the deployment		

GOAL: Investigate security events and analyze whether they are incidents

RESPONSIBILITY: Make sure sufficient artifacts are available

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
	Analyze which systems are being regularly scanned and which systems are being missed	Collect a sequence of events and continue to add information based on the investigation process	Review logs, network captures, and traces

RESPONSIBILITY: Make sure that personnel responsible for investigating security events understand what constitutes an actual event

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
	Communicate changes to user security tools and information regarding identified events and incidents	Maintain a current list of stakeholders' contact information and cross-listing with respect to notification requirements	
		Train staff on the incident response program/plan	
	Maintain professional credentials and networking relationships with professional organizations	Maintain professional credentials and networking relationships with professional organizations	Maintain professional credentials and networking relationships with professional organizations
	Maintain technical competence using industry tools for attacks (e.g., BackTrack Linux, Kali Linux)	Maintain technical competence using industry tools for attacks (e.g., BackTrack Linux, Kali Linux)	Maintain technical competence using industry tools for attacks (e.g., BackTrack Linux, Kali Linux)
	Prioritize alert after analysis into predefined buckets	Prioritize alert after analysis into predefined buckets	Prioritize alert after analysis into predefined buckets
		Select a team of internal experts that should be consulted	Select a team of internal experts that should be consulted
		Train Incident Response Team on the usage of an attack technique table	Train Incident Response Team on the usage of an attack technique table
		Train Incident Response Team on information collection, analysis, and dissemination	Train Incident Response Team on information collection, analysis, and dissemination

RESPONSIBILITY: Make sure the incident response plan is executed and followed

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
		Collect a sequence of events and continue to add information based on the investigation process	Analyze system logs for NTP synchronization anomaly messages
		Communicate with other analysts to “team work” larger incidents	Communicate with other analysts to “team work” larger incidents
		Report what was analyzed and the list of flagged events, key findings, issues, and actions taken	Report what was analyzed and the list of flagged events, key findings, issues, and actions taken
	Maintain chain of custody and integrity of log files if they are to be used by law enforcement at a later date	Maintain chain of custody and integrity of log files if they are to be used by law enforcement at a later date	Maintain chain of custody and integrity of log files if they are to be used by law enforcement at a later date
	Maintain documented procedures for analyzing logs and handling log archive	Maintain documented procedures for analyzing logs and handling log archive	Maintain documented procedures for analyzing logs and handling log archive
	Understand the basic components of an incident response process (Prepare, Identify, Contain, Eradicate, Recover, Lessons Learned)	Understand the basic components of an incident response process (Prepare, Identify, Contain, Eradicate, Recover, Lessons Learned)	Understand the basic components of an incident response process (Prepare, Identify, Contain, Eradicate, Recover, Lessons Learned)
		Coordinate reactive and proactive responses	
		Escalate analysis findings in accordance with defined plan	

RESPONSIBILITY: Make sure the security monitoring solution satisfies all organizational monitoring requirements

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
	Decide where to install security monitoring solutions such that the overall expense is minimized and the coverage is maximized		
	Maintain a security configuration/coverage map of tools used across the enterprise		
	Configure rules for SIEM tools to capture and flag events known to be intrusion indicators		Configure rules for SIEM tools to capture and flag events known to be intrusion indicators
	Configure your security log management tool to sort and filter data in a manner that is best suited for the event being analyzed		Configure your security log management tool to sort and filter data in a manner that is best suited for the event being analyzed
	Identify external scanning needs that an internal scanner may not be able to adequately assess		Identify external scanning needs that an internal scanner may not be able to adequately assess

GOAL: Maintain understanding of current attack tools, technologies, and techniques to compromise systems and intrude upon systems and networks

RESPONSIBILITY: Make sure company policies and procedures are followed for configuration management

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
Monitor industry groups and forums so that you are able to obtain the latest information on security vulnerabilities related to power systems security components	Monitor all logs associated with third parties accessing your systems; this may require a manual review against historic use profiles		
Identify methods to detect vulnerabilities in power systems components with help from industry groups	Develop a prioritized list of critical resources		Develop a prioritized list of critical resources

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
Collect vendor knowledge bases and U.S. Department of Energy (DOE)- and U.S. Department of Homeland Security (DHS)-generated testing reports of known vulnerabilities of specific power systems components. Supplement that information with open-source reporting and internal red teaming or tabletop assessments	Update database of device configurations upon changes to configurations		Update database of device configurations upon changes to configurations
	Monitor vulnerability reports	Monitor vulnerability reports	Monitor vulnerability reports

GOAL: Understand the security vulnerabilities of the power systems security components meters, headend, etc.

RESPONSIBILITY: Make sure communication plans are updated

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
		Collect necessary information for inclusion in the communications plan	
		Document call trees and reporting and coordinating procedures and supply them to all parties	

RESPONSIBILITY: Make sure that all employees, regardless of rank/role, are familiar with the most basic usages of office-wide security software, and know where to turn if an issue arises

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
	Communicate changes to user security tools and information regarding identified events and incidents	Document shortcomings and lessons learned from IR exercises and formulate action plans to make sure they are corrected as rapidly as possible	

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
	Coordinate with administrators from other departments (i.e., networking, operating systems, servers) to identify strengths and weaknesses in the organization's logging implementations		Coordinate with administrators from other departments (i.e., networking, operating systems, servers) to identify strengths and weaknesses in the organization's logging implementations

RESPONSIBILITY: Make sure that power system security components are put through an annual vulnerability assessment so that weaknesses can be identified

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
Analyze vulnerability reports	Monitor vulnerability reports	Monitor vulnerability reports	Monitor vulnerability reports
Analyze vulnerabilities to determine risk based on how you have deployed the technology and the likelihood of exploitation			
Implement penetration tests on deployed components			

RESPONSIBILITY: Make sure that you communicate with the vendors who make your power system components and request that they provide you with information related to vulnerabilities that they identify

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
Verify system processes or states that are authorized for power systems components with the vendor to identify unauthorized processes			Analyze vulnerabilities to determine risk based on how you have deployed the technology and the likelihood of exploitation
Communicate with suppliers and inventory the component supply chain			
Coordinate efforts with the vendor to develop an understanding of the component and security implications			

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
Understand the environment (culture, personnel) to create a better relationship for transmitting delicate and sometimes poorly understood information			
Understand the resources and processes used by the security monitoring tool, identify constraints, impacts to host or network systems, and required configurations to develop an implementation plan			

RESPONSIBILITY: Make sure vendors are contractually notifying you of exposures and security issues of interest

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
	Collect issues to identify trends with particular vendors or manufacturers		Collect issues to identify trends with particular vendors or manufacturers
	Subscribe to vendor publications relevant to the product line installed		Subscribe to vendor publications relevant to the product line installed
	Subscribe to vulnerability feeds and maintain information-sharing subscriptions		Subscribe to vulnerability feeds and maintain information-sharing subscriptions

F.7 Vignette: Data Leakage and Related Attacks

GOAL: Analyze log files for signs of an attack or compromise

RESPONSIBILITY: Make sure incident response and recovery procedures are tested regularly

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
Develop possible attack techniques against specific technologies and implementations in your power systems deployments	Alert end users of potential risks and vulnerabilities that they may be able to mitigate	Understand incident response process and initiate incident according to policies and procedures	
	Document deployment information in company asset management systems	Alert operators to events occurring so that they may increase system logging or retain logs, where normally such logs might be simply lost due to system storage constraints	Alert operators to events occurring so that they may increase system logging or retain logs, where normally such logs might be simply lost due to system storage constraints
	Maintain a security configuration/coverage map of tools used across the enterprise	Identify threat actors	Identify threat actors
	Understand incident response, notification, and log handling requirements of business	Understand incident response, notification, and log handling requirements of business	Understand incident response, notification, and log handling requirements of business
	Analyze test results to make sure systems are functioning nominally	Analyze test results to make sure systems are functioning nominally	Analyze test results to make sure systems are functioning nominally
	Maintain documented procedures for analyzing logs and handling log archive	Maintain documented procedures for analyzing logs and handling log archive	Maintain documented procedures for analyzing logs and handling log archive
	Maintain technical competence using industry tools for attacks (e.g., BackTrack Linux, Kali Linux)	Maintain technical competence using industry tools for attacks (e.g., BackTrack Linux, Kali Linux)	Maintain technical competence using industry tools for attacks (e.g., BackTrack Linux, Kali Linux)
	Test implementation with a testing regime to include events that should trigger alerts based on how the monitor has been configured	Test implementation with a testing regime to include events that should trigger alerts based on how the monitor has been configured	Test implementation with a testing regime to include events that should trigger alerts based on how the monitor has been configured

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
	Identify external scanning needs that an internal scanner may not be able to adequately assess	Coordinate with other departments to make sure that routine business operations are not affected during testing	Identify external scanning needs that an internal scanner may not be able to adequately assess
	Test the installation against the functional and performance requirements	Report status to management at defined stages of response per procedure	Test the installation against the functional and performance requirements
		Develop a schedule for testing elements of the incident response plan and organizations involved in the process	
		Document all incident response exercises and test them	
		Document shortcomings and lessons learned from IR exercises and formulate action plans to make sure they are corrected as rapidly as possible	
		Escalate analysis findings in accordance with defined plan	
		Maintain a set of packaged scenarios with injects and data to exercise the response process	
		Report internal and external incident stakeholders involved during and after incident response	

RESPONSIBILITY: Make sure IR Specialist has been trained in latest threat analysis

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
		Develop attack scenarios that might be used to intrude upon systems and networks and use tabletop exercises to gauge how personnel might respond in these situations	Develop attack scenarios that might be used to intrude upon systems and networks and use tabletop exercises to gauge how personnel might respond in these situations
		Identify training material and information sources regarding cyber attacks and techniques	Identify training material and information sources regarding cyber attacks and techniques
		Review all internal incidents for the purposes of staying current in threats and how to best analyze them	Review all internal incidents for the purposes of staying current in threats and how to best analyze them
		Test IR specialists to verify they maintain a current understanding of threats and how to analyze them	Test IR specialists to verify they maintain a current understanding of threats and how to analyze them
		Train on information collection, analysis, and dissemination	Train on information collection, analysis, and dissemination
	Maintain technical competence using industry tools for attacks (e.g., BackTrack Linux, Kali Linux)	Maintain technical competence using industry tools for attacks (e.g., BackTrack Linux, Kali Linux)	Maintain technical competence using industry tools for attacks (e.g., BackTrack Linux, Kali Linux)

RESPONSIBILITY: Make sure log sources are time-synched to a local NTP server

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
	Configure system against the baseline configuration manual	Collect a sequence of events and continue to add information based on the investigation process	Analyze system logs for NTP synchronization anomaly messages
			Review logs, network captures, and traces

RESPONSIBILITY: Make sure SIEM system is operating to expected functional and/or performance requirements

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
Configure SIEM rules and alerts for unsupported devices such as those used in the power systems and AMI	Analyze security device and application configurations for technical impacts (e.g., network congestion)		
	Analyze which systems are being regularly scanned and which systems are being missed	Analyze logs by correlating all suspect systems	Analyze logs by correlating all suspect systems
	Analyze monitoring technique to determine whether newer technology better accomplishes the mission	Analyze monitoring technique to determine whether newer technology better accomplishes the mission	Analyze monitoring technique to determine whether newer technology better accomplishes the mission
	Assign significance to custom SIEM rules for unknown event types	Assign significance to custom SIEM rules for unknown event types	Assign significance to custom SIEM rules for unknown event types
	Configure system against the baseline configuration manual	Configure rules for SIEM tools to capture and flag events known to be intrusion indicators	Configure rules for SIEM tools to capture and flag events known to be intrusion indicators
	Configure system technical policies that set thresholds and parameters for monitoring	Review “healthy” log collection metrics to understand baseline from which to measure normal performance	Review “healthy” log collection metrics to understand baseline from which to measure normal performance
	Verify all devices are being submitted to SIEM for full network visibility	Understand the selected SIEM tool	Understand the selected SIEM tool
	Maintain an asset inventory of both hardware and software. Link this inventory to other security tools		
	Coordinate with network operations and system administrators to plan for the implementation and schedule required outages or notifications during the deployment		

GOAL: Investigate security events and analyze whether they are incidents

RESPONSIBILITY: Make sure sufficient artifacts are available

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
	Analyze which systems are being regularly scanned and which systems are being missed	Collect a sequence of events and continue to add information based on the investigation process	Review logs, network captures, and traces

RESPONSIBILITY: Make sure that personnel responsible for investigating security events understand what constitutes an actual event

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
	Communicate changes to user security tools and information regarding identified events and incidents	Maintain a current list of stakeholders' contact information and cross-listing with respect to notification requirements	
		Train staff on the incident response program/plan	
	Maintain professional credentials and networking relationships with professional organizations	Maintain professional credentials and networking relationships with professional organizations	Maintain professional credentials and networking relationships with professional organizations
	Maintain technical competence using industry tools for attacks (e.g., BackTrack Linux, Kali Linux)	Maintain technical competence using industry tools for attacks (e.g., BackTrack Linux, Kali Linux)	Maintain technical competence using industry tools for attacks (e.g., BackTrack Linux, Kali Linux)
	Prioritize alert after analysis into predefined buckets	Prioritize alert after analysis into predefined buckets	Prioritize alert after analysis into predefined buckets
		Select a team of internal experts that should be consulted	Select a team of internal experts that should be consulted
		Train Incident Response Team on the usage of an attack technique table	Train Incident Response Team on the usage of an attack technique table
		Train Incident Response Team on information collection, analysis, and dissemination	Train Incident Response Team on information collection, analysis, and dissemination

RESPONSIBILITY: Make sure the incident response plan is executed and followed

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
		Collect a sequence of events and continue to add information based on the investigation process	Analyze system logs for NTP synchronization anomaly messages
		Communicate with other analysts to “team work” larger incidents	Communicate with other analysts to “team work” larger incidents
		Report what was analyzed and the list of flagged events, key findings, issues, and actions taken	Report what was analyzed and the list of flagged events, key findings, issues, and actions taken
	Maintain chain of custody and integrity of log files if they are to be used by law enforcement at a later date	Maintain chain of custody and integrity of log files if they are to be used by law enforcement at a later date	Maintain chain of custody and integrity of log files if they are to be used by law enforcement at a later date
	Maintain documented procedures for analyzing logs and handling log archive	Maintain documented procedures for analyzing logs and handling log archive	Maintain documented procedures for analyzing logs and handling log archive
	Understand the basic components of an incident response process (Prepare, Identify, Contain, Eradicate, Recover, Lessons Learned)	Understand the basic components of an incident response process (Prepare, Identify, Contain, Eradicate, Recover, Lessons Learned)	Understand the basic components of an incident response process (Prepare, Identify, Contain, Eradicate, Recover, Lessons Learned)
		Coordinate reactive and proactive responses	
		Escalate analysis findings in accordance with defined plan	

RESPONSIBILITY: Make sure the security monitoring solution satisfies all organizational monitoring requirements

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
	Decide where to install security monitoring solutions such that the overall expense is minimized and the coverage is maximized		
	Maintain a security configuration/coverage map of tools used across the enterprise		
	Configure rules for SIEM tools to capture and flag events known to be intrusion indicators		Configure rules for SIEM tools to capture and flag events known to be intrusion indicators
	Configure your security log management tool to sort and filter data in a manner that is best suited for the event being analyzed		Configure your security log management tool to sort and filter data in a manner that is best suited for the event being analyzed
	Identify external scanning needs that an internal scanner may not be able to adequately assess		Identify external scanning needs that an internal scanner may not be able to adequately assess

GOAL: Maintain understanding of current attack tools, technologies, and techniques to compromise systems and intrude upon systems and networks

RESPONSIBILITY: Make sure company policies and procedures are followed for configuration management

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
Monitor industry groups and forums so that you are able to obtain the latest information on security vulnerabilities related to power systems security components	Monitor all logs associated with third parties accessing your systems; this may require a manual review against historic use profiles		
Identify methods to detect vulnerabilities in power systems components with help from industry groups	Develop a prioritized list of critical resources		Develop a prioritized list of critical resources

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
Collect vendor knowledge bases and DOE- and DHS-generated testing reports of known vulnerabilities of specific power systems components. Supplement that information with open-source reporting and internal red teaming or tabletop assessments	Update database of device configurations upon changes to configurations		Update database of device configurations upon changes to configurations
	Monitor vulnerability reports	Monitor vulnerability reports	Monitor vulnerability reports

F.8 Vignette: Encryption and Phishing Incidents

GOAL: Investigate security events and analyze whether they are incidents

RESPONSIBILITY: Make sure sufficient artifacts are available

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
	Analyze which systems are being regularly scanned and which systems are being missed	Collect a sequence of events and continue to add information based on the investigation process	Review logs, network captures, and traces

RESPONSIBILITY: Make sure that personnel responsible for investigating security events understand what constitutes an actual event

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
	Communicate changes to user security tools and information regarding identified events and incidents	Maintain a current list of stakeholders’ contact information and cross-listing with respect to notification requirements	

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
		Train staff on the incident response program/plan	
	Maintain professional credentials and networking relationships with professional organizations	Maintain professional credentials and networking relationships with professional organizations	Maintain professional credentials and networking relationships with professional organizations
	Maintain technical competence using industry tools for attacks (e.g., BackTrack Linux, Kali Linux)	Maintain technical competence using industry tools for attacks (e.g., BackTrack Linux, Kali Linux)	Maintain technical competence using industry tools for attacks (e.g., BackTrack Linux, Kali Linux)
	Prioritize alert after analysis into predefined buckets	Prioritize alert after analysis into predefined buckets	Prioritize alert after analysis into predefined buckets
		Select a team of internal experts that should be consulted	Select a team of internal experts that should be consulted
		Train Incident Response Team on the usage of an attack technique table	Train Incident Response Team on the usage of an attack technique table
		Train Incident Response Team on information collection, analysis, and dissemination	Train Incident Response Team on information collection, analysis, and dissemination

RESPONSIBILITY: Make sure the incident response plan is executed and followed

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
		Collect a sequence of events and continue to add information based on the investigation process	Analyze system logs for NTP synchronization anomaly messages
		Communicate with other analysts to “team work” larger incidents	Communicate with other analysts to “team work” larger incidents
		Report what was analyzed and the list of flagged events, key findings, issues, and actions taken	Report what was analyzed and the list of flagged events, key findings, issues, and actions taken
	Maintain chain of custody and integrity of log files if they are to be used by law enforcement at a later date	Maintain chain of custody and integrity of log files if they are to be used by law enforcement at a later date	Maintain chain of custody and integrity of log files if they are to be used by law enforcement at a later date

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
	Maintain documented procedures for analyzing logs and handling log archive	Maintain documented procedures for analyzing logs and handling log archive	Maintain documented procedures for analyzing logs and handling log archive
	Understand the basic components of an incident response process (Prepare, Identify, Contain, Eradicate, Recover, Lessons Learned)	Understand the basic components of an incident response process (Prepare, Identify, Contain, Eradicate, Recover, Lessons Learned)	Understand the basic components of an incident response process (Prepare, Identify, Contain, Eradicate, Recover, Lessons Learned)
		Coordinate reactive and proactive responses	
		Escalate analysis findings in accordance with defined plan	

RESPONSIBILITY: Make sure the security monitoring solution satisfies all organizational monitoring requirements

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
	Decide where to install security monitoring solutions such that the overall expense is minimized and the coverage is maximized		
	Maintain a security configuration/coverage map of tools used across the enterprise		
	Configure rules for SIEM tools to capture and flag events known to be intrusion indicators		Configure rules for SIEM tools to capture and flag events known to be intrusion indicators
	Configure your security log management tool to sort and filter data in a manner that is best suited for the event being analyzed		Configure your security log management tool to sort and filter data in a manner that is best suited for the event being analyzed
	Identify external scanning needs that an internal scanner may not be able to adequately assess		Identify external scanning needs that an internal scanner may not be able to adequately assess

GOAL: Maintain understanding of current attack tools, technologies, and techniques to compromise systems and intrude upon systems and networks

RESPONSIBILITY: Make sure company policies and procedures are followed for configuration management

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
Monitor industry groups and forums so that you are able to obtain the latest information on security vulnerabilities related to power systems security components	Monitor all logs associated with third parties accessing your systems; this may require a manual review against historic use profiles		
Identify methods to detect vulnerabilities in power systems components with help from industry groups	Develop a prioritized list of critical resources		Develop a prioritized list of critical resources
Collect vendor knowledge bases and DOE- and DHS-generated testing reports of known vulnerabilities of specific power systems components. Supplement that information with open-source reporting and internal red teaming or tabletop assessments	Update database of device configurations upon changes to configurations		Update database of device configurations upon changes to configurations
	Monitor vulnerability reports	Monitor vulnerability reports	Monitor vulnerability reports

F.9 Vignette: Incident Response Process and Log Management

GOAL: Analyze log files for signs of an attack or compromise

RESPONSIBILITY: Make sure incident response and recovery procedures are tested regularly

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
Develop possible attack techniques against specific technologies and implementations in your power systems deployments	Alert end users of potential risks and vulnerabilities that they may be able to mitigate	Understand incident response process and initiate incident according to policies and procedures	
	Document deployment information in company asset management systems	Alert operators to events occurring so that they may increase system logging or retain logs, where normally such logs might be simply lost due to system storage constraints	Alert operators to events occurring so that they may increase system logging or retain logs, where normally such logs might be simply lost due to system storage constraints
	Maintain a security configuration/coverage map of tools used across the enterprise	Identify threat actors	Identify threat actors
	Understand incident response, notification, and log handling requirements of business	Understand incident response, notification, and log handling requirements of business	Understand incident response, notification, and log handling requirements of business
	Analyze test results to make sure systems are functioning nominally	Analyze test results to make sure systems are functioning nominally	Analyze test results to make sure systems are functioning nominally
	Maintain documented procedures for analyzing logs and handling log archive	Maintain documented procedures for analyzing logs and handling log archive	Maintain documented procedures for analyzing logs and handling log archive
	Maintain technical competence using industry tools for attacks (e.g., BackTrack Linux, Kali Linux)	Maintain technical competence using industry tools for attacks (e.g., BackTrack Linux, Kali Linux)	Maintain technical competence using industry tools for attacks (e.g., BackTrack Linux, Kali Linux)
	Review all internal incidents for the purposes of staying current in threats and how to best analyze them	Review all internal incidents for the purposes of staying current in threats and how to best analyze them	Review all internal incidents for the purposes of staying current in threats and how to best analyze them

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
	Test implementation with a testing regime to include events that should trigger alerts based on how the monitor has been configured	Test implementation with a testing regime to include events that should trigger alerts based on how the monitor has been configured	Test implementation with a testing regime to include events that should trigger alerts based on how the monitor has been configured
	Identify external scanning needs that an internal scanner may not be able to adequately assess	Coordinate with other departments to make sure that routine business operations are not affected during testing	Identify external scanning needs that an internal scanner may not be able to adequately assess
	Test the installation against the functional and performance requirements	Report status to management at defined stages of response per procedure	Test the installation against the functional and performance requirements
		Develop a schedule for testing elements of the incident response plan and organizations involved in the process	
		Document all incident response exercises and test them	
		Document shortcomings and lessons learned from IR exercises and formulate action plans to make sure they are corrected as rapidly as possible	
		Escalate analysis findings in accordance with defined plan	
		Maintain a set of packaged scenarios with injects and data to exercise the response process	
		Report internal and external incident stakeholders involved during and after incident response	

RESPONSIBILITY: Make sure IR Specialist has been trained in latest threat analysis

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
	Understand how to run Wireshark and tcpdump	Understand how to run Wireshark and tcpdump	Understand how to run Wireshark and tcpdump
	Maintain technical competence using industry tools for attacks (e.g., BackTrack Linux, Kali Linux)	Maintain technical competence using industry tools for attacks (e.g., BackTrack Linux, Kali Linux)	Maintain technical competence using industry tools for attacks (e.g., BackTrack Linux, Kali Linux)
		Develop attack scenarios that might be used to intrude upon systems and networks and use tabletop exercises to gauge how personnel might respond in these situations	Develop attack scenarios that might be used to intrude upon systems and networks and use tabletop exercises to gauge how personnel might respond in these situations
		Identify training material and information sources regarding cyber attacks and techniques	Identify training material and information sources regarding cyber attacks and techniques
		Review all internal incidents for the purposes of staying current in threats and how to best analyze them	Review all internal incidents for the purposes of staying current in threats and how to best analyze them
		Test IR specialists to verify they maintain a current understanding of threats and how to analyze them	Test IR specialists to verify they maintain a current understanding of threats and how to analyze them
		Train on information collection, analysis, and dissemination	Train on information collection, analysis, and dissemination

RESPONSIBILITY: Make sure log sources are time-synched to a local NTP server

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
	Configure system against the baseline configuration manual	Collect a sequence of events and continue to add information based on the investigation process	Analyze system logs for NTP synchronization anomaly messages
			Review logs, network captures, and traces

RESPONSIBILITY: Make sure SIEM system is operating to expected functional and/or performance requirements

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
Configure SIEM rules and alerts for unsupported devices such as those used in the power systems and AMI	Analyze security device and application configurations for technical impacts (e.g., network congestion)		
	Analyze which systems are being regularly scanned and which systems are being missed	Analyze logs by correlating all suspect systems	Analyze logs by correlating all suspect systems
	Analyze monitoring technique to determine whether newer technology better accomplishes the mission	Analyze monitoring technique to determine whether newer technology better accomplishes the mission	Analyze monitoring technique to determine whether newer technology better accomplishes the mission
	Assign significance to custom SIEM rules for unknown event types	Assign significance to custom SIEM rules for unknown event types	Assign significance to custom SIEM rules for unknown event types
	Configure system against the baseline configuration manual	Configure rules for SIEM tools to capture and flag events known to be intrusion indicators	Configure rules for SIEM tools to capture and flag events known to be intrusion indicators
	Configure system technical policies that set thresholds and parameters for monitoring	Review "healthy" log collection metrics to understand baseline from which to measure normal performance	Review "healthy" log collection metrics to understand baseline from which to measure normal performance
	Verify all devices are being submitted to SIEM for full network visibility	Understand the selected SIEM tool	Understand the selected SIEM tool
	Maintain an asset inventory of both hardware and software. Link this inventory to other security tools		
	Coordinate with network operations and system administrators to plan for the implementation and schedule required outages or notifications during the deployment		

GOAL: Install security monitoring solutions

RESPONSIBILITY: Make sure adequate budget has been apportioned for the monitoring solution

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
Access an up-to-date power systems inventory and asset list	Alert end users of potential risks and vulnerabilities that they may be able to mitigate	Alert operators to events occurring so that they may increase system logging or retain logs, where normally such logs might be simply lost due to system storage constraints	Alert operators to events occurring so that they may increase system logging or retain logs, where normally such logs might be simply lost due to system storage constraints
Develop a prioritized list of critical resources	Develop a prioritized list of critical resources		Develop a prioritized list of critical resources
		Review "healthy" log collection metrics to understand baseline from which to measure normal performance	Review "healthy" log collection metrics to understand baseline from which to measure normal performance

RESPONSIBILITY: Make sure all solutions being installed have been authorized

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
Analyze vendor knowledge bases and DOE- and DHS-generated testing reports of known vulnerabilities of specific smart grid components	Analyze security device and application configurations for technical impacts (e.g., network congestion)	Coordinate with other departments to make sure that routine business operations are not affected during testing	
Configure system against the baseline configuration manual	Configure system against the baseline configuration manual		
Verify operating systems, services and applications are hardened in conjunction with regulatory guidance	Verify operating systems, services and applications are hardened in conjunction with regulatory guidance		
Scan for gaps in system configuration against a benchmark configuration manual	Scan for gaps in system configuration against a benchmark configuration manual		Scan for gaps in system configuration against a benchmark configuration manual
Test the installation against the functional and performance requirements	Test the installation against the functional and performance requirements		Test the installation against the functional and performance requirements

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
Implement application (Layer 7) firewalls	Identify external scanning needs that an internal scanner may not be able to adequately assess		Identify external scanning needs that an internal scanner may not be able to adequately assess
Implement the multiple (layered) solution control options for mitigation	Monitor for new systems installed on the network		Monitor for new systems installed on the network
Implement Web content filtering	Scan internal and external networks for new and unauthorized systems		Scan internal and external networks for new and unauthorized systems
	Update database of device configurations upon changes to configurations		Update database of device configurations upon changes to configurations
	Coordinate with network operations and system administrators to plan for the implementation and schedule required outages or notifications during the deployment		
	Document deployment information in company asset management systems		
	Review checklist for implementing a device or system for necessary sign-offs		
	Review deployment plans and “as planned” configurations		
	Test implementation with planned configurations to determine any deployment issues		
	Verify all devices are being submitted to SIEM for full network visibility		

RESPONSIBILITY: Make sure monitoring solution is configured correctly to obtain vendor software and signature updates

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
Document any changes made to the operating system, etc., for look-back opportunities should something malfunction	Configure system technical policies that set thresholds and parameters for monitoring	Report what was analyzed and the list of flagged events, key findings, issues, and actions taken	Report what was analyzed and the list of flagged events, key findings, issues, and actions taken
Establish a test lab where tools can be practiced and learned	Decide on retirement of solutions that cannot handle abnormal network traffic	Test IR specialists to verify they maintain a current understanding of threats and how to analyze them	Test IR specialists to verify they maintain a current understanding of threats and how to analyze them
Test the installation against the functional and performance requirements	Test the installation against the functional and performance requirements		Test the installation against the functional and performance requirements
Verify operating systems, services and applications are hardened in conjunction with regulatory guidance	Analyze monitoring technique to determine whether newer technology better accomplishes the mission	Analyze monitoring technique to determine whether newer technology better accomplishes the mission	Analyze monitoring technique to determine whether newer technology better accomplishes the mission
	Assign significance to custom SIEM rules for unknown event types	Assign significance to custom SIEM rules for unknown event types	Assign significance to custom SIEM rules for unknown event types
	Test implementation with a testing regime to include events that should trigger alerts based on how the monitor has been configured	Test implementation with a testing regime to include events that should trigger alerts based on how the monitor has been configured	Test implementation with a testing regime to include events that should trigger alerts based on how the monitor has been configured
	Collect issues to identify trends with particular vendors or manufacturers		Collect issues to identify trends with particular vendors or manufacturers
	Review daily, weekly and monthly reports for systems that are not updating/are out of baseline with the rest of the system population		Review daily, weekly and monthly reports for systems that are not updating or are out of baseline with the rest of the system population
	Subscribe to vendor publications relevant to the product line installed		Subscribe to vendor publications relevant to the product line installed
	Update security tools (SIEM, intrusion detection system (IDS)/Intrusion Prevention Systems, firewalls) with information pertinent to net tools or attacks		Update security tools (SIEM, IDS/ Intrusion Prevention Systems, firewalls) with information pertinent to net tools or attacks

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
	Decide where to install security monitoring solutions such that the overall expense is minimized and the coverage is maximized		
	Review checklist for implementing a device or system for necessary sign-offs		
	Review updates and version and confirm with vendor		
	Test functionality after update to make sure system is operating		
	Update database of device configurations upon changes to configurations		

RESPONSIBILITY: Make sure that a methodology has been established for evaluating alert types and that those thresholds are programmed into the security monitoring solution by impact level

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
Understand North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) and audit requirements	Understand NERC CIP and audit requirements	Understand NERC CIP and audit requirements	Understand NERC CIP and audit requirements
Document any changes made to the operating system, etc., for look-back opportunities should something malfunction	Coordinate notification strategies with other units, such as Compliance	Coordinate notification strategies with other units, such as Compliance	Analyze system configuration (for systems under attack) by correlating with the alerts generated to determine whether the alert is real or whether the IDS is “gone fishing”
Establish a test lab where tools can be practiced and learned		Escalate analysis findings in accordance with defined plan	Develop policy to determine which critical systems are to be monitored and to what level

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
Prioritize systems within your network to determine which ones are of highest, moderate, and low impact value	Prioritize alerting after analysis into predefined buckets	Prioritize alerting after analysis into predefined buckets	Prioritize alerting after analysis into predefined buckets
Develop possible attack techniques against specific technologies and implementations in your power systems deployments	Understand incident response, notification, and log handling requirements of business	Understand incident response, notification, and log handling requirements of business	Understand incident response, notification, and log handling requirements of business
	Configure rules for SIEM tools to capture and flag events known to be intrusion indicators		Configure rules for SIEM tools to capture and flag events known to be intrusion indicators
	Configure your security log management tool to sort and filter data to best suit the event being analyzed		Configure your security log management tool to sort and filter data to best suit the event being analyzed
	Coordinate with administrators from other departments (i.e., networking, operating systems, servers) to identify strengths and weaknesses in the organization’s logging implementations		Coordinate with administrators from other departments (i.e., networking, operating systems, servers) to identify strengths and weaknesses in the organization’s logging implementations

RESPONSIBILITY: Make sure that all assets that require monitoring are logging to the security monitoring solution and that you are able to identify each asset that is supposed to be logging

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
Scan for gaps in system configuration against a benchmark configuration manual	Monitor vendor notifications for updates to software and signatures and compare against deployed versions		Analyze available logs and note gaps and time periods
Test the installation against the functional and performance requirements	Verify all devices are being submitted to SIEM for full network visibility		Collect data from proxies and email systems to profile events involving malicious links or attachments and try to correlate to business process and assets
	Verify that all systems are logging to a central location		

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
	Collect existing device configurations		Collect existing device configurations
	Collect issues to identify trends with particular vendors or manufacturers		Collect issues to identify trends with particular vendors or manufacturers

RESPONSIBILITY: Make sure that all employees, regardless of rank/role, are familiar with the most basic usages of office-wide security software, and know where to turn if an issue arises

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
Understand the basic components of an incident response process (Prepare, Identify, Contain, Eradicate, Recover, Lessons Learned)	Understand the basic components of an incident response process (Prepare, Identify, Contain, Eradicate, Recover, Lessons Learned)	Understand the basic components of an incident response process (Prepare, Identify, Contain, Eradicate, Recover, Lessons Learned)	Understand the basic components of an incident response process (Prepare, Identify, Contain, Eradicate, Recover, Lessons Learned)
Develop configuration manuals on all custom solutions	Communicate changes to user security tools and information regarding identified events and incidents	Document shortcomings and lessons learned from IR exercises and formulate action plans to make sure they are corrected as rapidly as possible	
	Coordinate with administrators from other departments (i.e., networking, operating systems, servers) to identify strengths and weaknesses in the organization's logging implementations		Coordinate with administrators from other departments (i.e., networking, operating systems, servers) to identify strengths and weaknesses in the organization's logging implementations

RESPONSIBILITY: Make sure that security event types have been defined by classification

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
	Understand data classification levels and how to identify such levels with assets	Analyze all events and correlate to incidents if applicable	Understand data classification levels and how to identify such levels with assets
		Define security events and incidents with evaluation criteria	

GOAL: Investigate security events and analyze whether they are incidents

RESPONSIBILITY: Make sure sufficient artifacts are available

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
	Analyze which systems are being regularly scanned and which systems are being missed	Collect a sequence of events and continue to add information based on the investigation process	Review logs, network captures, and traces

RESPONSIBILITY: Make sure that personnel responsible for investigating security events understand what constitutes an actual event

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
	Communicate changes to user security tools and information regarding identified events and incidents	Maintain a current list of stakeholders' contact information and cross-listing with respect to notification requirements	
		Train staff on the incident response program/plan	
	Maintain professional credentials and networking relationships with professional organizations	Maintain professional credentials and networking relationships with professional organizations	Maintain professional credentials and networking relationships with professional organizations
	Maintain technical competence using industry tools for attacks (e.g., BackTrack Linux, Kali Linux)	Maintain technical competence using industry tools for attacks (e.g., BackTrack Linux, Kali Linux)	Maintain technical competence using industry tools for attacks (e.g., BackTrack Linux, Kali Linux)
	Prioritize alert after analysis into predefined buckets	Prioritize alert after analysis into predefined buckets	Prioritize alert after analysis into predefined buckets
		Select a team of internal experts that should be consulted	Select a team of internal experts that should be consulted
		Train Incident Response Team on the usage of an attack technique table	Train Incident Response Team on the usage of an attack technique table
		Train Incident Response Team on information collection, analysis, and dissemination	Train Incident Response Team on information collection, analysis, and dissemination

RESPONSIBILITY: Make sure the incident response plan is executed and followed

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
		Collect a sequence of events and continue to add information based on the investigation process	Analyze system logs for NTP synchronization anomaly messages
		Communicate with other analysts to “team work” larger incidents	Communicate with other analysts to “team work” larger incidents
		Report what was analyzed and the list of flagged events, key findings, issues, and actions taken	Report what was analyzed and the list of flagged events, key findings, issues, and actions taken
	Maintain chain of custody and integrity of log files if they are to be used by law enforcement at a later date	Maintain chain of custody and integrity of log files if they are to be used by law enforcement at a later date	Maintain chain of custody and integrity of log files if they are to be used by law enforcement at a later date
	Maintain documented procedures for analyzing logs and handling log archive	Maintain documented procedures for analyzing logs and handling log archive	Maintain documented procedures for analyzing logs and handling log archive
	Understand the basic components of an incident response process (Prepare, Identify, Contain, Eradicate, Recover, Lessons Learned)	Understand the basic components of an incident response process (Prepare, Identify, Contain, Eradicate, Recover, Lessons Learned)	Understand the basic components of an incident response process (Prepare, Identify, Contain, Eradicate, Recover, Lessons Learned)
		Coordinate reactive and proactive responses	
		Escalate analysis findings in accordance with defined plan	

RESPONSIBILITY: Make sure the security monitoring solution satisfies all organizational monitoring requirements

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
	Decide where to install security monitoring solutions such that the overall expense is minimized and the coverage is maximized		
	Maintain a security configuration/coverage map of tools used across the enterprise		
	Configure rules for SIEM tools to capture and flag events known to be intrusion indicators		Configure rules for SIEM tools to capture and flag events known to be intrusion indicators
	Configure your security log management tool to sort and filter data in a manner that is best suited for the event being analyzed		Configure your security log management tool to sort and filter data in a manner that is best suited for the event being analyzed
	Identify external scanning needs that an internal scanner may not be able to adequately assess		Identify external scanning needs that an internal scanner may not be able to adequately assess

GOAL: Maintain understanding of current attack tools, technologies, and techniques to compromise systems and intrude upon systems and networks

RESPONSIBILITY: Make sure company policies and procedures are followed for configuration management

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
Monitor industry groups and forums so that you are able to obtain the latest information on security vulnerabilities related to power systems security components	Monitor all logs associated with third parties accessing your systems; this may require a manual review against historic use profiles		
Identify methods to detect vulnerabilities in power systems components with help from industry groups	Develop a prioritized list of critical resources		Develop a prioritized list of critical resources

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
Collect vendor knowledge bases and DOE- and DHS-generated testing reports of known vulnerabilities of specific power systems components. Supplement that information with open-source reporting and internal red teaming or tabletop assessments	Update database of device configurations upon changes to configurations		Update database of device configurations upon changes to configurations
	Monitor vulnerability reports	Monitor vulnerability reports	Monitor vulnerability reports

F.10 References

43 FR 38290–38315. 1978. “Equal Employment Opportunity Commission, Civil Service Commission, Department of Labor and Department of Justice. Adoption by four agencies of Uniform Guidelines on Employee Selection Procedures.” U.S. Department of Energy, *Federal Register*.

Arvey, RD. 1979. “Unfair discrimination in the employment interview: Legal and psychological aspects.” *Psychological Bulletin*, 86(4):736–765.

Campion, MA, AA Fink, BJ Ruggenberg, L Carr, GM Phillips, and RB Odman. 2011. “Doing competencies well: Best practices in competency modeling.” *Personnel Psychology*, 64:225–262.

Kesselman, GA and FE Lopez. 1979. “The impact of job analysis on employment test validation for minority and nonminority accounting personnel.” *Personnel Psychology*, 32(1):91–108.

O’Neil, LR, MJ Assante, and DH Tobey. 2012. *Smart Grid Cybersecurity: Job Performance Model Report* (Technical Report No. PNNL-21639). Alexandria, VA: National Technical Information Service.

Pursell, ED, MA Campion, and SR Gaylord. 1980. “Structured interviewing: Avoiding selection problems.” *Personnel Journal*, 59(11):907–912.

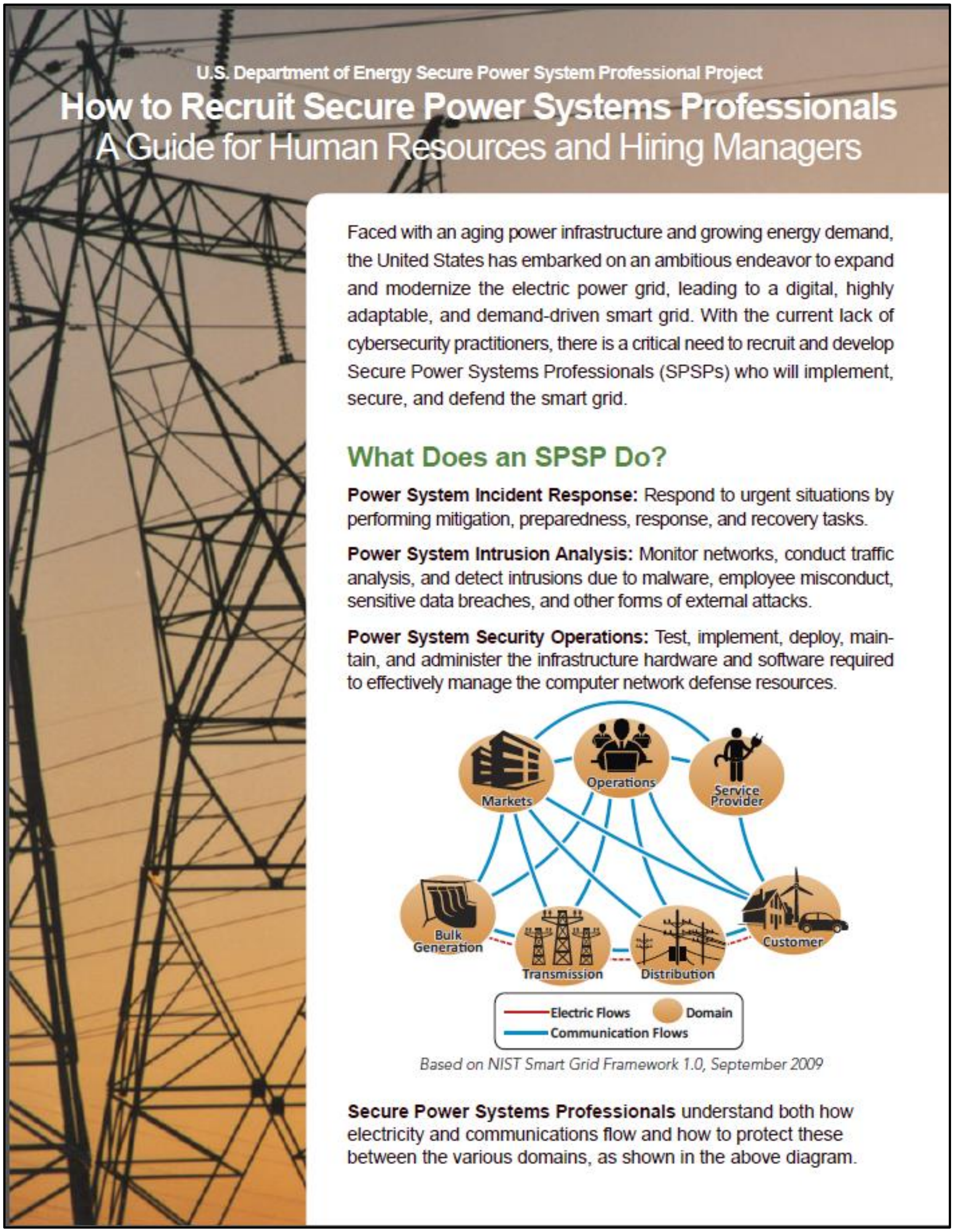
Tobey, DH. 2011. *A competency model of advanced threat response. ATR Working Group Report NBISE-ATR-11-02.* Idaho Falls, ID: National Board of Information Security Examiners.

Appendix G

Guides for Hiring and Developing Secure Power Systems Professionals

Appendix G

Guides for Hiring and Developing Secure Power Systems Professionals



U.S. Department of Energy Secure Power System Professional Project

How to Recruit Secure Power Systems Professionals

A Guide for Human Resources and Hiring Managers

Faced with an aging power infrastructure and growing energy demand, the United States 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, there is a critical need to recruit and develop Secure Power Systems Professionals (SPSPs) who will implement, secure, and defend the smart grid.

What Does an SPSP Do?

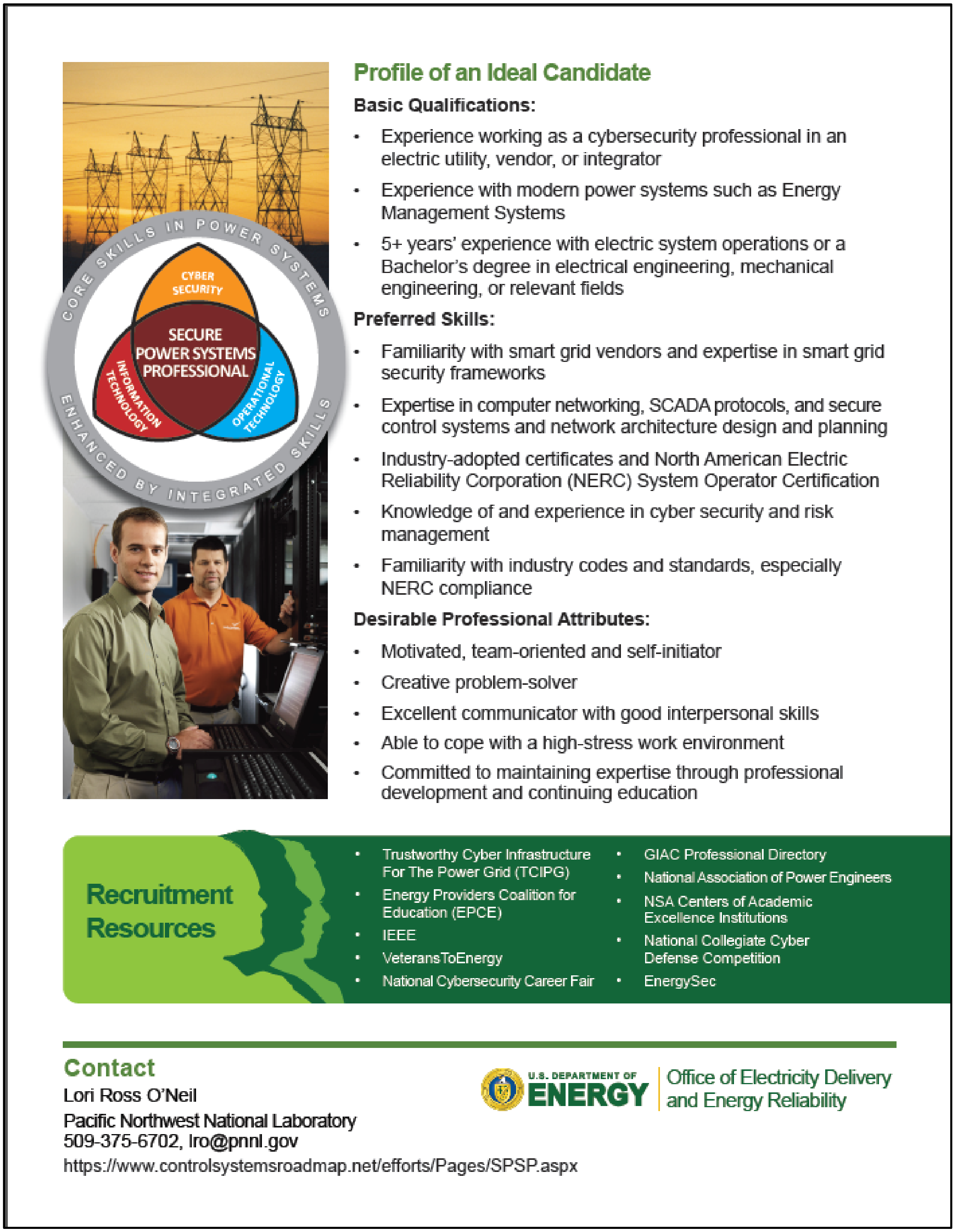
Power System Incident Response: Respond to urgent situations by performing mitigation, preparedness, response, and recovery tasks.

Power System Intrusion Analysis: Monitor networks, conduct traffic analysis, and detect intrusions due to malware, employee misconduct, sensitive data breaches, and other forms of external attacks.

Power System Security Operations: Test, implement, deploy, maintain, and administer the infrastructure hardware and software required to effectively manage the computer network defense resources.

Based on NIST Smart Grid Framework 1.0, September 2009

Secure Power Systems Professionals understand both how electricity and communications flow and how to protect these between the various domains, as shown in the above diagram.


CORE SKILLS IN POWER SYSTEMS
ENHANCED BY INTEGRATED SKILLS
CYBER SECURITY
SECURE POWER SYSTEMS PROFESSIONAL
INFORMATION TECHNOLOGY
OPERATIONAL TECHNOLOGY

Profile of an Ideal Candidate

Basic Qualifications:

- Experience working as a cybersecurity professional in an electric utility, vendor, or integrator
- Experience with modern power systems such as Energy Management Systems
- 5+ years' experience with electric system operations or a Bachelor's degree in electrical engineering, mechanical engineering, or relevant fields

Preferred Skills:

- Familiarity with smart grid vendors and expertise in smart grid security frameworks
- Expertise in computer networking, SCADA protocols, and secure control systems and network architecture design and planning
- Industry-adopted certificates and North American Electric Reliability Corporation (NERC) System Operator Certification
- Knowledge of and experience in cyber security and risk management
- Familiarity with industry codes and standards, especially NERC compliance

Desirable Professional Attributes:

- Motivated, team-oriented and self-initiator
- Creative problem-solver
- Excellent communicator with good interpersonal skills
- Able to cope with a high-stress work environment
- Committed to maintaining expertise through professional development and continuing education

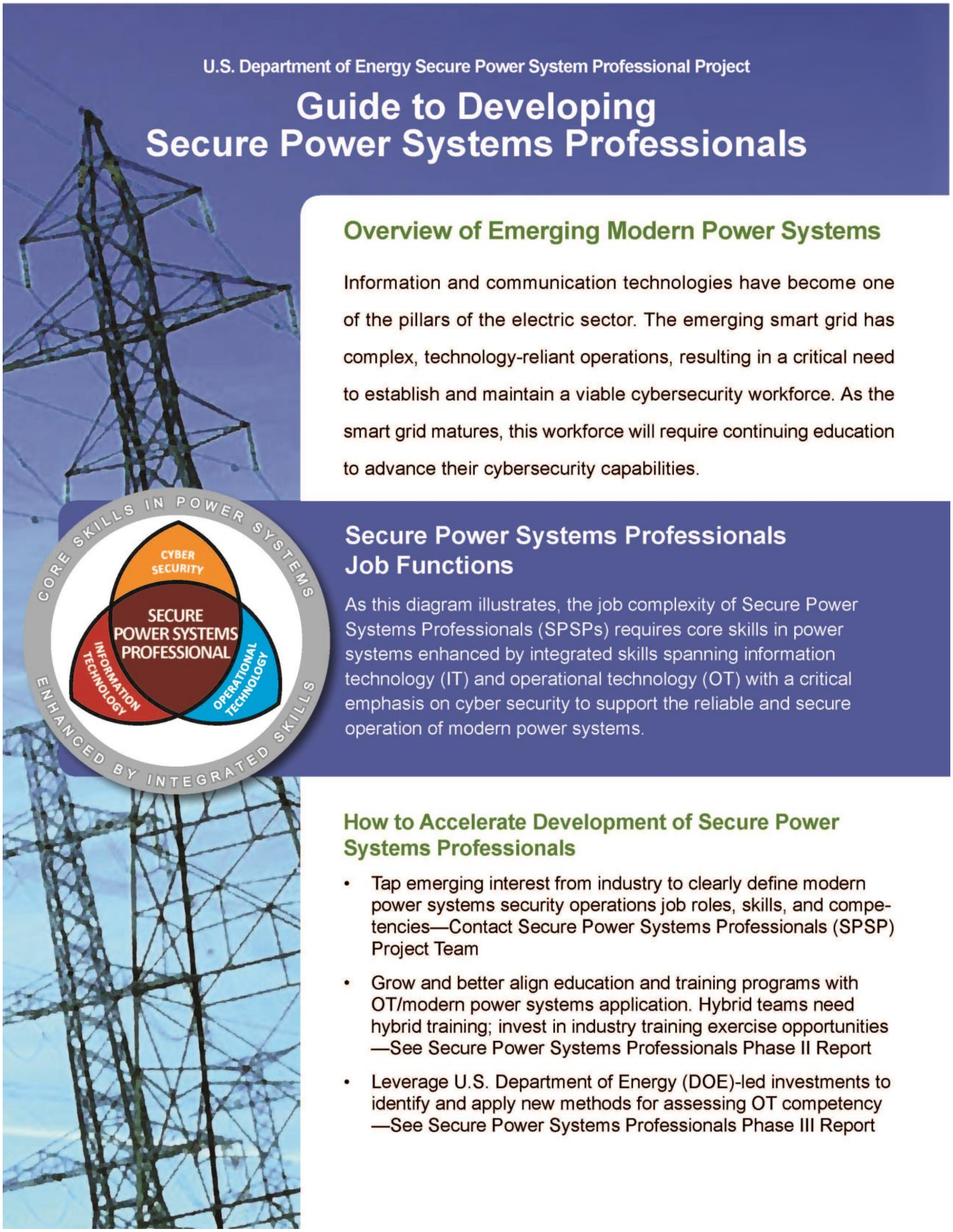
Recruitment Resources

- Trustworthy Cyber Infrastructure For The Power Grid (TCIPG)
- Energy Providers Coalition for Education (EPCE)
- IEEE
- VeteransToEnergy
- National Cybersecurity Career Fair
- GIAC Professional Directory
- National Association of Power Engineers
- NSA Centers of Academic Excellence Institutions
- National Collegiate Cyber Defense Competition
- EnergySec

Contact

Lori Ross O'Neil
Pacific Northwest National Laboratory
509-375-6702, lro@pnnl.gov
https://www.controlsystemsroadmap.net/efforts/Pages/SPSP.aspx

U.S. DEPARTMENT OF ENERGY | Office of Electricity Delivery and Energy Reliability



U.S. Department of Energy Secure Power System Professional Project

Guide to Developing Secure Power Systems Professionals

Overview of Emerging Modern Power Systems

Information and communication technologies have become one of the pillars of the electric sector. The emerging smart grid has complex, technology-reliant operations, resulting in a critical need to establish and maintain a viable cybersecurity workforce. As the smart grid matures, this workforce will require continuing education to advance their cybersecurity capabilities.

CORE SKILLS IN POWER SYSTEMS
CYBER SECURITY
SECURE POWER SYSTEMS PROFESSIONAL
INFORMATION TECHNOLOGY
OPERATIONAL TECHNOLOGY
ENHANCED BY INTEGRATED SKILLS

Secure Power Systems Professionals Job Functions

As this diagram illustrates, the job complexity of Secure Power Systems Professionals (SPSPs) requires core skills in power systems enhanced by integrated skills spanning information technology (IT) and operational technology (OT) with a critical emphasis on cyber security to support the reliable and secure operation of modern power systems.

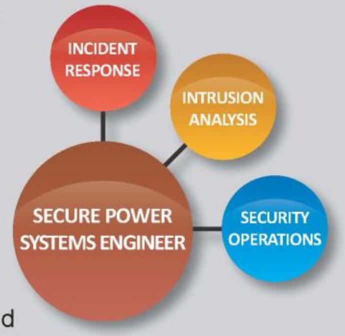
How to Accelerate Development of Secure Power Systems Professionals

- Tap emerging interest from industry to clearly define modern power systems security operations job roles, skills, and competencies—Contact Secure Power Systems Professionals (SPSP) Project Team
- Grow and better align education and training programs with OT/modern power systems application. Hybrid teams need hybrid training; invest in industry training exercise opportunities —See Secure Power Systems Professionals Phase II Report
- Leverage U.S. Department of Energy (DOE)-led investments to identify and apply new methods for assessing OT competency —See Secure Power Systems Professionals Phase III Report

How Are SPSP Skills Acquired?

Experience: Working as power engineers in utilities with experience in

- cyber security
- information security
- IT
- OT
- data management
- smart grid security
- networking and telecommunications
- SCADA protocols



SECURE POWER SYSTEMS ENGINEER

INCIDENT RESPONSE

INTRUSION ANALYSIS

SECURITY OPERATIONS

Certification: The SPSP Project examined existing certification programs and identified the following SPSP-specific certifications:

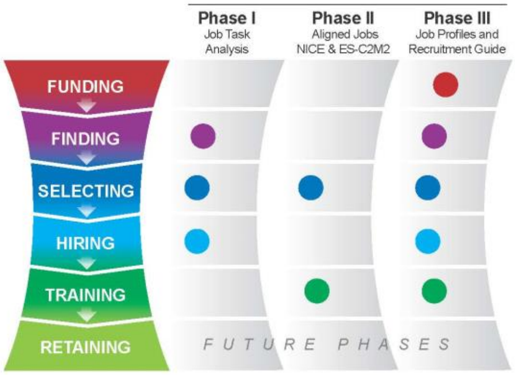
- Certified Ethical Hacker (EC-Council)
- Certified Incident Handler (GIAC)
- Certified Information Security Manager (ISACA)
- Certified Intrusion Analyst (GIAC)
- Certified Information Systems Security Professional (ISC^2)
- Certified SCADA Security Architect (IACRB)
- Control Systems Engineer license (ISA)
- System Operator Certification (NERC)
- Global Industrial Cyber Security Professional (GIAC)

How DOE SPSP Project Contributes to SPSP Workforce Development

This three-phase project identified the following critical junctures in the SPSP workforce development lifecycle:

- justifying **funding** for the position
- **finding** qualified candidates
- **selecting** cyber aware power engineers
- **hiring** qualified staff
- **training** new employees to work within the organization
- **retaining** SPSPs through professional development

Major outcomes and impacts of each phase of the SPSP project are shown in the figure at right.



	Phase I Job Task Analysis	Phase II Aligned Jobs NICE & ES-C2M2	Phase III Job Profiles and Recruitment Guide
FUNDING			●
FINDING	●		●
SELECTING	●	●	●
HIRING	●		●
TRAINING		●	●
RETAINING	FUTURE PHASES		

SPSP Project Meeting Key Secure Power Systems Challenges

Education Resources

- Energy Providers Coalition for Education (EPCE)
- NSA Centers of Academic Excellence Institutions
- IEEE
- SANS ICS
- ICS-CERT
- InfoSec Institute
- CYBATI
- SCADAhacker

Contact

Lori Ross O'Neil

Pacific Northwest National Laboratory
509-375-6702, lro@pnnl.gov
https://www.controlsystemsroadmap.net/efforts/Pages/SPSP.aspx

U.S. DEPARTMENT OF ENERGY | Office of Electricity Delivery and Energy Reliability

G.1 References

Dalton AC, and LR O’Neil. 2014. *Guide to Developing Secure Power Systems Professionals* (Technical Report No. PNNL-SA-103183). Pacific Northwest National Laboratory, Richland, WA. Available at https://www.controlsystemsroadmap.net/ieRoadmap%20Documents/SPSPCareerDevelopmentGuideFlyer.pdf.

Dalton AC, and LR O’Neil. 2014. *How to Recruit Secure Power Systems Professionals – A Guide for Human Resources and Hiring Managers* (Technical Report No. PNNL-SA-103184). Pacific Northwest National Laboratory, Richland, WA. Available at https://www.controlsystemsroadmap.net/ieRoadmap%20Documents/SPSPRecruitmentGuideFlyer.pdf.

Pacific Northwest
NATIONAL LABORATORY

U.S. DEPARTMENT OF
ENERGY

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

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

www.pnnl.gov