U.S. DEPARTMENT OF ENERGY

PNNL- 21639

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

Smart Grid Cybersecurity: Job Performance Model Report

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

August 2012

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

DISCLAIMER

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

Printed in the United States of America

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

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

(8/2010)

PNNL- 21639

Smart Grid Cybersecurity: Job Performance Model Report

August 2012

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

Pacific Northwest National Laboratory
Richland, Washington 99352

Summary

Evidence from the Center for Strategic and International Studies and the Defense Science Board starkly illuminate serious shortages in the talent available in the United States for cyber defense and cyber operations. The need for technically skilled people crosses both the government and private sectors. Faced with an aging power infrastructure, the U.S. has embarked on an epic program of grid modernization and expansion that will result in a fully digital, highly adaptable and demand-driven smart grid. But grid modernization and smart grid initiatives could be greatly hampered by the current lack of a viable workforce development framework for cybersecurity and infrastructure risk-management personnel. Grid modernization efforts require very advanced and continually maturing cybersecurity capabilities; without them the power system will not be resilient or reliable.

In the spring of 2011, the U.S. Department of Energy awarded a project to Pacific Northwest National Laboratory in partnership with the National Board of Information Security Examiners to develop a set of guidelines to enhance development of the smart grid cybersecurity workforce and provide a foundation for future certifications. The initial scope of the project is limited to operational security job functions.

The primary purpose is to develop a measurement model that may be used to guide curriculum, assessments, and other development of technical and operational smart grid cybersecurity knowledge, skills, and abilities. “Knowledge” is defined as the understanding of a concept, strategy, or procedure; thus, knowledge is measured by depth of understanding, from shallow to deep. “Skill” is defined as the reliable application of knowledge to achieve desired outcomes; thus, skill is measured by the degree of reliability, from inconsistent to consistent. “Ability” is defined as the application of skills to new domains; thus, ability is measured by the extent of skill transfer, from narrow to broad. Unlike traditional credentialing instruments that provide simple pass/fail results, this measurement model is expected to identify the position of an individual along the progression through novice, beginner, proficient, competent, expert, and master levels of expertise. Our review of both the smart grid and job analysis literature suggests this is the first comprehensive analysis of smart grid cybersecurity tasks.

The project has three phases. The first phase produced an exploratory Job Performance Model based on a factor analysis of responses to a multi-page survey, the Job Analysis Questionnaire (JAQ). The second phase will seek to validate the exploratory model in laboratory simulation studies of a small group of critical incidents. A “critical incident” is defined as any event or situation that threatens individual or organizational harm. The third phase will involve analyzing the data generated in the previous phase to produce and validate a measurement model for calculating potential performance on the job.

The initial Smart Grid Cybersecurity panel included 28 subject matter experts (SMEs), a panel chair, and a panel vice chair. This panel included nine members (32.1%) from energy industry end-users; eight members (28.6%) from the professional services sector; seven members (25%) from electricity industry vendors; three members (10.7%) from academic or corporate research organizations; and one representative (3.6%) from government.

The project has already begun defining performance and establishing the building blocks for measuring it across three highly technical cybersecurity roles. The process for the elicitation of job goals and tasks can be accomplished in six weeks and begins with the identification and elaboration of security scenarios to drive the remainder of the process. The level of detail that is produced provides a

comprehensive look at the tasks to be performed and the underlying knowledge and skills. The panel and broader community rank the tasks (over 500 identified) to understand which are critical and how competency impacts execution.

Project preliminary results:

The factor analysis process began with a detailed literature review and collection of job descriptions and individual development plans. The National Board of Information Security Examiners developed an innovative process for eliciting predictors of job performance combined with a group decision-support system to accelerate the competency modeling process. This cycle-time reduction from months to weeks supports the infusion of *ground truth*—information on the latest vulnerabilities, adversary strategy and tactics, and best practices for detection and defense—that determines the fundamental and differentiating factors that predict job performance.

The background information, developed from the literature review, provided the context for the definition of vignettes (i.e., real-world security workflow initiating scenarios). A "vignette" is a terse statement that identifies a critical incident or activity which provides the context for job performance. The panel identified a total of **109 vignettes**, which were sorted by the program manager, the panel chairperson, and the panel vice-chairperson, into 13 master vignettes that were used to classify the work in smart grid cybersecurity jobs. The **roles identified during the Job Classification step (over 40)** were then categorized into functional roles aligned with the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.[1] The list of roles was discussed with the panel of SMEs, and ranked by them based on vignette interaction; they selected three job roles to focus on for the remainder of the modeling process: *Security Operations*, *Intrusion Analysis*, and *Incident Response*.

During the next step, the SME panel developed a list of goals and objectives that could establish a criterion for assessing performance in the selected job roles. The panel identified a total of **108 goals and objective measures**. The goals were sorted into primary, secondary, and tertiary levels. Primary goals must be accomplished to achieve the organizational mission. Secondary and tertiary goals must be accomplished to successfully achieve a higher-level goal. This ranking resulted in a list of **27 primary goals**.

Finally, the tasks necessary to fulfill this mission were elicited from the panel. A **total of 516 tasks** were identified as potentially relevant for determining the level of expertise and predicting performance. These tasks were included in the JAQ, in which panel members and invited industry experts rate the frequency and importance of task performance by individuals at one of three levels of expertise: novice, intermediate, or expert. Response to the questionnaire will continue into the second phase of the project.

The main body of the JAQ is the task-statement ratings. Our goal is to collect sufficient ratings to support inferences regarding the criticality and differentiation of each task in determining the factors impacting performance of individuals with varying levels of expertise.

The respondent data also suggests which tasks should become the focus for Phase II activities and further analysis by the SME panel. These results arise from an innovative new technique for identifying influential task performance, the Critical-Differentiation Matrix (CDM). The CDM identifies the

[1] NICE Cybersecurity Workforce Framework: http://csrc.nist.gov/nice/framework/

fundamental and differentiating tasks that should best predict job performance. We define "criticality" as the product of the arithmetic means of frequency and importance across all levels of expertise. We define "differentiation" as the slope of criticality scores relative to level of expertise, signifying the frequency that a person with a given skill level must be involved, and the importance of that task for determining the performer's skill level. "Fundamental" tasks are defined as those that are rated as highly critical but show little differentiation across these three levels. Performance on these tasks is essential and should be considered minimal entrance requirements for the field. Finally, "differentiating tasks" are those that exhibit both high criticality and high differentiation scores.

The **CDM analysis revealed 83 tasks as fundamental** to job performance across the three smart grid cybersecurity job roles that were studied. Twenty tasks were identified as indicators of the development of individual competence along the six levels of expertise.

In brief, this project developed a new approach to job task and competency analysis that is intended to identify the knowledge, skills and abilities necessary to successfully perform the responsibilities of three smart grid cybersecurity job roles: Security Operations, Intrusion Analysis, and Incident Response.

The next phase of the project will involve a practice analysis to guide selection from the list of fundamental and differentiating tasks. These tasks will be further elaborated using cognitive task and protocol analysis. The primary outcome from this effort should be the development and validation of a set of proficiency and situational-judgment-test item pools, as well as simulation configurations that may be used to validate the construct and predictive validity of the Job Performance Model and the test items. The confirmatory analysis performed during this phase will prepare the material necessary to develop a potential performance analysis that can distinguish the contributions of knowledge, skill, and ability factors in producing effective smart grid cybersecurity job performance.

A summary version of this report titled: *Smart Grid Cybersecurity Certification Phase 1 Overview* August 2012, document clearance number PNNL-21638 is available. Please contact Lori Ross O'Neil (lro@pnnl.gov) for a copy of this report.

Acronyms and Abbreviations

AMI	advanced metering infrastructure
ATR	Advanced Threat Response
CDM	Critical-Differentiation Matrix
CIA	Critical Incident Analysis
DHS	U.S. Department of Homeland Security
GDSS	Group Decision Support Systems
GWA	General Work Activities
IT	Information Technology
IDS	Intrusion Detection System
JAQ	Job Audit (or Analysis) Questionnaire
JPM	Job Performance Model
KSA	Knowledge, Skills, Ability
KSAO	Knowledge, Skills, Abilities and Other
NBISE	National Board of Information Security Examiners
NERC	North American Electric Reliability Corporation
NESCO	National Electric Sector Cybersecurity Organization
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
OST	Operational Security Testing
OT	Operational Technology
PNNL	Pacific Northwest National Laboratory
PPA	Potential Performance Analysis
PPIK	Processing, Personality, Interests, and Knowledge
PRISM	Premier, Robust, Improved, Satisfactory, and Moot
SCA	Sub-Component Areas
SCADA	supervisory control and data acquisition
SGC	Smart Grid Cybersecurity
SME	subject matter expert
VUCA	Volatility, Uncertainty, Complexity and Ambiguity

Contents

Figures

Tables

1.0 Introduction

1.1 Impetus for the Study

Faced with an aging power infrastructure, the U.S has embarked on an epic program of grid modernization and expansion that will result in a fully digital, highly adaptable and demand-driven smart grid. But grid modernization and smart grid initiatives could be greatly hampered by the current lack of a viable workforce development framework for cybersecurity and infrastructure risk-management personnel. Grid modernization efforts must include very advanced and continually maturing cybersecurity capabilities or the power system will not be resilient or reliable.

With thousands of generation plants and many thousands of miles of delivery lines, the North American power grid presents a vast and ever-growing cyber-attack surface that may never be fully mapped and documented from a vulnerability-, asset- and risk-management standpoint. The mapping of assets, vulnerabilities and dependencies will continue indefinitely, but meanwhile the grid is increasingly vulnerable. Cybersecurity experts and operational staff must protect the grid until the perfect security automation model and the ideal threat-response reference library are developed. The protection of the smart grid network and core supervisory control and data acquisition (SCADA) control systems requires a very challenging blend of control engineering and security; this can only be executed by senior security engineers who have a very special mix of general abilities, acquired skills and knowledge.

Government and industry executives now largely agree that the deficit of workers with sufficient cybersecurity expertise is approaching a crisis point as grid complexity increases and the current generation of grid security experts retires. Usually it takes many years to mature a cybersecurity worker's knowledge, skills and performance. Senior cybersecurity professionals possess a special mix of information security, technology infrastructure, risk, operations, social, analytical and organizational skills. To reach peak performance, senior security engineers had to first become highly proficient information technology (IT) professionals. Years of accumulation of IT knowledge are then enhanced with years of additional security experiences, which eventually produce mastery of the principles of forensics, risk management and business impact. This path ultimately allows a seasoned information security expert to perform highly skilled actions that protect grid control systems on infrastructure in a way that is aligned with organizational and regulatory policies and goals.

Recently, the North American Electric Reliability Council’s Long-Term Reliability Assessment Report noted that the potential loss of this expertise as industry’s workforce ages poses a long-term threat to bulk system reliability. There is a growing need to not only replace large numbers of departing cybersecurity workers, but also to greatly augment the workforce with new skills and advanced capabilities. Thus, the energy industry needs a large-scale transfer of expertise plus increased agility and productivity of the cybersecurity workforce to bridge the gap.

The U.S. Department of Energy recognized that the electric industry needs a workforce development program that can make up for the accelerating loss of security workforce professionals, while at the same time building substantial new cybersecurity expertise capabilities to protect the expanded attack surface of the modernized smart grid. Accordingly, in Spring 2011 a contract was awarded to Pacific Northwest National Laboratory (PNNL) to develop a set of guidelines for the development of a certification program for smart grid cybersecurity specialists. The initial scope was defined as the operational security functions

for day-to-day operations, (but not engineering and architecture), and smart grid environments. The project would examine the technical, problem-solving, social and analytical skills used by senior cybersecurity staff in the daily execution of their responsibilities. The primary purpose is to develop a measurement model for assessing technical and operational cybersecurity knowledge, skills, and abilities.

A workforce development program must be holistic in the way it measures, develops and supports cybersecurity expertise (Assante and Tobey 2011). "Holistic" in this context means:

- addressing all human factors of accelerated expertise development (book-knowledge, hands-on skills, innate abilities, cognitive/behavioral influences)
- including all phases of the workforce development cycle (assessment, training, certification, re-testing, professional development, communities of practice, etc.).

Existing cybersecurity training and certification programs focus on the job of testing the "book-learning" of security engineers who often study preparation guides before taking the certification tests. Certification bodies (the Information Systems Audit and Control Association [ISACA], the Computing Technology Industry Association [CompTIA], the International Information Systems Security Certification Consortium [ISC/2] and many others) provide a gauge of intellectual knowledge in specific cybersecurity areas. However, existing certification solutions do not measure or certify competence in the real world where multi-discipline problem solving and social and intuitive analytical skills are used by senior security engineers in the daily battle to protect the grid. Even the most advanced "performance based" certifications (e.g., Global Information Assurance Certification [GIAC] or GIAC Security Expert [GSE]) have not kept up with the latest research advances in the cognitive science of human expertise development. Traditional security certification organizations cannot create an adequate cybersecurity protection workforce for the modernized smart grid.

In addition to the lack of comprehensive assessment and testing, current approaches do not provide a blueprint or roadmap for a life-cycle program of workforce expertise management. Current assessment and evaluation services have these deficiencies:

- 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 that effectively resolve problems quickly and despite distractions or the stress surrounding an attack?)
- 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?)
- Support gap (How do we support the certified cybersecurity elite with advanced problem-solving tools, communities of practice, canonical knowledge bases, and other performance support tools?)

The National Board of Information Security Examiners (NBISE) was formed to leverage the latest advances in performance assessment and learning science toward the solution of one of the United States' most critical workforce shortages: cybersecurity professionals. NBISE's mission, working with program participants, is to analyze and design assessment instruments and practical challenges that are both fair and valid and to enhance the confidence of skill measurement instruments as predictors of actual job

performance. In fulfilling this mission, NBISE is developing methodologies for defining and measuring the factors that determine successful job performance. Because this project required the use of new techniques to support workforce development that impart the knowledge and include the practice exercises that foster skill development, NBISE was selected to partner with PNNL to conduct a three-phase study for the U.S. Department of Energy.

This report will consist of a cumulative analysis and report of the three-phase study to produce a comprehensive Job Performance Model (JPM) for Smart Grid Cybersecurity: a list of competencies, often organized into five or more groupings or clusters, attributable to satisfactory or exceptional employee performance for a specific job role. The first phase produced an exploratory JPM based on a factor analysis of responses to a Job Analysis Questionnaire (JAQ), culminating in the Smart Grid Cybersecurity Job Analysis Report. During this phase, critical incidents (Flanagan 1954; Klein et al. 1989) captured as a series of vignettes, or deconstructed stories (Boje 2001; Tobey 2007), of a significant or potentially significant event transformed into a detailed list of goals, objectives, responsibilities, and tasks for the functional and job roles involved in smart grid cybersecurity. The second phase will seek to validate the exploratory model in laboratory simulation studies of these critical incidents. Protocol analysis (Ericsson 2006; Ericsson and Simon 1980, 1993) and confirmatory factor analysis (Brown 2006; Long 1983) will be used to validate the exploratory JPM. The third phase will involve analyzing data generated in the previous phase to produce and validate a measurement model for calculating potential performance on the job (Tobey, Reiter-Palmon, and Callens, forthcoming). Based on all three phases, a final report will provide guidance on the development of assessment instruments, training modules, and simulation practice environments that may be used to accelerate proficiency in smart grid cybersecurity jobs.

The sections below discuss the science behind the development of JPMs (adapted from Tobey, Reiter-Palmon and Callens, forthcoming), the method that will be used to develop a job description report and task analysis, and provide preliminary results for the definition of functional and job roles based on a job classification analysis.

1.2 Job Analysis: Early Attempts at Performance Modeling

"Job analysis" is a method by which we understand the nature of work activities by breaking them down into smaller components (Brannick et al. 2007; McCormick 1979). As the name implies, many job analyses focus primarily on the attributes of work itself, and then link these work attributes to job-relevant knowledge, skills, abilities, and other work-related characteristics including attitudes and motivation (KSAOs). Collectively, the KSAOs represent the competencies required for a job. An individual employee would need to possess these competencies to successfully perform the work (Shippmann et al. 2000). The purpose of the job analysis is to provide detailed information about the job that will guide various aspects related to managing performance such as the development of training materials, testing for selection and competency evaluation, and developmental plans.

Information about the job may be gained from focus groups, surveys, and interviews of job incumbents, supervisors, and others that are familiar with the day-to-day task requirements of the job. Sampling subject matter experts (SMEs) with different levels of expertise and who work in different organizational settings allows the results to be more easily generalized across domains (Morgeson and Dierdorff 2011).

Historically, work-oriented job analyses began by using general work activities (GWAs) as a framework to capture position-specific job tasks. These GWAs are broad collections of similar work activities such as "interacting with computers" or "getting information" (Jeanneret et al. 1999). GWAs were designed to be applicable to all work domains and allow for comparisons across dissimilar jobs (Reiter-Palmon et al. 2006). Work tasks, on the other hand, are more specific to a given occupation than are GWAs. For instance, most occupations share the GWA of "interact with computers;" an associated task of "analyze output of port scanners" would only be required of a rather limited subset of jobs. Typical job analyses yield between 30 and 250 work tasks that are somewhat unique to a specific industry (Brannick and Levine 2002). After describing and evaluating work tasks, the focus of many job analyses then shifts to the KSAOs that are needed to complete job tasks. Like GWAs, KSAOs are standardized to facilitate generalizing them across job domains. As such, KSAOs may be appropriate when comparing across jobs, but more specific work goals may be necessary to adequately capture worker requirements within a given occupation. It is important to note that in many cases only one component (tasks or KSAOs) may be the focus of the job analysis. However, obtaining both types of information is critical for some uses of job analysis.

1.3 From Job Analysis to Competency Modeling

Compared to the "historical snapshot of work" produced by a job analysis, competency modeling is considered a more employee-focused examination of working conditions because it actively links employee behaviors to business goals (Sanchez and Levine 2009). Competency models "typically include(s) a fairly substantial effort to understand an organization's business context and competitive strategy and to establish some direct line-of-sight between individual competency requirements and the broader goals of the organization" (Shippmann et al. 2000, p. 725). By focusing on clearly defined business goals, managers are then in a position to distinguish between levels of performance in goal attainment (Campion et al. 2011; Parry 1996).

In practice, there can be significant overlap between job analysis and competency modeling. For example, Campion and his associates (2011) suggest that competencies be developed using job analysis procedures such as observations, interviewing, and focus groups. Similarly, applied research by Lievens et al. (2004) showed that providing SMEs with the tasks derived from a job analysis enhanced the quality of the competencies they identified.

Despite this progress in the development of job analysis and competency modeling techniques, concerns continue to arise about their ability to capture the relevant requirements of a job necessary to accurately predict performance. These concerns are especially pronounced in highly technical jobs involving hands-on skills (Arvey et al. 1992). Current methodologies have frequently failed to capture dynamic aspects of a job, especially those involving integration across job roles and the interpersonal processes involved in such collaborative work (Sanchez and Levine 2001; Schmidt 1993; Schuler 1989). Since existing methods focus primarily on GWAs rather than the goals and objectives of a job, they may fail to identify the practices that differentiate levels of expertise and performance (Offermann and Gowing 1993). In summary, research suggests that innovations are necessary to increase the depth and complexity of these models to match the increasing complexity of today's jobs (Smit-Voskuijl 2005). In a recent summary of best practices in competency modeling, Campion, et al. (2011) identified 20 critical innovations that would address deficiencies in identifying, organizing, presenting, and using competency information (see Table 1.1).

Table 1.1. Best Practices in Competency Modeling

Analyzing Competency Information (Identifying Competencies)
1. Considering organizational context
2. Linking competency models to organizational goals and objectives
3. Starting at the top
4. Using rigorous job-analysis methods to develop competencies
5. Considering future-oriented job requirements
6. Using additional unique methods
Organizing and Presenting Competency Information
1. Defining the anatomy of a competency (the language of competencies)
2. Defining levels of proficiency on competencies
3. Using organizational language
4. Including both fundamental (cross-job) and technical (job-specific) competencies
5. Using competency libraries
6. Achieving the proper level of granularity (number of competencies and amount of detail)
7. Using diagrams, pictures, and heuristics to communicate competency models to employees
Using Competency Information
1. Using organizational development techniques to ensure competency modeling acceptance and use
2. Using competencies to develop Human Resources systems (hiring, appraisal, promotion, compensation)
3. Using competencies to align the Human Resources systems
4. Using competencies to develop practical "theory" of effective job performance tailored to the organization
5. Using information technology to enhance the usability of competency models
6. Maintaining the currency of competencies over time
7. Using competency modeling for legal defensibility (e.g., test validation)

1.4 Adapting Competency Models to Understand Cybersecurity Jobs

There is perhaps no more complex and dynamic work environment than cybersecurity. Further exacerbating the challenge of defining such a dynamic job is that little is known about the competencies required to meet the new vulnerabilities introduced with the advent of the smart grid. Extant research has focused mainly on cybersecurity policy or the technological manifestations of these threats, rather than the individual competencies necessary to identify, diagnose, and effectively respond to such threats. In a recent essay recounting the past 30 years of cybersecurity, Ryan (2011, p. 8) argues that the thinking about computer security needs to change. She says, "it is critical that the security community embrace non-technical aspects as part of the whole problem space….A focus on enterprise security goals rather than security technologies would be a good start – when security is an architectural goal, there is less temptation to try to bolt on exotic solutions focusing on tiny slivers of the technological challenge. Instead, holistic and synergistic solutions must be developed. It is increasingly important that we architect solutions that incorporate human brains, taking into account intellectual property and human inadvertent activity."

MITRE Corporation has developed a framework intended to improve the preparedness of organizations to meet the challenges of the cybersecurity threat. In their description of this framework, Bodeau et al. (2010) propose a five-level model delineating the strategies and objectives comprising effective cyber-preparedness. The levels correspond to "distinct break points in adversary capabilities, intent, and technical sophistication, as well as in the operational complexity involved in an attack" (p. 2). This model suggests that developing a secure cybersecurity posture requires development of capabilities

in foundational defense, critical information protection, responsive awareness, architectural resilience, and pervasive agility. Organizations may experience increasing cost and coordination to raise organizational preparedness to match the level of threat. According to Bodeau et al. (2010, Table 2), based on the level of adversary capabilities, organizations must:

1. Prepare for known external attacks and minor internal incidents;
2. Prevent unauthorized access to critical or sensitive information;
3. Deter adversaries from gaining a foothold in the organization's information infrastructure;
4. Constrain exfiltrations of critical data, continue critical operations, minimize damage despite successful attacks from adversaries who have established a foothold; and
5. Maintain operations on a continuing basis and adapt to current and future coordinated, successful attacks, regardless of their origin.

However, typical of the few studies in this area, the model concludes with a listing of technologies that can safeguard critical assets, rather than a specification of the competencies needed by the cybersecurity workforce to address the growing threats to critical infrastructure.

In a study of the recent attack on RSA, Binde et al. (2011) suggested that a complex set of competencies is required. According to their findings, an effective threat response must include the ability to identify phishing campaigns, recognize and block malicious traffic, and monitor operating systems for attack signatures. However, they offered no guidance as to the specific KSAOs that may support development of these abilities.

Frincke and Ford (2010) indicate why the development of a competency map for cybersecurity professionals has been so difficult. Even the development of a simple depiction of knowledge requirements is challenging. First, it is difficult or impossible to define a typical practitioner. Second, it is not known how practitioners derive their knowledge—from books or on the internet through tweets or Really Simple Syndication (RSS) feeds? Finally, it is unclear what differentiates foundational knowledge from specialized knowledge. They conclude that a competency framework must determine whether the knowledge needed is universal or changes based on role and responsibility. For instance, a researcher trying to design a lab test of an advanced persistent threat would need knowledge of past attacks in order to design a test that could accurately respond to an attack. On the other hand, a security expert would not only need the basic knowledge of past attacks but also the knowledge of how to detect an attack and produce the right defenses in real time.

Therefore traditional job analysis or competency modeling based on surveys of job incumbents may fail to fully capture the job of a smart grid cybersecurity specialist. As Campion et al. (2011) have suggested, competency models in such a dynamic and ill-defined domain must employ unique methods for eliciting job context, goals, objectives, tasks, and KSAOs across different roles and proficiency levels. Accordingly, to fully understand and model success in these jobs, NBISE is innovating many of the 20 areas shown in Table 1.1. In this section, we will describe some of these innovations used to develop the beginning of a *Job Performance Model*. The JPM seeks to predict performance and assess aptitude necessary to not only understand past performance, but also develop a profile of future abilities. Accordingly, the JPM that will evolve from this Job, Task and Competency analysis will include:

- context elicitation through vignettes and responsibilities

- the Premier, Robust, Improved, Satisfactory, and Moot (PRISM) method for eliciting goals and objectives (Tobey 2007)
- models that include both technical, operational, and interpersonal skills
- functional responsibility analysis that recognizes the collaboration that occurs among roles, and the consequent overlap in task performance
- competencies defined at novice, apprentice, journeyman, and expert levels for multiple roles based on industry vernacular
- exploratory factor analysis to develop a causal model of performance that can be subsequently validated and used to support design of instructional modules, proficiency and performance assessments, and lab exercises that facilitate converting knowledge into skill.

1.5 Developing a Job Performance Model

Developing a list of tasks or competencies necessary to perform a job requires a greater depth of analysis than that identified as the current state of the art in Table 1.1. First, and perhaps most important, is the transition from descriptive models of job performance to prescriptive or predictive models. The traditional approaches tend to produce lists of job duties and KSAOs that are sufficiently general to apply broadly but lack the detail necessary to predict, based on an assessment instrument, how an individual will actually perform on the job. These techniques tend toward a focus on frequent and important tasks, obtained through a factor analysis, as a descriptive model of the responsibilities which must be executed by a job incumbent. An exception is models that combine factor analyses with logistic or structural regression analysis. While inductive in nature, this approach may identify and subsequently confirm a model of job performance over two or more studies. Thus, one step toward moving from modeling competency to modeling job performance is to create a nomological network of factor relationships that fits the patterns derived from a statistically valid sample of incumbents on the job. Figure 1.1 shows an example of such a model for Operational Security Testing (OST) prepared recently by NBISE.

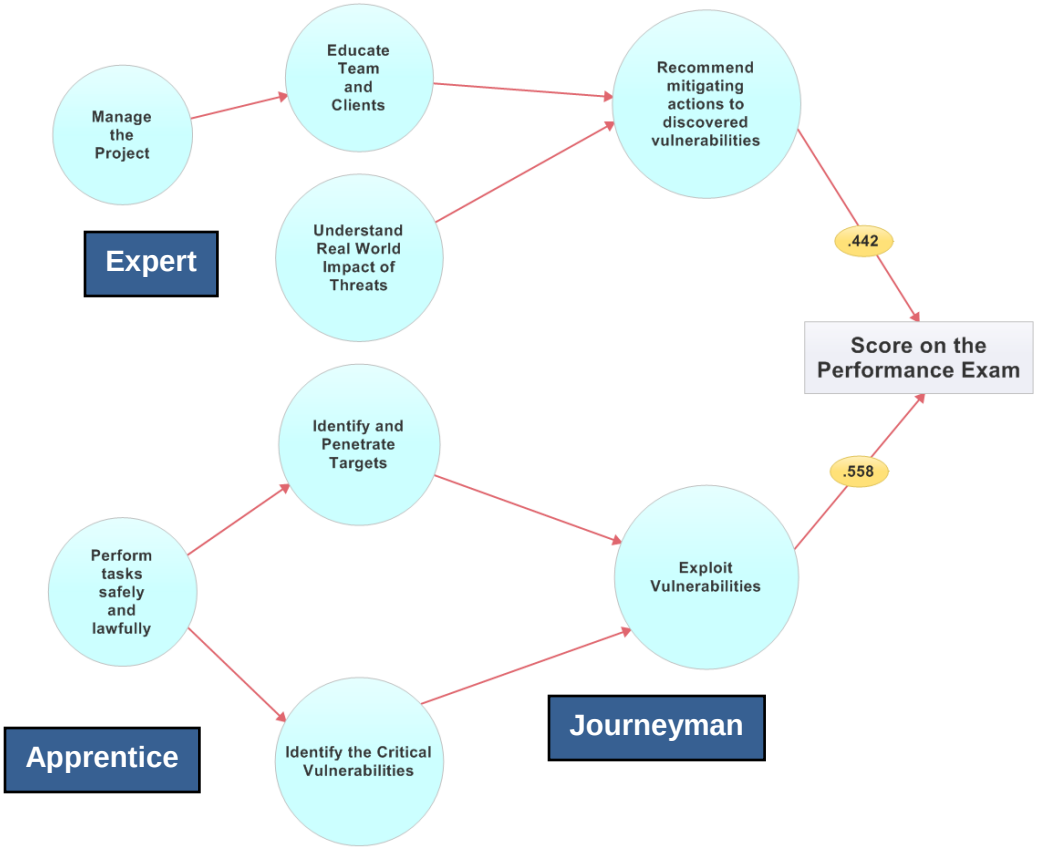


Figure 1.1. Example Job Performance Model

For example, Dainty et al. (2005) used this approach to develop a predictive model of the construction project management job. Their study demonstrates that an important benefit of such an approach is the creation of a parsimonious model of job performance. By identifying the critical factors, a JPM is able to focus training, skill development, and assessment on the few variables which explain the most variance in job performance. Consequently, investment in workforce development can become more targeted, efficient, and effective in accelerating proficiency (Hoffman and Feltovich 2010).

The transition from competency to JPMs is also facilitated by a more detailed understanding of the building blocks of competence: knowledge, skill, and ability. Le Deist and Winterton (2005) reviewed definitions of competence from around the world. While the U.S. and the U.K. have primarily focused on functional or occupational definitions of competence, which tend to conflate the definition of the knowledge, skills, and abilities (KSA) elements, other European countries have moved toward a multidimensional conception of competence. For instance, France has created the *triptyque*: a three-dimensional view separating knowledge (*savoir*), experience (*savoir faire*), and behavior (*savior être*). This multidimensional view is consistent with recent development of an engineering model of learning (Hoffmann 2011, p. 270) that defines: ***knowledge*** as "retrievable information" created through learning; ***skill*** as "courses of action" (or habituated behavior) created as a result of practice in applying knowledge; and ***ability*** as the application of knowledge and skill to "novel and unusual situations" (thereby showing the benefit of experience in adapting to unforeseen circumstances). Similarly, Trafimow and Rice (2008,

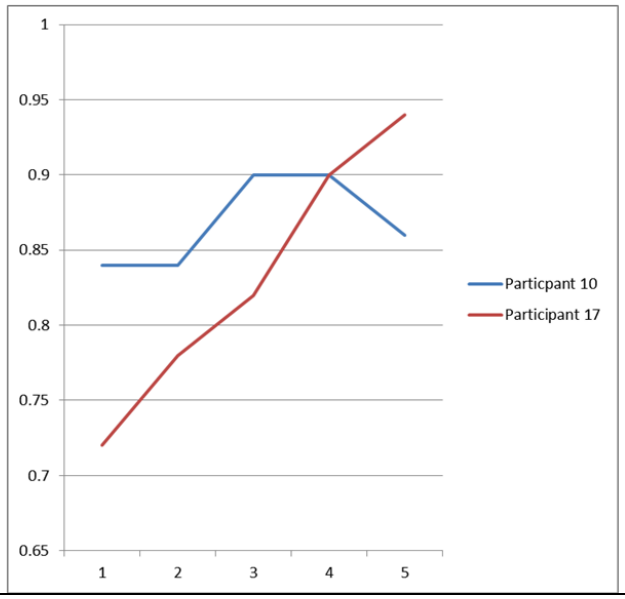
2009) recently proposed *Potential Performance Theory* to explain and provide independent measures of knowledge (strategy), skill (consistency), and ability (potential). Based on these, and other findings from study of expertise (Chi et al. 1988; Ericsson 2004; Ericsson and Charness 1994; Ericsson et al. 2006; Hoffman 1992), we have developed a tripartite competency framework in which knowledge, skill, and ability provide distinct contributions to the development of mastery over time. As shown in Figure 7.1, a JPM using this framework may extend job task and competency analysis by differentiating the expected performance of novices, apprentices, journeymen, and masters through the values of three distinct but interacting variables: "**knowledge" defined and measured as a *depth of understanding*, "skill" defined and measured by the *consistency* by which knowledge is applied, and "ability" defined and measured by the *adaptation* of skill to address novel or unusual situations.**

As expertise progresses from novice through master levels, the relative contributions of knowledge, skill, and ability to performance change. Also, the progression may take any of several trajectories inside the "competency box:" a specialist may be positioned more toward the upper front of the box, demonstrating deep understanding, consistently applied across many projects; however, specialists are limited in the application of this knowledge and skill to a narrow domain. A master may not have substantially greater knowledge than a journeyman, and perhaps less than a specialist, but demonstrates skilled application of expertise across a broad set of domains.

Figure 1.3 below shows an example of using this framework to perform a Potential Performance Analysis (PPA) adapted from the study conducted by Trafimow and Rice (2009, Table 2). In PPA, *potential performance* is assumed to be a function of the *knowledge* (strategy employed), *skill* (consistency of knowledge application), and *ability* to adapt to new situations. Each of the three dimensions is separately measured: knowledge is measured by the observed scores; skill is measured by the consistency coefficient; and ability is measured by the rate of change (slope of the line) in the True Score, or potential, over time. This study showed that knowledge, skill, and ability are not simply separate components of competence. Each dimension provides a unique and differential impact on the overall potential for an individual to perform the job over time. Somewhat surprisingly, Trafimow and Rice found that an individual who has become skilled in using a less effective strategy may underperform a less skillful person who can more easily adapt to novel conditions.

Table 2
Individual-Level Data From PPT Analyses

	Session 1			Session 2			Session 3			Session 4			Session 5		
Participant	Observed Score	True Score	*r*	Observed Score	True Score	*r*	Observed Score	True Score	*r*	Observed Score	True Score	*r*	Observed Score	True Score	*r*
10	.84	0.89	.75	.84	0.87	.87	.90	0.93	.87	.90	0.96	.75	.86	0.90	.83
17	.72	0.84	.42	.78	0.86	.59	.82	0.88	.72	.90	0.95	.80	.94	0.97	.88



While observed score (proficiency) provides a measure of past accomplishment, the coefficient of consistency (*r*) is a measure of the degree of knowledge vs. skill employed. PPA is thus a better predictor of future performance. Highly consistent performers will tend to remain within a performance band determined by their level of skill, while inconsistent performers have much more room for improvement if they apply their knowledge using deliberate practice (Ericsson, 2004).

Implication
With practice, a poor performer working from mere knowledge can outperform a skilled, average performer.

Source: Trafimow & Rice (2009) Potential Performance Theory

Figure 1.2. Potential Performance Analysis

This can be seen by comparing the scores over time of Participant 17 to Participant 10 as shown in the diagram in Figure 1.3. Even though Participant 17 employed a less effective strategy at the outset, the lack of skill and a greater ability to adapt to the new job over time enabled this individual to outperform a worker who had a reasonably effective strategy which was skillfully applied, but who lacked an ability to adopt a more effective strategy. Thus, we propose that when defining a JPM it is essential to identify those tasks in which performance greatly differs among those with varying knowledge, skill and ability. The traditional focus on importance and frequency of tasks is necessary but insufficient to develop a predictive model of job performance.

Each of the detailed analyses presented above increases our understanding of the antecedents to job performance, the factors which define the job and the dimensions which affect behavior, but to predict performance we also need to understand how variance in performance is evaluated. Some advanced job task and competency models (for example, Dainty et al. 2005) have incorporated better factor analysis to improve their prescriptive value. We have yet to see one which combines advanced factor analysis with multiple methods for assessing the differential impacts of knowledge, skill and ability. However, even doing so would only improve the definition and measurement of the independent variables comprising a performance model. To determine aptitude and proficiency to perform a job, we must accurately measure variance in the dependent variable—job performance—as well.

Robert Mislevy and his colleagues have been studying methods for assessing and tutoring technical workers for more than 30 years (for examples, see Behrens et al. 2006; Mislevy 1994, 2006; Mislevy and Bock 1983; Mislevy et al. 1999; Williamson et al. 2004). This work has culminated in the development of

an evidence-centered design approach to the development of training and assessment systems that has recently been adopted by Cisco Systems to increase the predictive and prescriptive value of their Cisco Networking Academy program (Behrens et al. 2010). Central to the success of this program, deployed in over 160 countries, is the clear understanding and modeling of the context of the job: "the ways people use [their competencies] and the kinds of situations they use [them] in" (Behrens et al. 2010, p. 11). These and other studies increasingly show the context-sensitive nature of expertise. Consequently, we propose that a JPM must explicitly explore how tasks and KSAO usage differ by scenario, what job roles perform these functions, and how they interact. Finally, we seek to extend traditional job task and competency analysis by defining the set of goals, objective metrics, and performance against these metrics that typify workers at different competency levels.

The next section will report our application of these new methods. We will begin with a review of the composition of the SME panel, attendance and constituencies represented in each focus group session, and changes made to the panel roster to improve participation or representativeness of panel members. We will then describe the methods to be used during the elicitation phases. This will be followed by a review the four steps of job and task definition: context definition; role definition; mission definition; and process definition, which collectively form the basis for the Job Description Report. This report will be appended during the next phase of the project during which the SME panel will elaborate the process definition to produce a detailed list of tasks, methods, and tools. During the final phase of the exploratory JPM development, the panel will define a set of KSAs that are expected to determine performance on the job.

2.0 Panel Composition

The initial Smart Grid Cybersecurity panel included 28 SMEs, a panel chair and a panel vice chair (for a complete roster, see Appendix A). The panel (28 male, 2 female) is advised by the NBISE and PNNL project team (3 male, 2 female) and five outside advisors (all male) representing industry, government, and academic perspectives. The initial panel was formed with nine members (32.1%) from the energy industry; eight members (28.6%) from the professional services sector; seven members (25%) from technology vendors; three members (10.7%) from academic or corporate research organizations; and one representative (3.6%) from government. The selection of panelists was based on their expertise in the relevant fields, availability of sufficient time to commit to the project, and maintaining a diverse representation of the interested stakeholders. The panelists are also widely distributed geographically.

Since the panelists are volunteers it is expected that their involvement may change over time. The cybersecurity profession is in high demand and the need for cybersecurity skills is unpredictable. Previous SME panels have seen participation rates drop dramatically after the first focus sessions, often with more than 50% attrition as the volunteers find that their primary work activities will no longer permit continual attendance on weekly panel calls or making contributions between calls necessary to complete assigned activities. Accordingly, NBISE maintains a list of alternates who may be added to the panel if participation rates fall significantly.

Over the first four sessions, five panel members withdrew from the panel and two alternates were added, bringing the active roster to 25 panel members. The greatest change occurred in industry representation as year-end business planning and plant maintenance reduced the time available to participate in panel activities. Table 2.1 shows the changes in panel composition over the first four sessions, and that at the conclusion of this period the panel composition had become six members (24%) from the energy industry; seven members (28 %) from the professional services sector; seven members (28%) from technology vendors; three members (12%) from academic or corporate research organizations; and two representatives (8%) from government.

Table 2.1. Changes in Panel Composition

Initial Panel Representation			
Total	**28**		
Service		8	28.57%
Government		1	3.57%
Industry		9	32.14%
Vendor		7	25.00%
Research		3	10.71%
Changes to representation over the first four sessions			
Total	**25**		
Service		7	28.00%
Government		2	8.00%
Industry		6	24.00%
Vendor		7	28.00%
Research		3	12.00%

3.0 Elicitation Methodology

Throughout the process, a collection of collaboration tools is used to facilitate the thinking and contributions of the SME panel. The online collaboration environment has been designed and configured based on dozens of years of research on Group Decision Support Systems (GDSS) (Nunamaker et al. 1997). GDSS has been found to dramatically increase the productivity and scale of processes similar to job performance modeling which involve complex intellective tasks requiring collective intelligence (Briggs et al. 2003; Briggs et al. 2001). The GDSS tools are embedded in a web portal that also includes a clear statement of the SME panel's purpose, the steps in the JPM process, and links to the activities the panel is to complete each week.

Typical of cycle-time reductions found in other uses of collaboration engineering environments (Tobey 2001), the process for eliciting job performance constructs can be dramatically reduced from months to weeks. Figure 3.1 below shows the time line for the preparation of a job, task and competency analysis using the traditional techniques developed for the U.S. Office of Personnel Management (Reiter-Palmon et al. 2006). This process uses GWAs to provide the context for task definitions which are analyzed using frequency and criticality ratings. The result is a database of job descriptions called O*NET which is a publicly available reference for personnel managers in government and private sector organizations seeking to develop job specifications. When used to develop the Job Description Report for OST (Tobey et al., forthcoming) this approach required six months to produce a task list suitable for including in a JAQ. While this is much too long for a dynamic profession such as cybersecurity, traditional approaches using face-to-face interviews by industrial psychologists, rather than focus groups supported by a GDSS, have often taken years to accomplish the same results.

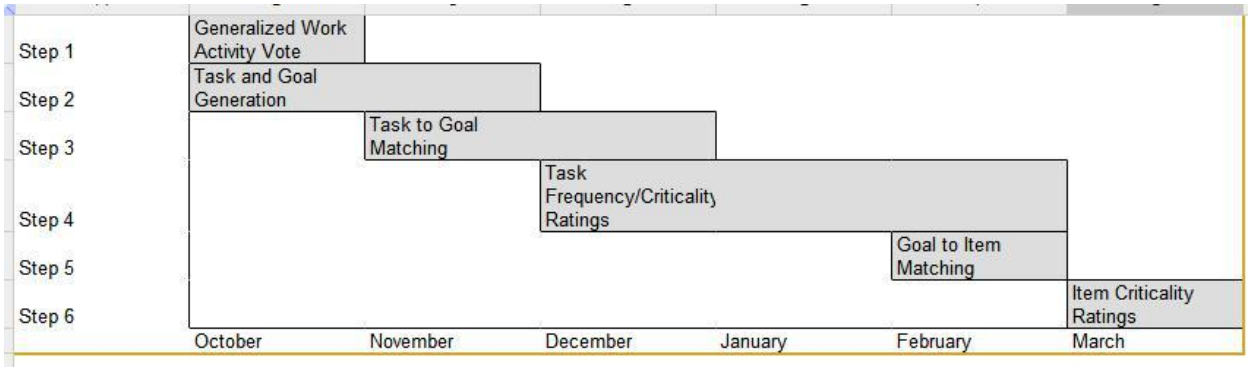


Figure 3.1. O*NET Methodology Timeline

The elicitation method used in this study, and piloted during the development of a Job Competency Model for Advanced Threat Response (Tobey, forthcoming) is shown in Figure 3.2. The traditional elicitation process was altered by adding vignettes and more detailed mission definition to provide scaffolding that could help spur the generation of task descriptors by panel participants. The provision of increased structure in conjunction with revisions to the collaboration infrastructure reported elsewhere (Tobey et al. forthcoming) appeared to support a further acceleration of the process. In just six weeks a comprehensive task list was developed suitable for surveying the profession. Moreover, while the modified US. OPM process produced approximately 120 tasks across two job roles, the JPM process approach to be used for developing the Smart Grid Cybersecurity Job Performance Model produced a list of 706 tasks across four functional roles.

Figure 3.2. Job Performance Model Process Methodology Timeline

In the next section we will present and discuss the results of the first four sessions.[2] The overall goal of these sessions was to produce a Job Description Report that would identify the context, mission, roles, and processes involved in smart grid cybersecurity. This job definition was then used to develop a JAQ by elaborating and evaluating the most critical job responsibilities and tasks.

[2]The session objectives and participation of panel members for each of the sessions conducted through the date of this report are available from the author upon request.

4.0 Job Description Report

4.1 Job Classification

The iterative process described above begins at the abstract level typical of job descriptions and individual development plans. Traditional job task analysis starts with a taxonomy of GWAs but such high-level descriptors have been found to be poor discriminators of jobs (Gibson et al. 2007). The result is a job description that is frequently used to develop employment inventories and recruiting advertisements. Competency modeling may extend these lists to produce guides for training and testing or certification underlying individual/personal development plans. Existing job or functional role taxonomies and definitions are consulted to identify areas of alignment or misalignment in current conceptions of a job. Recruitment advertisements and performance evaluations are evaluated for role definitions, responsibilities and capabilities expected to be determinants of performance. Finally, stories of critical incidents demonstrating either exemplary performance (use cases) or errors and omissions ("mis-use" cases) are collected. Collectively, the job descriptions, development plans, performance evaluations, and critical incident descriptions establish the job context.

The word "incident" in job task analysis is not simply an event requiring a response, as is frequently the case in the cybersecurity domain. Instead, it represents a defining moment in which the differences in skill level are notable in clearly identifiable outcomes of action taken. This may be an actual or a potential event, and includes not only sense-and-respond situations but also proactive or sustaining events critical to achievement of goals and objectives. Hence, the word "incident" here is more broadly defined. Accordingly, John Flanagan, the inventor of the critical-incident technique, defined an incident as:

> "…any observable human activity that is sufficiently complete in itself to permit inferences and predictions to be made about the person performing the act. To be critical, an incident must occur in a situation where the purpose or intent of the act seems fairly clear to the observer and where its consequences are sufficiently definite to leave little doubt concerning its effects." (Flanagan 1954, p. 327).

We define a "vignette" as the collection of: a critical-incident title or description; when the incident occurs (frequency and/or action sequence); what happens during the incident (problem or situation); who is involved (entities or roles); and where the incident might happen, now or in the future (systems or setting). Further definition of a vignette might include why it is important (severity or priority of response) and how the critical incident is addressed (method or tools that might be used). A collection of vignettes and the associated job context form the basis for developing a Job Classification Report that may be used for comparison with other jobs or to identify when an individual is performing the job as classified.

4.2 Job Roles and Responsibilities

The roles identified during the Job Classification step are categorized into functional roles. The functional roles are discussed with, or ranked by, the panel of SMEs who then select one or more functional roles to focus on for the remainder of the modeling process. This selection of functional roles establishes an important boundary condition for the JPM. A guide to the selection process may be the

roles targeted by a sponsoring organization or roles identified in an existing competency model, such as the NICE Information Assurance Compliance Specialty Area ("NICE Cybersecurity Workforce Framework" 2011) in the cybersecurity profession.

During the next step, the SME panel is asked to develop a list of responsibilities for the selected functional role(s) for each vignette. These responsibilities may bear resemblance to the tasks defined during a job task analysis or competency model, but in JPMs they represent the starting point for decomposing a job into finer levels of detail. In effect, the responsibilities align with job duties often listed in job descriptions or performance evaluations. One fundamental difference between job performance modeling and previous approaches is the use of multiple roles at this step in the process. Guided by the vignette description, the panel defines responsibilities across the entire group of functional roles determined by the panel to provide the role boundary for the JPM process. This approach enables elicitation of job overlap and the establishment of collaborative requirements of the job where responsibilities are duplicated across functional roles.

During the final step for eliciting roles and responsibilities, the SME panel collaborates on developing a list of expected outcomes, both positive (best practices) and negative (errors and omissions) for each role involved in each vignette. These outcomes can serve to establish both learning objectives for training programs and situational judgment outcomes for assessment instruments. In the former case, the mis-use cases (errors and omissions) are especially important. By identifying likely errors, a training program may be developed that enables "failing forward" where common mistakes are addressed by appropriate remedial instruction modules and practice exercises that guide the learner through a problem-based approach to deliberate practice. Research has shown that deliberate practice is necessary to accelerate proficiency. In the case of situational judgment test development, the mis-use cases can form a set of distractor choices to make sure that the test taker has developed sufficient understanding, or is able to demonstrate skilled performance during the PPA described above.

4.3 Goals and Objectives

Measurement of job performance requires the establishment of a criterion which determines the level of success achieved (Berk 1980). Each job has a mission—a primary set of actions that are expected to produce valued results. These primary goals are often accomplished through the pursuit of secondary goals, and secondary goals through other subsidiary goals, collectively forming a goal hierarchy (Cropanzano et al. 1993; Miller et al. 1960; Powers 1973; Wicker et al. 1984). Consequently, to establish a performance model it is important to elicit multiple levels of goals to be accomplished in a job. Further, research has shown that each goal definition should specify clear measures of performance across a broad range of varying degrees of effort and difficulty (Locke et al. 1981). Accordingly, the SME panel is asked to contribute goal definitions that indicate whether a goal is primary, secondary, or tertiary. For each goal an objective measure is provided as the criterion by which performance will be assessed. Finally, specific criterion-based outcomes are specified at five levels of performance based on the PRISM method of goal setting (Tobey et al. 2007): Premier, Robust, Improved, Satisfactory, and Moot. Responsibilities are then sorted into these goal categories to prepare for the next stage of the JPM process.

5.0 Task Analysis

Task analysis in the development of a JPM marks an important departure from traditional approaches discussed above. Our method is based on recent advances in cognitive task analysis methodology (Crandall et al. 2006) which expand the depth of incident descriptions that are critical to understanding and predicting job performance. While improving the elicitation of critical knowledge and skills, this process usually requires dozens of hours of interviewing and transcribing to develop a rich description. Thus, we need to adapt this approach to the conditions facing smart grid cybersecurity professionals, in which the context, challenges, and required responses change rapidly. Accordingly, we developed and tested a new approach with the Smart Grid Cybersecurity panel based on group decision support techniques that have been found to repeatedly and predictively produce substantial increases in the quality and quantity of creative productivity in brainstorming groups with cycle-time reductions of 80% or more (Briggs et al. 2001; Nunamaker et al. 1997).

During the facilitated elicitation sessions, panel members begin by documenting recollections of events or hypothetical situations facing smart grid cybersecurity professionals, called a *vignette*. A "vignette" is defined as the label given to each event. They elaborate these brief descriptions by identifying the goals that must be accomplished to address each of these situations. Next, they develop a matrix of responsibilities that the SME panel determines are appropriate to be fulfilled by the job roles in accomplishing each goal. Following that, the tasks that form the steps for fulfilling the responsibilities are enumerated for each functional role. Optionally, published methods or software tools may be identified for each task. Consequently, the JPM represents the documentation of how the job is performed, rather than simply a description of job responsibilities. The detailed list of tasks is then assembled into a survey to determine the relative frequency and importance for individuals at entry, intermediate, and master levels of performance in the JAQ.

This section will describe the facilitation techniques used to support the SME panel virtual sessions and weekly assignments. We will begin by reviewing definitions of key terms and then outline the elicitation and analytical procedures for selecting goals, roles, responsibilities, and tasks. The next section will provide a brief overview of how this information will be used to develop and administer a JAQ that will provide the data for an exploratory factor model of job performance in the targeted job roles.

5.1 Definitions

In a review of task analysis methods, Schraagen (2006, p. 185) defines the word "task" as "what a person is required to do, in terms of actions and/or cognitive processes, to achieve a system goal." This definition implies several important constructs which need to be elicited from SMEs to fully understand the factors affecting performance on the job. A complete task definition would include detailed *goals*, *objectives*, and job *responsibilities*. Finally, these statements, and those describing tasks, must be written specifically to highlight the *action verb* that indicates the execution of the task. It is often the case, though not a requirement of task analysis, that the action verbs used to describe goals and tasks align with Bloom's taxonomy of action verbs (Anderson et al. 2001; Bloom 1956).

We define a *goal* as a statement that expresses an action that must be successfully completed to accomplish the job mission, or to facilitate the accomplishment of another goal. The goal *objective* is defined as the measurable outcome that establishes the criteria by which the degree of success or

effectiveness may be assessed. *Job responsibilities* are defined as action statements which result in outcome states that may be monitored or assessed to determine whether an objective has been accomplished. Accordingly, responsibility statements use passive verbs, such as "ensure," "follow," or "obtain" that are not included in Bloom's taxonomy.

For example, the SME panel identified the goal "Analyze log files for signs of an attack or compromise" with the objectives (criterion) of "*Percentage of logs that are reviewed*" and the "*Time required to review each source*." Goal accomplishment could be monitored or assessed by the job responsibility "*Ensure incident response and recovery procedures are tested regularly*." The targeted outcomes of this monitoring action would be the percentage of logs being reviewed by these procedures and the time required to conduct each review.

Finally, following the suggestion of Crandall et al. (2006), we apply methods for capturing the SME panelists' stories of cybersecurity events (e.g., Boje 1991, 2001; Tobey 2008) to facilitate a deconstruction of the tacit understanding that experts have of the relationships between goals, objectives, responsibilities and tasks. These methods, and the studies upon which they are based, recognize that expert stories are living, dynamic, interactive constructions between the storytellers and their audience in which the latter do not understand the terse descriptions by which experts communicate with each other (Boje 1991, 1995). Expert stories are not simply holistic constructions requiring interpretation or translation (Czarniawska 1997), but are instead interconnecting fragments that are woven together into a complete perspective only in the presence of an interlocutor (Boje 2008; Tobey 2007). Consequently, in addition to their definition as a classification of who, what, when, where, how or why events occur (see Job Classification section above), *vignettes* are also a collection of story fragments which SMEs construct collaboratively into a multifaceted depiction of an event or scenario requiring skilled performance. These fragments then may be categorized into collections, or *master vignettes*, which experts frequently label using terse phrases such as a "Network Attack" or a "Data Leakage."

5.2 Role and Vignette Selection

The first critical decisions that the SME panel must make are which job roles and which master vignettes will become the focus of the Smart Grid Cybersecurity Job Performance Model Panel. During the sessions in which the vignettes were identified and elaborated, the panel indicated which job roles are involved at each stage and step of the situational response process. A frequency distribution of roles across vignettes can therefore assist in determining which job roles are the most critical, and consequently which vignettes (that heavily involve these job roles) are most relevant for further analysis. Accordingly, we calculate the percentage of steps in which a job role is involved for each of the master vignettes. Those roles which have the broadest involvement across the vignettes will be candidates for selection. This information is presented to the SME panel and they are asked to select, by a consensus of at least two-thirds of panel members, the most critical roles which they believe should be the focus of the initial JPM. Once the panel has made its selection, the master vignettes in which the selected roles collectively have substantial involvement will be selected for further analysis. "Substantial" involvement will be defined as a simple majority (equal to or greater than 50%, rounded to the nearest decile) of steps in which the selected job roles are involved.

5.3 Goal Selection

In the Job Description Report section above we briefly described the panel process for developing a list of goal definitions that guide the elicitation of responsibilities for each job role. A complete detailing of the responsibilities and tasks necessary to accomplish the goals of all smart grid cybersecurity functions would be far beyond the scope and resources of this project. Therefore, although a broad list of goals will facilitate establishing clear boundaries for the smart grid cybersecurity profession, we need to focus on a few select critical goals to guide the modeling of job performance. In order for this initial JPM to have the greatest impact it is desirable for the selected goals to effectively address the largest number of master vignettes identified by the panel. Consequently, the SME panel individually assigns the goals elicited during a previous session to the list of master vignettes which involve the selected job roles. We select for further analysis those goals which the panelists rank as important. The importance ranking is based on a majority percentage of panelists (rounded to the nearest decile) indicating that the goal was related to successful performance in at least three master vignettes.

5.4 Elicitation of Responsibilities for the Selected Roles and Goals

The selected roles and the vignette steps in which they are involved can now be used to assist the SME panel members in brainstorming a list of responsibilities associated with each goal using the VivoWorks VivoInsight[3] idea generation tool. The VivoInsight collaboration tool includes a feature called *Follow Me* which enables a facilitator to synchronize participant displays in a virtual session. Moving down the goal list one at a time, the facilitator presents an entry screen to each participant to elicit a list of responsibilities. The goal statement is displayed at the top of the screen. The selected job roles and the vignette steps are shown on the left to prompt idea generation. Below an entry box where the participant may type a new responsibility statement associated with the focal goal, a real-time feed is shown to allow easy viewing of the contributions of others.

5.5 Task Creation

The creation of a list of tasks necessary to fill each responsibility is facilitated by the VivoInsight Task Creation tool. The facilitator uses the *Follow Me* function to present the same responsibility to all panelists at the tops of their respective screens. In addition to facilitator instructions at the start of the activity, a help video is provided to guide the panelists through the creation of tasks associated with each responsibility. Figure 5.1 shows an example slide from this video. The task elicitation activity begins with the selection of an action verb from the Bloom taxonomy (Anderson et al. 2001; Bloom 1956) that matches an idea for a task that needs to be performed to fulfill this responsibility. After selecting an action verb, a list of current tasks using that verb or its synonyms is shown on the left-hand pane. If the task is already listed, simply clicking on the box next to the task description will add it to the live-feed section below the entry box. If the task is not listed, the remaining portion of the description after the leading action verb may be typed into the entry box and the "Add" button clicked to add it to the live feed (see Figure 5.2). Once all the tasks necessary to fulfill this responsibility have been added to the live feed, the panelists may assign each task to any job role or roles they believe should be involved in executing this task. Clicking the "Submit" circle at the end of the row records their role assignments.

[3] VivoInsight and SiteSpace are Software-as-a-Service programs which are the intellectual property of VivoWorks, Inc. who has approved reference to their copyrighted and trademarked products in this report.

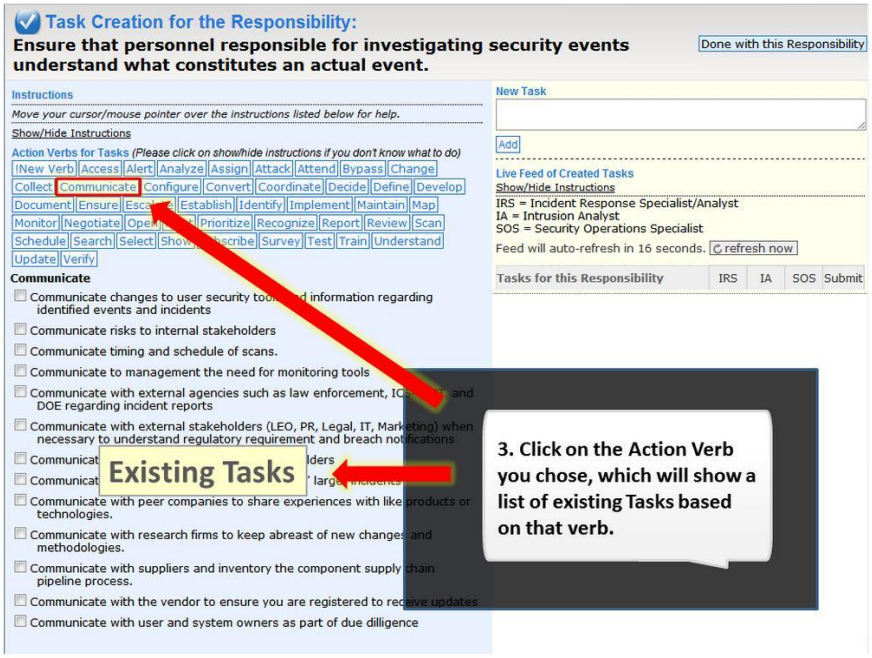


Figure 5.1. VivoInsight Help Video Showing How to Select an Action Verb

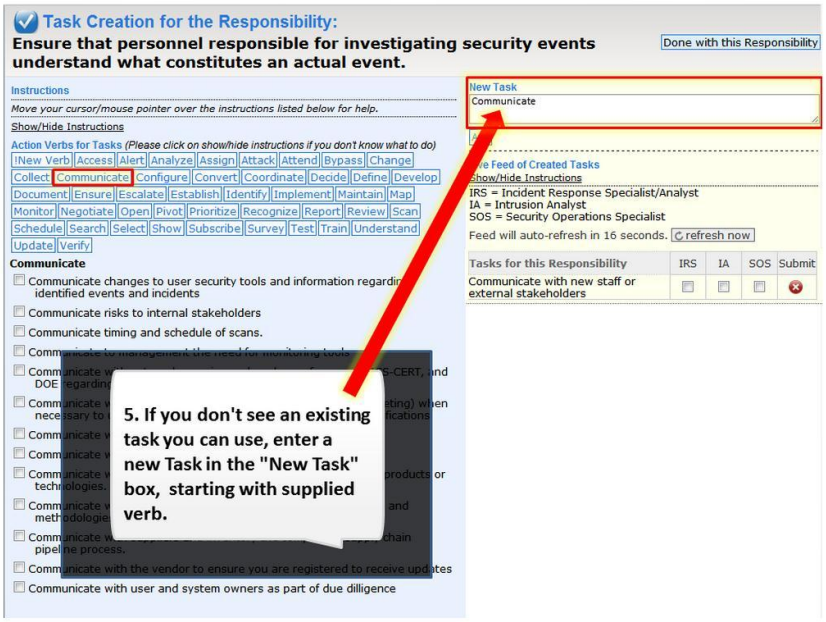


Figure 5.2. VivoInsight Help System Showing How to Add a New Task

6.0 Job Analysis Questionnaire

The JAQ is the primary data collection method for developing a theoretical model of job performance in three smart grid cybersecurity roles: Security Operations, Incident Response, and Intrusion Analysis. Our review of both the smart grid and job analysis literature suggests this is the first comprehensive analysis of smart grid cybersecurity tasks. The task statements contained in the JAQ will be evaluated by nominated SMEs to determine those tasks that are most critical to perform and those tasks which best differentiate between the performance of individuals possessing basic, intermediate, and advanced skills.

The results of the JAQ will be used in several ways. First, by identifying the most critical and differentiating tasks we can better target workforce development programs and investments to accelerate the proficiency of cybersecurity professionals working on the smart grid. Second, the results will be provided to organizations distributing the survey to their members and affiliates, enabling them to compare the responses of their community of practitioners to the overall population and highlighting areas where differences may indicate unique requirements or emphasis for effective job performance. Third, survey results will be published to the entire community of smart grid cybersecurity practitioners to guide individual development plans and self-assessment of skill areas. Fourth, Human Resource managers in organizations employing smart grid cybersecurity professionals can utilize the results to prepare competency maps for purposes of recruiting, workforce planning and development, and performance evaluation. Fifth, the results will support the development of simulation systems that facilitate the transfer of knowledge into skill by enabling individuals to practice the most critical and differentiating tasks. Sixth, the results will inform the development of new technology tools that may lower the skill requirement to perform certain critical tasks that lend themselves to automation. By guiding the skilled performance of novice or apprentice practitioners, these technologies would free valuable expert resources to focus on the more difficult or novel problems. Finally, and perhaps most important, the results will inform development of formative assessments which can be used to identify aptitude, skill profiles, and potential performance of individuals for specific jobs. These assessments will enable improved career paths, team composition, and targeting of learning and practice interventions necessary to secure and defend the smart grid.

A three-phase purposive-sampling strategy combined with random selection of survey groups is used to improve the likelihood of achieving a representative sample of SMEs with experience in one or more of the targeted job roles. Phase one identified respondents obtained through organizations related to smart grid cybersecurity. Phase two will send reminders through these organizational channels but also add individuals who can complete the entire JAQ (i.e., all 37 survey groups) to obtain an adequate sample size and to address grossly unequal distribution of responses across the three job roles. Phase three will identify other channels through which the JAQ can be distributed to address any remaining concerns regarding sample size or representation.

During each phase, a respondent begins by choosing from the list of the targeted job roles (i.e., Security Operations, Incident Response, and Intrusion Analysis) the one that most closely relates to their current position or experience. Upon selecting a role, they are taken to a demographic survey of ten questions (see Appendix B for a listing of these questions). The respondent next receives sequential access to a random selection of three survey pages containing 14 task statements (for an example see Figure 6.1). The respondent may pause the survey at any time and an e-mail will be sent to them allowing them to continue the survey where they left off. Once they have completed the three required

task-statement survey pages, they have the option to continue answering more of the 37 survey pages or exiting the JAQ.

A pilot test of this process using both full and partial responses to survey pages was conducted prior to the beginning of the first phase. The purpose of the pilot JAQ is to review and verify the survey administration process and to evaluate the instructions, task statements, and other survey text. SME panel members and select individuals at PNNL and Sandia National Laboratories were recruited to participate in the pilot JAQ. Results of their analysis are provided in Appendix C along with the list of finalized task statements and a sample section of the survey showing the rating system used to evaluate the task statements.

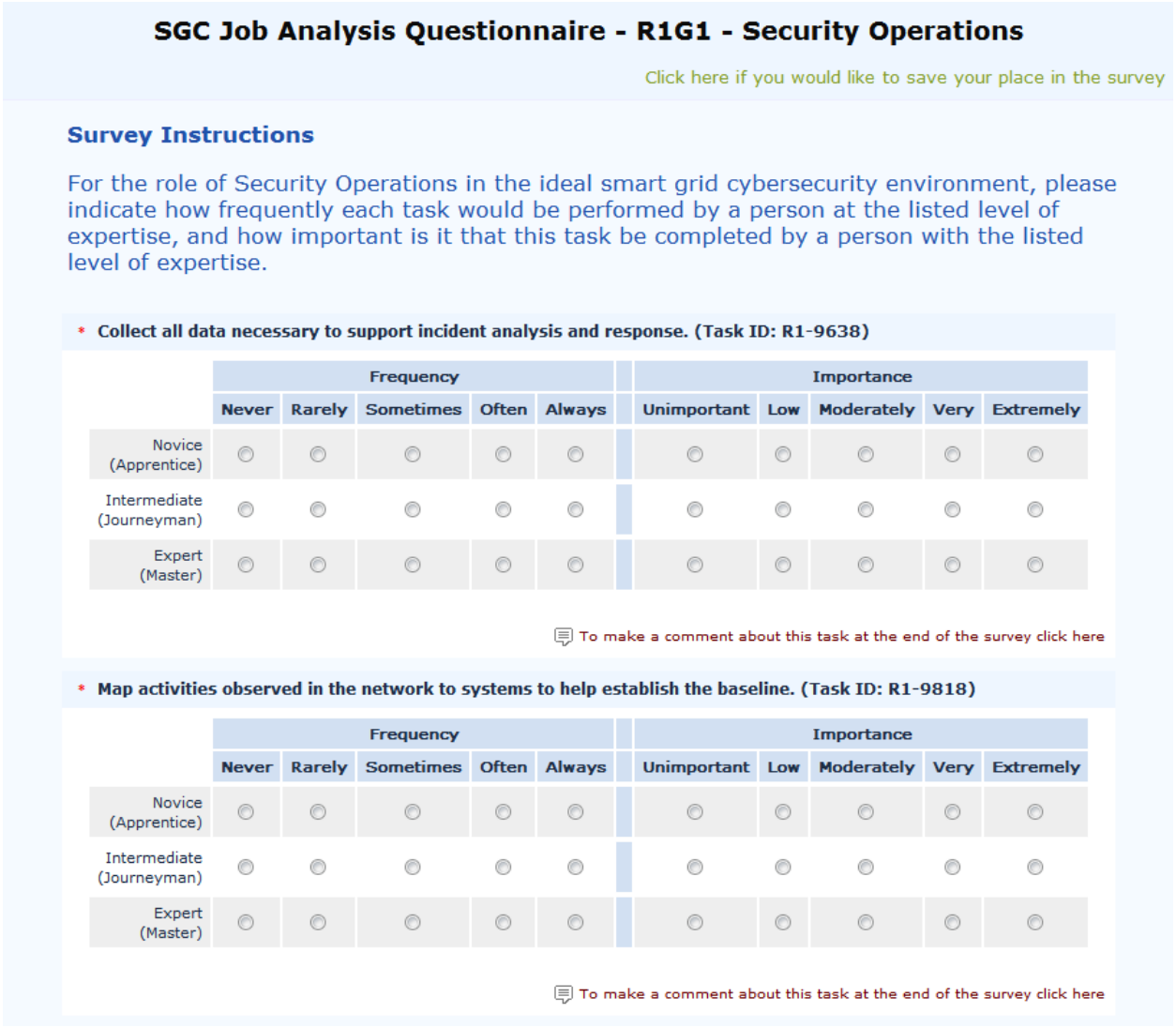


Figure 6.1. Sample Job Analysis Questionnaire Task Statement Survey Page

7.0 The Competency Grid

In the Developing a JPM section above, we outlined a multidimensional framework for understanding an individual's development and position along a learning trajectory from novice to master. This framework, which we called the Competency Box (Tobey, Reiter-Palmon, and Callens, forthcoming), is summarized in Figure 7.1. The purpose of this section is to propose a new method for analyzing job analysis data that will facilitate mapping of an individual's competency development, as well as the tasks that best demonstrate such development, to positions within the Competency Box.

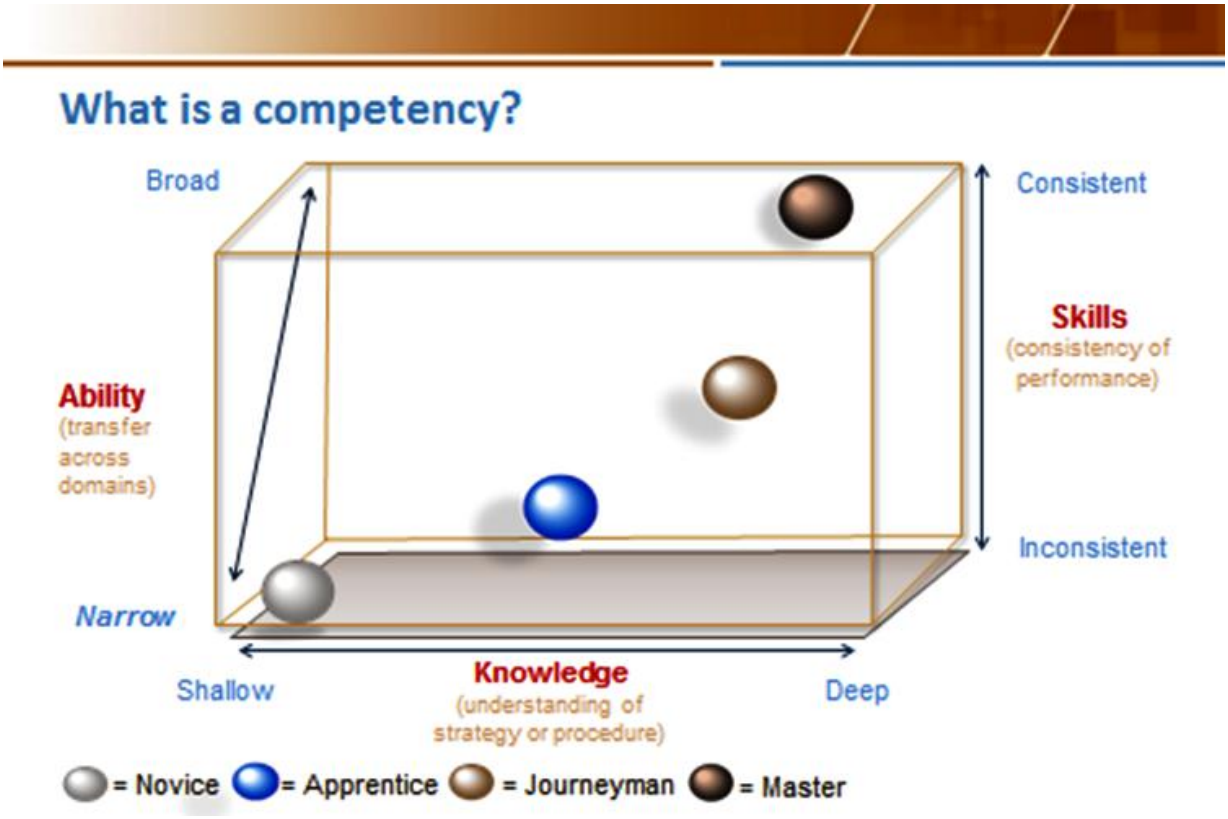


Figure 7.1. The Competency Box

We will begin by reviewing a brief history of the development of competence and intelligence theory and the resulting testing protocols (adapted from Tobey, Reiter-Palmon, and Callens, forthcoming). This review will demonstrate how the Competency Box may resolve long-standing disputes over the identification and development of expertise. Our goal is to develop a technique that can address three important constraints to determining the capabilities of the smart grid cybersecurity workforce:

1. Job performance has not been highly correlated with existing industry measures of competence (Evans and Reeder 2010).
2. Cyber threats are constantly changing and the practice of cybersecurity is still emerging (Assante and Tobey 2011). Thus, measures of past performance are not good indicators of future potential to perform.

3. Given the emergent nature of the workforce, development is of greater importance than selection. We therefore need formative measures that can help to identify those with the aptitude to excel, and that can also be used to validate the interventions that shorten learning curves and help individuals reach their maximum potential as quickly as possible.

7.1 Deriving a Measurable Definition of Intelligence and Competence

The Competency Box model is aligned with findings from research on intelligence, competence, and cognitive neuroscience.

Research on intelligence testing provides insight for the conceptualization of the Competency Box (cf. Ree and Earles 1991, 1993; Ree et al. 1994, Sternberg and Wagner 1993; Carroll 1993; Ackerman 1996). Recent research suggests that intelligence should be a multidimensional construct. Cattell (1963) decomposed general intelligence into fluid intelligence, i.e. the *ability* to learn and encode historical events to information; and crystalize intelligence, i.e., *skills* or habits formed through repeated operation. Based on Carroll (1993) and Cattell (1963), Ackerman (1996) produced a four-factor model that differentiated between processing, personality, interests, and knowledge. Similarly, we can adapt Ackerman's model to better understand the Competency Box structure and how it may help define what intelligence (or competence) is and how to measure it. Knowledge in Ackerman's theory clearly maps to the knowledge dimension of the Competency Box as it measures the degree of understanding one has gained about a specific domain. Processing relates to abilities as they facilitate perceptual speed, memory span, spatial rotation and other generalizable capabilities that enable transfer of knowledge and skill to an unknown or novel situation. The skill dimension of the Competency Box is most aligned with personality in Ackerman's theory. In this dimension, habituated activities generate consistent behavior underlying characteristic performance by which others ascribe a personality profile to someone. However, unlike Ackerman's model, we propose that interest is not actually a dimension of intelligence. Instead, interest represents the state of arousal that underlies the activation of all three dimensions of the Competency Box, determining whether ability, knowledge, or skill are enacted in a particular situation (Tobey 2007, 2010; Tobey and Benson 2009; Tobey and Manning 2009; Tobey et al. 2010).

The Competency Box model also draws insight from research on competence. Anderson (1993) theorized that two components of competence, declarative knowledge and procedural skill, should be measured independently since they involve different cognitive functions and therefore. Proctor and Vu (2006) argue that during skill acquisition, a "hierarchy of habits" forms, thus resulting in consistent performance as a result of practice. These skills are differentiated from the algorithmic approach taken in performing tasks on the basis of what we might call *mere* knowledge. With sufficient and deliberate practice (Ericsson 1996), knowledge is converted into "holistic representations" (Proctor and Vu, p. 269) that become automatically retrieved when needed. The Competency Box model suggests that these patterns of memory formation are the instantiation of a skill in neural form, and their automatic execution ensures consistent performance that can be measured.

Cognitive neuroscience studies show support for the Competency Box dimensions and separate measurement of knowledge, skill, and ability, as well as the activating mechanism of arousal. For instance, Markowitsch (2000) found that the location of activity in the brain shifts with time and practice, driving the formation of networks that connect the diverse regions of the brain involved in the task. Other studies have found that these networks are restructured over time to maximize flexibility while

minimizing the distance and energy required for neuronal communication (Bassett and Bullmore 2006). As the neural network coalesces, links form between higher and lower brain centers (Joel 1999) that may trigger behavior outside conscious awareness. In the end, these networks may become sufficiently optimized into a behavioral sequence, a stepwise activation of the entire neural network, which is triggered by a single neuron based on release of a "command" hormone (Kim et al. 2006). In turn, these command hormones are controlled by a part of the brain usually associated with motor or "non-cognitive" functions, but which was found to be activated during conditioned and intuitive responses (Lieberman 2000). A previous study discovered that this unconscious, instantaneous execution of neural patterns could be identified with behavioral and physiological methods (Tobey 2001).

In summary, skilled performance is distinguishable from *mere* knowledge of a task and the ability to adapt knowledge or skill to address a novel domain. The Competency Box model assumes that fluid-intelligence tests measure abilities, while crystallized-intelligence tests must be devised to separately measure declarative knowledge and procedural skills. The former may be measured using traditional proficiency tests, but the latter requires a test of judgment, decision making, and action choices typical of situational judgment tests (McDaniel et al. 2001; McDaniel and Whetzel 2005) and performance-based tests.

7.2 The Role of Motivation and Prospective Memory

The Competency Box implies that the certification of competence requires, at a minimum, measures of proficiency (knowledge), performance (skill), and potential (ability) for each task. For example, measuring competency at performing a vulnerability scan would involve testing the degree of *knowledge* of the procedure and tool functions, the *skill* at performing the scans under varying conditions, and the *ability* to adapt the procedures to detect a previously undiscovered vulnerability. Furthermore, since skill is measured as the degree of performance consistency, each skill test must contain enough trials to determine whether performance vacillates under varying conditions. Prior research on achievement motivation and prospective memory suggest measurement techniques and conditions that can be used to design these skill-test trials.

According to White's (1959) theory of effectance, a moderate state of arousal is an indicator of competent performance. This level of neural activation is sufficient to create a motive state, but not so intense as to evoke attributions of anxiety or fear. Once effective behavior has been executed, the aroused motive state is expected to dissipate quickly. However, if arousal rises to extreme levels, it will tend to narrow responses and reduce exploration of options. This relationship between arousal state and competent performance, known as the Yerkes-Dodson Law, has been found repeatedly in empirical studies.

Interpreting White's effectance theory through the lens of the Competency Box suggests that it is best applied to understanding skill, rather than competence in general. Accordingly, we propose that arousal level and duration are expected to be good indicators of skilled performance. In other words, arousal should peak at higher levels of stress (e.g., time pressure) in experts than in novices or those who are proficient or competent.

Finally, effectance theory and the Yerkes-Dodson Law suggest that tests of skill should include conditions that vary stress levels across a series of trials to determine whether responses become

inconsistent and errors increase as the level of distress rises and extends. This may be accomplished, for example, by varying time pressure and/or noise.

The Yerkes-Dodson effect of stress on performance is similar to the impact of distraction and cognitive load on memory recall for actions required to prepare for, or respond to, a cybersecurity incident. The act of remembering to perform a future action at the appropriate time or in response to a relevant cue is called prospective memory (Ellis 1996). Research supports the theory of a dual-process model of prospective memory (Guynn 2003; Guynn et al. 2000; Scullin et al. 2010), which suggests that remembering to perform a future event (e.g., a step in a cybersecurity response protocol) may occur either through monitoring of cues or through automatic activation of existing memory representations. This dual-process theory of prospective memory suggests that deliberate process will be negatively impacted by distraction while more automated retrieval processes will not be significantly impacted.

The Competency Box framework provides a further clarification of these dual processes and may guide measurement of the prospective memory process engaged during execution of a complex task sequence involving recall of future process steps. The framework suggests that the deliberate prospective memory process involves the use of procedural understanding of the process steps. Individuals using this memory process are operating on the basis of *mere* knowledge. Therefore, during a deliberate retrieval process, arousal levels indicating motivation of intentional action should be higher and remain active longer. The framework also suggests that an automatic prospective memory process involves an automatic retrieval process when there is an activation of habituated memory that consists of the encoded sequence of behaviors necessary to accomplish the goal (Aarts and Dijksterjuis 2000). A recent study by McDaniel and Scullin (2010) found that practice enabled recall of future actions despite increased cognitive load. Their finding suggests that the level of expertise will be directly related to prospective memory performance. Therefore, distractions should cause greater performance detriments for novice and proficient individuals, while experts and masters are able to perform despite having to attend to distractive cues and stimuli.

In summary, the Competency Box framework provides an answer to the call made by Scherbaum et al. (2012) for clearer distinction and measurement of the components of competence. We believe: 1) the framework provides a distinct differentiation between the three proposed dimensions of knowledge, skill, and ability as well as understanding when and how to measure which dimension is activated; 2) these constructs and their measures are consistent with recent discoveries in cognitive science; and 3) the model can be applied to the practical pursuit of developing talent by distinguishing the roles of knowledge, skill, ability, and motivation as factors in predicting performance. Next, we will discuss how this can be used to analyze the JAQ data to facilitate categorization of tasks to produce a CDM that can identify the indicators of fundamental and differential competence. In the second phase of the project we will test the propositions presented here.

7.3 Critical-Differentiation Matrix

The primary lesson learned from intelligence, motivation, and memory studies is that competence is multidimensional. Competency is more than just ability, which is adequately measured by intelligence tests. Competency is more than mere knowledge, which is adequately measured by proficiency tests, such as many of the current cybersecurity certification exams. To the complete the picture, competency measurement requires the identification of fundamental and differentiating skills: those activities which

determine the threshold of performance that all must pass, and those activities that are performed differently with substantively different outcomes if performed by someone with more expertise rather than someone with less skill. This section will describe our approach to determining which tasks may be assessed to best identify these critical and differentiating skills.

Early development of competency studies recognized the importance of identifying threshold and differentiating tasks. In Boyatzis' (1982) landmark study of managerial competence, he discovered clusters of behaviors that were expected of anyone entering the field (i.e., threshold performance) and other clusters of behaviors that differentiated excellent managers from those with less managerial expertise. Similar to the conclusions of Scherbaum et al. (2012) and Senge (1990) discussed above, Boyatzis found that master managers had developed skill in systems thinking and pattern recognition. However, Boyatzis's study showed that master managers have more than cognitive skills. His data suggested two additional forms of competence: emotional intelligence and social intelligence (see also Goleman 1995, 2006). In his most recent review of this work, Boyatzis (2008: 8) summarized the characteristics of behaviors that might be monitored or assessed to indicate development of these threshold and differentiating skills. These tasks should:

- be behaviorally observable
- be differentially supported by neural circuits (i.e., it should be possible to measure knowledge and skill separately)
- be related to specific job outcomes (or goals)
- be sufficiently different from other constructs or indicators
- demonstrate convergent and discriminant validity as indicators of a skill.

Spencer and Spencer (1993: p.15) summarized and extended the work of Boyatzis and created clearer definitions for threshold and differentiating competencies:

- Threshold Competencies: these are the essential characteristics (usually knowledge or basic skills, such as the ability to read) that everyone in a job needs to be minimally effective but that do not distinguish superior from average performers.
- Differentiating Competencies: these factors distinguish superior from average performers.

We constructed the JAQ to meet all five of the criteria above, though further research is required before asserting predictive and construct validity (see Section 15.2, Implications for Future Research, for a discussion of this issue). Following the guidance of Mansfield (1996) on the development of multiple-job competency models, we obtained ratings for each task at three levels of proficiency: novice, intermediate, and expert. The ratings were collected from individuals identified by their organization as qualified to complete the JAQ because of their expertise and experience in smart grid cybersecurity. The background and experience of these respondents is detailed in Section 13, Data Analysis. A pilot test of the questionnaire was conducted with the members of the SME panel to make sure that the task statements and rating instructions were clear and to determine the best way to segment and randomize the survey sections to provide for a reasonably equal distribution of responses while minimizing the time requirement to complete the portion, or portions, of the JAQ in which the respondent elected to participate. Since the JAQ statements and instructions were substantively changed during the process of

conducting the pilot test, the results obtained could not be reasonably compared with the final JAQ and are therefore not reported here.

The collected ratings of frequency and importance at each of these three levels of expertise enable the creation of two measures, criticality and differentiation. These measures may be combined to categorize tasks that should be strongly related to job performance, reflect current ground truth (Assante and Tobey 2011), and can be assessed to determine the position and development path within the Competency Box for individuals or teams.

The *criticality* of a task is defined as the product of the arithmetic means of frequency and importance across all levels of expertise. The *differentiation* of a task is determined by the slope of criticality scores, signifying the frequency that a person with a given skill level must be involved, and the importance of that task for determining the performer's skill level. We define *fundamental* tasks as those that are rated as highly critical but show little differentiation across these three levels of expertise. Performance on these tasks is essential and should be considered minimal entrance requirements for the field. We define *differentiating* tasks as those that exhibit both high criticality and high differentiation scores.

The result of this analysis is a 2 x 2 matrix that we call the Critical-Differentiation Matrix (CDM; Tobey, Reiter-Palmon, and Callens, forthcoming) shown in Figure 7.2. Quadrant 1, shown in black, contains those tasks that have low criticality and low differentiation. These tasks might be labeled "inhibitors" because they actually inhibit determination of the competence. Measuring performance on these tasks would likely attenuate difference scores between individuals as they would constrain variance in test scores. This is not to suggest that these tasks should not be performed, simply that they are not good candidates for development of assessment instruments. Quadrant 2, shown in blue, contains those tasks that are low in criticality but high in differentiation. These tasks might be labeled "esoteric" because while the methods used or results gained by experts differ significantly from those of novices, they are likely to make trivial difference in overall job performance. The final two quadrants are the most relevant for our further analysis. Quadrant 3, shown in green, would list the *Fundamental Tasks*. Quadrant 4, shown in red, would list the *Differentiating Tasks*.

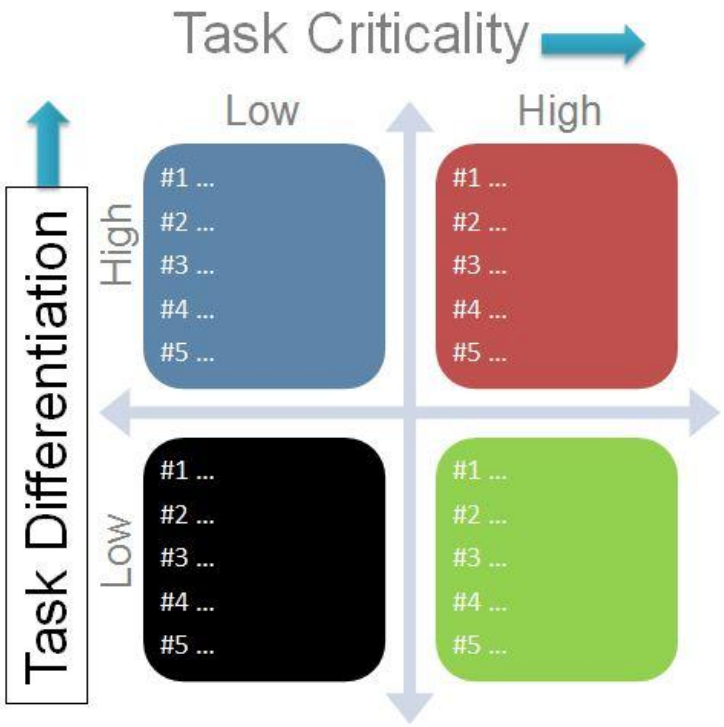


Figure 7.2. Critical-Differentiation Matrix

The CDM guides development of a theoretical JPM by suggesting those tasks which are best performed by individuals who are novices (Quadrant 1), proficient (Quadrant 2), competent (Quadrant 3), and expert (Quadrant 4). This, of course, would be a very crude depiction of the work of smart grid cybersecurity practitioners across the three target job roles. Accordingly, once a sufficient sample has provided input through the JAQ, an exploratory factor analysis of the tasks will be conducted to identify the task clusters which are predicted by the respondents to explain the performance of those at varying levels of expertise.

The next section reviews the results of our research to date. We begin with the results of the literature review followed by the outcomes of the SME panel discussions on vignettes, processes, goals, and tasks involved in smart grid cybersecurity work. We conclude the results section with the status of our analysis of the JAQ responses and the plans to create a CDM and JPM for the three smart grid cybersecurity job roles.

8.0 Literature Review

The NBISE and PNNL research teams, with help from the panel advisors and panel members, assembled the preliminary list of documents shown in Appendix D. These documents will be consulted by the panel members to support their collaboration during the elicitation sessions. Links to uniform resource locators (URLs) or copies of files are made available through the panel portal site in a public Evernote notebook entitled Smart Grid Cybersecurity Panel Literature. The initial bibliography will be expanded during the term of the project.

8.1 Preliminary List of Job Roles

In addition to the literature above, PNNL researchers assembled a library of job requisition and recruitment advertisements for roles expected to play a part in smart grid cybersecurity. The job roles listed in Table 8.1 include a broad range of levels and departmental affiliations, such as analyst, consultant, engineer, researcher, supervisor, and manager. Appendix E includes copies of the job descriptions listed below.

8.2 Integrating the Job Roles and Classification with the NICE Framework

The NICE, led by the National Institute of Standards and Technology (NIST) and the Department of Homeland Security (DHS), is working to establish an operational, sustainable, and continually improving cybersecurity education program for the nation to use sound cyber practices that will enhance the nation's security. The initiative comprises over 20 federal departments and agencies and its work products are to serve as a resource to both the public and private sectors.

Table 8.1. Preliminary List of Job Roles

Job Title	Classification
Manager of Technology	Manager
IT Development Supervisor	Supervisor
Information Security Risk Analyst III	Analyst
Network Security Analyst	Analyst
Senior Software Security Analyst	Analyst
Smart Grid Senior Manager – Professional Services	Consultant
Smart Grid Consultant	Consultant
Protection Emphasis Engineer	Engineer
Substation SCADA Integration Engineer	Engineer
SCADA Protocol Engineer	Engineer
Smart Grid Security Engineer	Engineer
Integrative Security Assessment Researcher	Researcher

There are four components under the NICE initiative, but the work of the Smart Grid Cybersecurity panel is relevant to component three, titled "Cybersecurity Workforce Structure." The lead agency for component three is DHS, which is coordinating its efforts through the National Cyber Security Division. The goal is to define cybersecurity jobs, attraction, recruitment, retention, and career path strategies. The component contains the following Sub-Component Areas (SCAs):

- SCA1 – Federal Workforce (Led by the U.S. Office of Personnel Management)
- SCA2 – Government Workforce (non-Federal, led by DHS)
- SCA3 – Private Sector Workforce (led by the U.S. Small Business Administration, U.S. Department of Labor, and NIST)

The initial work product under this initiative includes a draft framework document that enumerates cybersecurity functional roles across the government and extending into the private sector. This document leveraged work performed by the U.S. Office of Personnel Management (OPM) and others to identify cybersecurity roles and responsibilities across the federal government. OPM surveyed approximately 50,000 federal employees and their supervisors to establish a high-level view of cyber responsibilities and to construct a cybersecurity-specific competency model. The development of an overarching framework has been difficult as cybersecurity encompasses a breadth of disciplines involving law enforcement investigations, intelligence community analysis, IT design, engineering, and operations and cyber defense.

The NICE effort will serve as a focal point for existing and future cybersecurity workforce development initiatives. The program outputs will certainly drive future development efforts and are likely to shape cybersecurity roles over time. The Smart Grid Cybersecurity Project team has been monitoring and engaging with NICE program leadership and activities to align our work and help build upon this nationwide effort. The Smart Grid Cybersecurity Project has partnered with the NICE organizers to improve capabilities and effectiveness of cybersecurity professionals and specifically to align the needs of smart grid cybersecurity roles and responsibilities with this evolving standard competency framework.

The starting point for the alignment begins by evaluating the current draft of the NICE Cybersecurity Workforce Framework. The framework captures 31 high-level cybersecurity specialties across seven categories. The categories include:

- Securely Provision
- Operate and Maintain
- Support
- Protect and Defend
- Investigate
- Operate and Collect
- Analyze

The scope of the Smart Grid Cybersecurity Project places a focus on operational cybersecurity job roles employed by utilities. This focus draws cybersecurity specialties that fall primarily under the

“Operate and Maintain” and “Protect and Defend” categories. The structure of the Framework document identifies and describes a specialty and provides sample job titles. The document further describes applicable job tasks and lists high-level competencies and KSAs.

It is important to note that job roles shown in Table 8.2 below do not necessarily equate to job titles or functional roles defined in the NICE Framework, and several roles may be represented by one specific employee/job position. In addition to the job roles identified in the literature review, panel leadership has suggested that the following roles may also be associated with smart grid operational cybersecurity:

- Advanced Meter Security Specialist (Platform Specialist)
- Security Administrator (certificate management, etc.)
- Security Architect (many architects are involved and consulted in new technology deployments on operational matters)
- Network Security Specialist
- Security Operations Specialist
- Incident Response Specialist/Analyst
- Intrusion Analyst
- Penetration Tester/Red Team Technician
- Risk/Vulnerability Analyst
- Telecommunications Engineer
- Reverse Engineer
- Meter or Field Device Technician

The project team reviewed cybersecurity specialties in the following NICE Framework categories: Securely Provision; Operate and Maintain; Protect and Defend; and Investigate. The review compared Job Performance Panel (JPP) member input and literature review results against the current description of the cybersecurity specialties to include the corresponding task, competencies, and KSA fields. The review included a broader list of utility smart grid related job roles, knowing that the panel will select three to four operational job roles to focus its work. The greatest alignment appears to be with the cybersecurity specialties by category, summarized in Table 8.2. The complete mapping is shown in Appendix F.

Smart Grid Cybersecurity panel members extended the NICE Framework by adding roles and responsibilities that must work closely with cybersecurity specialties to address cybersecurity issues within the context of an organization. Panel members identified job roles within legal and public relations department that consistently interface with cybersecurity functional roles to manage security. The Smart Grid Cybersecurity Project team will provide that feedback to NICE representatives and share the overall alignment review.

It is also important to note that Smart Grid Cybersecurity Project team members have joined the Industrial Control Systems Joint Working Group Workforce Development Subgroup to help align the current framework with the broader industrial control systems (ICS) community and continue to provide relevant input and monitor the progression of the framework.

Table 8.2. Mapping Smart Grid Cybersecurity Job Roles to NICE Framework

Category	Smart Grid Cybersecurity Job Role	NIST Sample Job Title
Securely Provision	Smart Grid Risk & Vulnerability Analyst	Risk/Vulnerability Analyst
	Smart Grid Security Architect	Solutions Architect, Systems Engineer, Systems Consultant, etc.
Operate and Maintain	Smart Grid Meter or Field Device Technician	Technical Support Specialist
	Telecommunications Engineer	Converged Network Engineer, Network Engineer, Telecommunications Engineer/Personnel/Specialist, etc.
	Advanced Meter Security Specialist	Platform Specialist
Protect and Defend	Network Security Specialist	Network Defense Technician
	Security Operations Specialist	Security Operator, IDS Technician, Network Security Specialist
	Incident Response Specialist	Incident Handler, Incident Responder, Computer Crime Investigator
	Intrusion Analyst	Intrusion Analyst
	Penetration Tester/Red Team Technician	Penetration Tester, Red Team Technician, Ethical Hacker, Blue Team Technician
	Reverse Engineer	Reverse Engineer

9.0 Vignettes

The SME panel developed a list of vignettes using VivoInsight which supports anonymity for participants, parallel input by participants, and shifting perspectives of the participants through display of others' insights. These features of GDSS are frequently shown to be critical for maximizing the productivity and creativity of problem-solving and brainstorming groups (Nunamaker et al. 1997). In the current study, the panel identified a total of 109 vignettes in 20 minutes, though a few had been created prior to the session by the panel leadership. This represents an idea generation rate of over 5 vignettes per participant. A previous study (Tobey, forthcoming) using the Groupmind IdeaSet online collaboration system which also supports anonymity and parallel input, but where perspective-shifting was constrained by the display design, had shown idea generation rates of 2.5 vignettes per participant during a 20-minute brainstorming session. The user interface of the VivoInsight tool selected for this panel was specifically designed to draw attention to new contributions through highlighting the contributions by other panel members within the focal frame of each panel participant. This may explain the significant increase in creative production which occurred.

These vignettes were then categorized by the type of response required and analyzed to determine those most critical to determining smart grid cybersecurity job performance. The entire list of vignettes identified by the panel is provided in appendices at the end of this report: Appendix G lists those vignettes that are related to maintaining a secure posture through operational excellence, and Appendix H lists those vignettes that are related to effective response to a threat or vulnerability.

These vignette listings were included in a survey to determine the criticality of the vignette. Criticality was defined by how frequently the issue arose (using a 5-point Likert scale ranging from *Never* to *Constantly*) and/or how severe a problem it posed or how high a priority it was that the issue was resolved (using a 5-point Likert scale ranging from *Not a Problem* to *Critical Problem*). Items were determined to be frequent or severe if they had an average rating greater than 3.5. These highly critical vignettes were used to develop job descriptions by defining the roles, mission, responsibilities, and processes necessary for effective performance.

Twenty-six of the 30 panel members responded to the survey, providing a response rate of 86.6%. However, seven of these responses were incomplete and had to be removed from the results, resulting in 19 survey responses. Interrater agreement was calculated using the aWG index (Brown and Hauenstein 2005). The panel responses were found to exhibit a moderate level of agreement (aWG = 0.556) according to LeBreton and Senter (2008, Table 3). Overall frequency estimates showed slightly higher levels of interrater agreement (FREQaWG = 0.582) than estimates of severity (SEVaWG = 0.53). There was slightly greater agreement on noncritical vignettes (FREQaWG = 0.604; SEVaWG = 0.552) than on critical vignettes (FREQaWG = 0.574; SEVaWG = 0.5211), but this difference was not significant ($p > 0.4$ in both cases).

The survey results indicated that 30 vignettes should be archived as they were not critical to maintaining an effective smart grid security posture. The results were reviewed with the panel during the next step in the job performance modeling process to define the context for developing a Smart Grid Cybersecurity Job Description. During this review it was determined that an additional 10 vignettes should be included in the critical list. This final list of critical vignettes was sorted by the program manager, the panel chairperson, and the panel vice-chairperson, into 13 master vignettes (see Appendix I).

While on average there were 6.85 vignettes that served as examples of each master vignette, the number of these example scenarios per master vignette ranged from a low of 3 to a high of 15. The master vignette Network Attacks had the largest number of example vignettes. This was followed by Threat and Vulnerability Management with 11 example vignettes. The master vignettes with the least number of example scenarios were Access Control Maintenance, Phishing Incidents, and Security Testing; each of these had only three examples.

Each of these 13 master vignettes was loaded into a knowledge exchange tool that is available at all times through the VivoWorks SiteSpace portal system. The panelists were asked to: 1) discuss whether the examples listed shared a common set of roles and methods (steps); 2) describe any notable differences; and 3) suggest additional examples necessary to fully define this class of situations or indicate whether an example should not be included in this classification. The unstated purpose of these discussions is to help the panel evolve a common understanding regarding the scope of the job description and exploratory performance model they would be developing. Panelists clearly picked up on the need for setting these boundaries as can be seen in the anonymous posts below provided in the discussion of the Phishing Incidents and Data Leakage and Theft vignettes:

> **PHISHING INCIDENTS**
> *While this is a real threat and occurring [sic] all the time and with greater frequency - is this too far off the main topic for defining key roles for Smart Grid? This is a much larger issue and relates to much more than just Smart Grid.*
>
> **DATA LEAKAGE AND THEFT**
> *Similar to the phishing vignette, how far removed from direct Smart Grid experience are some of these items? These are all significant issues, but some of them need to be dealt with at different levels and/or more holistically and not just as it relates to Smart Grid. Loss of PII is a much larger problem. I am only making the comment to fully understand the actual scope of defining these roles.*

Similarly, a dialogue regarding Substation/SCADA Attacks vignettes questioned whether some of the examples were too broad and whether additional examples were necessary to address smart-grid-specific components, such as substation controls:

> *These vignettes appear to be specifically targetted [sic] at malware or improper physical controls. What about substation specific concerns; e.g. how does a vulnerability or intrusion into a substation control affect that substation, or how does it affect networked substations, etc.*
>
> *Important question as system health or status will ultimately impact grid operation decisions and supporting technology decisions. Real time response decisions are very difficult in operational systems. The coordination, planning, and communication is essential when considering actions that may impact operational systems.*
>
> *The examples given don't really fit the main topic here.*
>
> - *Poisoned Timing Data Input to Disrupt Synchronization: This example can happen at multiple places.*

- *False data input into power system state estimation model: Usually, we run the state estimation at the utility control center.*
- *Rogue devices with wireless communications enabled are being place in multiple substations and accessed remotely by attacker to probe the substation infrastructure and communications links back to the Utility. It is unknown how many substations are affected: It is unclear whether this example is referring to AMI, or wireless SCADA?*
- *Compromised device has maliciously embedded hardware or chipset. Can apply to any equipment placed in the power system.*
- *zero day attack - new malware detected on control system components. This is too broad and can apply to any equipment controlling the power system.*
- *Physical security vulnerability: LAN ports in common areas in Office premises/ Sub-stations/Datacenter allow access to anyone connecting to that port. Also applies to different domains.*

Each JPP must achieve a working consensus on the degree of specificity and scope that is necessary to fully articulate the critical performance factors that will determine success on the job. While the examples above suggest the panel is concerned about too broad a scope, other discussions focused on whether some vignettes had been too narrowly defined by merging together under one master vignette important events that may need to be analyzed separately. The vignettes therefore appear to serve as important artifacts which may help the panel to develop a richer and more robust articulation of the practices through which expertise and skill development affect security posture and effective response. While the ultimate test of this will come in future JPM steps in which the panel develops the list of tasks, methods, and tools, a good example of how vignettes serve as an impetus to a richer understanding is shown in the dialogue around one of the examples categorized into Encryption Attacks. The discussion ranges from whether examples are appropriately categorized to whether the scope needs to go beyond internal staff to include vendors and other external parties:

> *This vignette seems out of place: Running security tests on equipment and software that might brick [sic], reset, or crash a system [188]. Rather than an encryption attack, I think this is a vulnerability-management vignette.*
> *Different vendor networks probably have very different models for handling encryption keys and the PKI in general. These differences will result in very different understandings of what is possible and what is not, and how damaging a key compromise may be… If a vendor has no way of revoking keys the loss of keys is a major problem. If a vendor has well exercised tools for key revocation, then loss of keys is a simple matter of executing the key replacement procedure and carrying out the revocation procedure… I suspect there is a great deal of vendor specific details here.*
> *Some of the current solutions have components that are managed by third-party organizations. Understanding how to manage these situations is going to be critical. Implementors [sic] need to understand how third-party services impact their deployed encryption technologies. They also need to be training on how to interact with these third-party organizations so that these concerns are outlined during acquisition.*

The next sections will discuss further elaboration of these master vignettes by the panel. They began by defining a list of process stages in addition to three common stages that all vignettes share: preconditions, onset, and conclusion. The panel reviewed and expanded the list of job roles and assigned these to each process stage. Finally, they defined a set of goals and objectives which may be used to assess performance in the 13 master vignettes. Collectively, these definitions form the job description for smart grid cybersecurity.

Further elaboration of the master vignettes occurred over the remainder of the first phase of the project. For each stage of the master vignette process, the panel detailed the plot and storyline of the vignette. This included:

- *What* may happen: the situational conditions (tools, systems, software, data asset, identities, products, monitoring, alerting and response systems) and key concepts (what prior knowledge is required)
- *Where* it may happen: the physical location (e.g., office, virtual, plant floor, data center), virtual location (layer of the stack, e.g., network, operating system, application) and organizational level or area (e.g., department, division, workgroup, center)
- *Why* it may happen: breakdown of root cause (specific events) or why actions are taken
- *How* it may happen: the decisions, procedures, options, common errors or best practices.

10.0 Process Stages Defining Functional Responsibilities

The panel began elaborating the master vignettes by listing the stages in which the vignette was likely to progress along with the roles that would need to be involved at each stage (see Appendix J). Each vignette includes three stages by default: preconditions, onset, and conclusion. The "preconditions" stage occurs just prior to the organization becoming aware that the vignette had begun to play out and describes monitoring or other situation awareness functions intended to identify when a vignette has become active. The "onset" stage begins upon the occurrence of the critical event that signals the vignette has begun. The "conclusion" stage occurs upon resolution of the vignette and describes ongoing maintenance of post-vignette conditions.

11.0 Job Role Involvement in Master Vignettes

Each of the above stages was analyzed by the panel members and they assigned roles to each stage. An analysis was performed to determine the nominal (total) and relative (percent of all) assignments that were made for each job role. Appendix K lists each of the job roles and the number of stages within each vignette assigned to this job role. The list is sorted by the total number of stages in which each job role appeared. The top ten roles by a nominal count of assignments collectively represent nearly half of all role assignments. Appendix L lists the relative involvement of roles in the vignettes. This analysis suggests which roles may be the most critical to analyze further as they may have greater responsibility for the overall effectiveness of cybersecurity operations. The SME panel reviewed these analyses and unanimously agreed that further development of the performance model should focus on the three job roles of Security Operations, Incident Response, and Intrusion Analysis.

Once the focal job roles were identified, an analysis was performed to determine the master vignettes in which the selected roles collectively have substantial involvement. Based on the majority involvement rule described in Section 5.2 above, the decision was made to eliminate 5 of the 13 master vignettes from further consideration. The remaining master vignettes in which the three job roles have significant involvement are: Advanced Metering Infrastructure (AMI) Attacks; Client-Side Attacks; Encryption Attacks; Network Attacks; Substation/SCADA Attacks; Network Separation and Attack Paths; Phishing Incidents; and Incident Response and Log Management.

12.0 Goals and Objectives for Assessing Performance

The final component of a job description is a list of goals that the panel believes must be accomplished for effective performance, and the criterion, i.e., objective measure, that will be used to assess such performance. The panel identified a total of 108 goals and sorted them into categories: primary, secondary, and tertiary. Primary goals must be accomplished to achieve the organizational mission. Secondary and tertiary goals must be accomplished to successfully achieve a higher-level goal. This resulted in a list of 27 primary goals (see Appendix M). Each goal description was elaborated using the PRISM method for goal setting (Tobey et al. 2007) to produce a set of outcome indicators that may later be used in assessments and certification exams to determine the relative level of performance.

The SME panel ranked the importance of each goal to achieving an effective response during each of eight selected master vignettes. Appendix N lists the seven goals determined to be most important. Appendix O shows the PRISM definitions for these goals which were edited to be consistent with the Bloom taxonomy of action verbs.

13.0 Data Analysis

Data collection from the JAQ will continue into the second phase of the project. This report provides the preliminary results from data collected through May 22, 2012. In this section we will review information collected about those expressing interest and responding to the JAQ. This will be followed by a brief summary of the trends that appear to be developing through these responses. In the next section we will report a very preliminary set of findings regarding the development of the CDM which, as discussed above, will be the primary analytical tool along with an exploratory factor analysis of the JAQ responses in developing the Smart Grid Cybersecurity Job Performance Model.

13.1 Participants and Respondents

As of the closing date for this report, 129 people had responded to the JAQ (100 male, 23 female, and 6 not reported). Response rates are difficult to measure for internet surveys, but the design of the VivoSurvey™ system did enable us to track the number of people who expressed interest in the JAQ by clicking on the link in their e-mail and accessing the introductory landing page shown in Figure 13.1 below which appeared on the survey system website.

From this landing page the interested participant could elect to participate by clicking on a link to access the demographic survey page. We created two response-rate statistics based on this information. First, we calculated the number of people expressing interest as a percentage of the total number of invitations sent through the various channels distributing the JAQ. However, there was much duplication in these lists, so we include in the calculation of interest only those channels that had at least one respondent access the survey site. We refer to the resulting statistic as the Participation Rate, which was 7% of May 22, 2012. Second, we calculated the number completing the JAQ demographic page as a percentage of the total number expressing interest in participating. We refer to this statistic as the Response Rate. The response rate as of May 22, 2012 was 43.6%.

The participation rate and the response rate were monitored throughout the administration of the JAQ and continue to be an important source for targeting groups most likely to participate. Based on this data, we conducted three waves of survey administration. The first wave was broadly disseminated to approximately 18 trade associations and organizations representing a large number of potential respondents. However, the participation rate from this group was only 3.2%. Consequently, during Waves 2 and 3 of the survey administration our efforts were concentrated on utilities and related organizations that received far fewer invitations but seemed to be yielding much higher rates of expressed interest and response. This second group represents only 741 of the approximately 4,300 invitees, but had a participation rate to date of 25%. Furthermore, the response rate from this group has been fantastic with over 62% of participants becoming respondents to the JAQ. We have begun to further our focus with this group, with webinars planned for select utilities that have committed to have their staff complete the entire JAQ in one or more sittings.

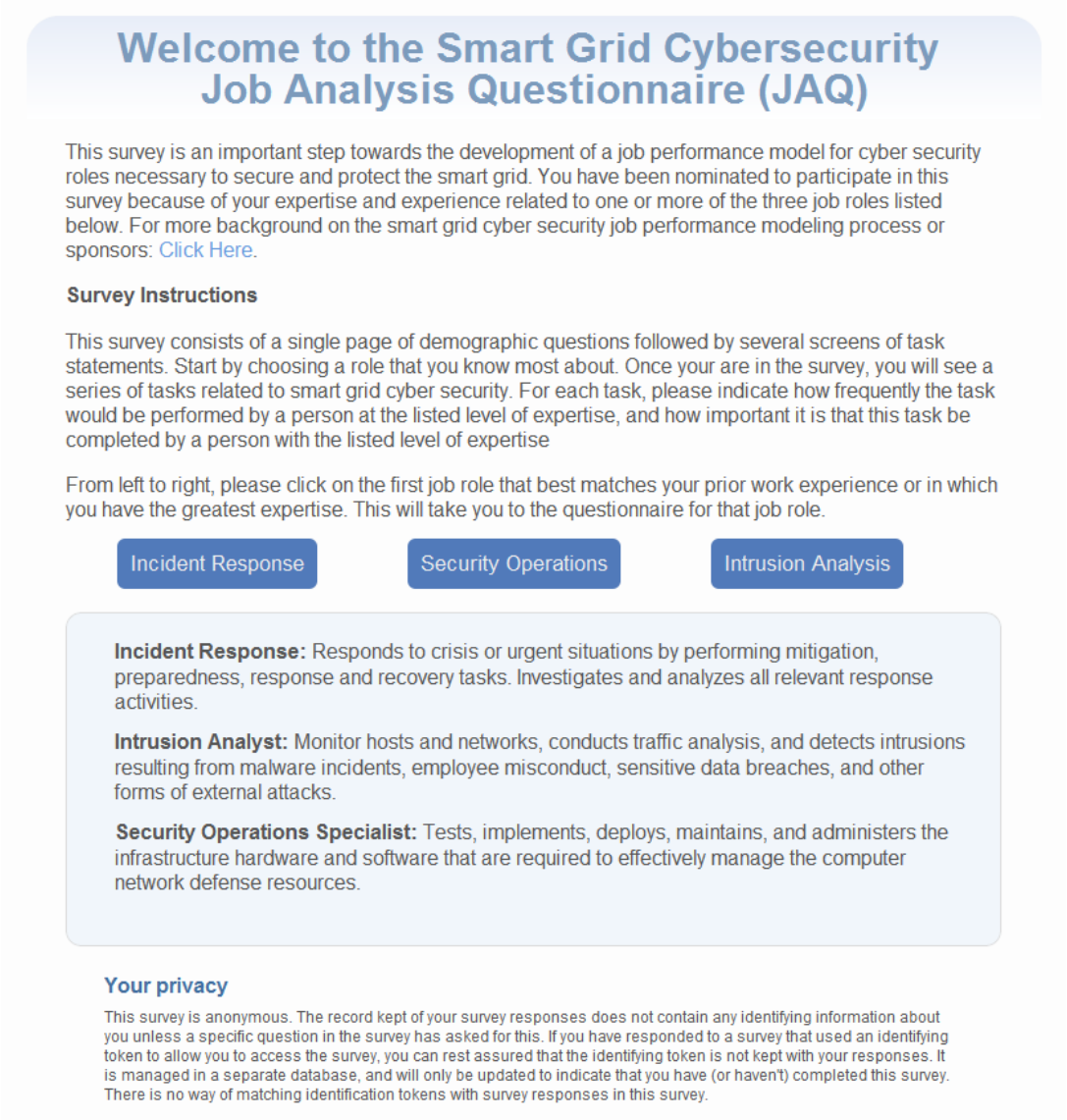


Figure 13.1. Job Analysis Questionnaire Landing Page

13.2 Demographic Survey Responses

The demographic survey collected basic information about the respondents that will be useful for post-hoc comparative analyses of the JAQ data. All the information reported in this section is based on the 129 responses received to date. The 129 respondents are well distributed across age groups (see Appendix P) and come from organizations of various sizes, though most (43% of respondents) work at large organizations with 10,000 or more employees (see Appendix Q). When asked to identify their job title (or titles) from a list of 19 titles, including an "Other" option, the most common job title selected by respondents was *Cybersecurity Analyst* (28.47% of respondents). However, while the remaining job titles were selected by respondents, it is interesting that the second most common choice of respondents was *Other* at 20.44% of respondents (see Appendix R). Note that this question entitled the respondent to select multiple categories, thus the total will exceed 100%. Respondents indicated that they have held their position an average of 4.84 years (standard deviation = 4.68). Finally, the results of respondents' answers

to the two questions on level of experience indicate that our objective to reach those with a broad range of experience was achieved with nearly equal representation from the Proficient, Competent, and Expert categories in cybersecurity (see Appendix S). Responses regarding level of familiarity with smart grid operations have a similar structure but skewed toward the early stages of development in smart grid operations, reflecting the emergent nature of this field (see Appendix S).

13.3 Ratings of Frequency and Importance by Level of Expertise

The main body of the JAQ is the task statement ratings. As explained in Section 7, our goal is to collect sufficient ratings to support inferences regarding the criticality and differentiation of each task in determining the need for and factors affecting performance of individuals with varying levels of expertise. As explained in Section 6, a number of survey pages must be submitted to obtain a complete JAQ submission. As of the closing date of this report, between 10 and 17 responses were received for each task in the JAQ. While this number of responses is far below that needed to effectively analyze and make inferences from the data, we will report some trends that will be interesting to monitor as data collection continues during the second phase of the project.

Table 13.1 provides a brief overview of the responses collected through the closing date of this report. It is important to emphasize that the sample size is currently far too small to conclude anything from these statistics, so they are provided simply to suggest trends that may be worth monitoring as further data is collected. The variance in the current data set is quite broad as demonstrated by the low average agreement using the *a*WG index (Brown and Hauenstein 2005). Currently, when combining ratings across all expertise levels only three items show sufficient agreement in frequency ratings to suggest that a consensus is emerging. Further, though it may be premature, it does appear that we can conclude that the panel did an excellent job of identifying tasks that are essential to job performance. As shown in Figure 13.2, the ratings are highly skewed but resemble a normal distribution within the upper bounds of the rating scale.

Table 13.1. Overall Trends

	Frequency	Importance	
Average AWG	0.263	0.082	
Maximum AWG	0.751	0.514	
Count AWG > .65	3	0	
			Criticality
Overall Mean	3.47	3.29	11.42
Overall Median	3.49	3.31	11.53
Overall Std	1.21	1.36	

An analysis of the ratings by expertise level shown in Table 13.2 suggests further interesting trends are developing. First, it appears that the instructions for rating items are effective, as the ratings are increasing as the level of expertise rises. This should be expected because individuals with lower-level skills should not be as frequently involved and the tasks they perform should be less important in determining the overall skill level of the performer. Also interesting is that the agreement indices vary substantially across the levels of expertise. As reported above, overall levels of consensus on ratings are

very low. However, the frequency ratings on novice and intermediate levels of expertise are much higher. This may reflect that people may easily understand the limitations of early development of expertise, but not be as clear about when experts are required. Alternatively, this artifact might have arisen because the participants are themselves in the early stage of expertise development in smart grid operations, and hence may be more familiar with the roles played by those with developing expertise. Finally, it is also important to note that criticality scores are trending in the expected direction, with the criticality of tasks performed by novices rated much lower than the criticality of those performed by individuals with higher levels of expertise.

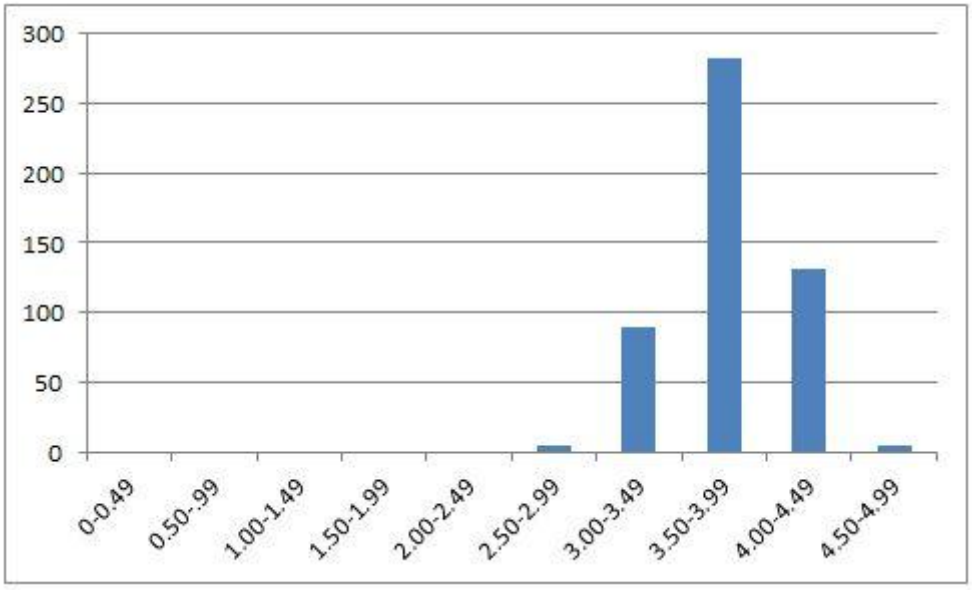


Figure 13.2. Histogram of Frequency Ratings
(The y-axis is the number of items rated in the range listed on the x-axis)

Table 13.2. Summary of Preliminary Job Analysis Questionnaire Results by Level of Expertise

	NOVICE RATINGS			INTERMEDIATE RATINGS			EXPERT RATINGS		
	Frequency	Importance		Frequency	Importance		Frequency	Importance	
Average AWG	0.360	0.168		0.482	0.173		0.230	0.042	
Maximum AWG	0.955	0.766		0.944	0.617		0.814	0.651	
Count AWG > .65	40	5		127	0		12	1	
			Criticality			Criticality			Criticality
Overall Mean	2.86	2.86	8.19	3.64	3.43	12.50	3.89	3.59	13.98
Overall Median	2.91	2.91	8.46	3.67	3.45	12.67	3.91	3.60	14.07
Overall Std	1.21	1.34		1.02	1.28		1.16	1.35	

14.0 Differentiating Performance on Critical Tasks

Based on the responses received to date we can begin to suggest some tasks that should possibly become the focus for Phase II activities and further analysis by the SME panel. While additional data collection is necessary to fully analyze the results, the distribution of responses has been sufficient to develop an initial CDM of tasks. In Section 7 above we defined *criticality* as the product of arithmetic means of frequency and importance across all levels of expertise. We defined *differentiation* as the slope of criticality scores, signifying the frequency that a person with a given skill level must be involved, and the importance of that task for determining the performer's skill level. *Fundamental tasks* were defined as those that are rated as highly critical but show little differentiation across these three levels. Performance on fundamental tasks is essential and should be considered minimal entrance requirements for the field. Finally, *differentiating* tasks are those that exhibit both high criticality and high differentiation scores.

Table 14.1 lists the scores for criticality and differentiation by decile. The range of scores is encouraging and permits experimentation with cutoff scores for development of the quadrant analysis. Currently, especially due to the small sample size, we have elected to focus on those tasks which are found in the top three deciles. The preliminary list of Fundamental Tasks is shown in Appendix T and the Differentiating Tasks are listed in Appendix U. We expect that these lists will change as data is collected, but will provide a good starting point for the initial panel discussions to take place during the first step of Phase II of this project. The lists below are ordered by task identification because insufficient data is available to prepare reliable weights for these tasks at this time.

Table 14.1. Criticality and Differentiation Scores by Decile

Criticality	9.21	10.09	10.58	11.14	11.70	12.22	12.70	13.35	14.17	18.37
Differentiation	0.36	0.52	0.61	0.68	0.74	0.79	0.84	0.93	1.03	3.50
Decile	1	2	3	4	5	6	7	8	9	10

15.0 Conclusion

The NBISE has developed a new approach to job task and competency analysis that is intended to identify the KSAs necessary to successfully perform the responsibilities of three smart grid cybersecurity job roles: Security Operations, Intrusion Analysis, and Incident Response. The overall goal of this first phase of the project was to develop the frameworks and models necessary to promote advances in workforce development to better prepare entry-level candidates for new jobs in the field. The report will contribute to the development of valid curricula and assessments that markedly improve the knowledge, skill and ability of all practitioners involved in smart grid cybersecurity job functions, across the continuum from novice to expert.

The results of the preliminary analysis of job description data has demonstrated the value of shifting away from traditional job analysis and competency models that tend to define jobs at a high level suitable only for descriptive modeling of a job. We proposed a new approach based on an integrative, multidimensional theory of human performance, called The Competency Box. This theory proposes that discrete definition and measurement of knowledge, skill, and ability enables better understanding of learning curves and individual or team positioning within the competency development space. Accordingly, a new approach was developed to elicit the tasks that serve as indicators of progression within the Competency Box.

This project seeks to make important contributions to the science of competency modeling and to the practice of smart grid cybersecurity competence assessment and development:

1. Develop innovations in modeling techniques that may predict the potential of individuals or teams to meet the future demands of a dynamic threat landscape.
2. Develop innovations in the elicitation and definition of tasks that can dramatically shorten the time required to create and maintain detailed competency models to facilitate the inclusion of ground truth regarding vulnerabilities, adversary strategy and tactics, and best practices for detection and defense.
3. Develop a method to produce multiple-role competency models that facilitate the creation of interrelated competency profiles to support the maturation of organizational competence in smart grid cybersecurity teams.

The primary objective of the initial project phase was to use this theory to derive a JPM. Unlike prior descriptive models, JPMs are intended to support predictive inferences through the development of a factor model. A second objective of this initial effort was to develop competency models that could extend these inferences to predict future performance, rather than simply providing an assessment of prior accomplishments or producing normative lists of what a job should entail. Accordingly, we developed innovations in both the evaluation and analysis of tasks, and a method for determining whether a task is fundamental or differentiating based on the results of a detailed JAQ in which practitioners of varying backgrounds and experience rate the frequency and importance of tasks performed by individuals with varying levels of expertise.

The tasks listed in the JAQ were identified through a series of brainstorming sessions with a group of 30 SMEs with broad representation across industry, academia and government. The development of a structured elicitation protocol enabled the SME panel to generate increasing layers of detail in just a few weeks, resulting in detailed lists of job behaviors, processes, and goals supporting effective response in

real-world scenarios, or vignettes. Moreover, the process substantially reduced the cycle time for competency modeling, while grounding the process in the current truths regarding vulnerability, adversary tactics and effective defense techniques. Consequently, we expect the resulting JPM to achieve higher fidelity than previous approaches. Finally, we argue that this ground truth approach to expertise development may help to align education, training, practice, and assessments with the current threat landscape and current best practices for detection and mitigation techniques.

Throughout this process, cybersecurity in the smart grid environment was presumed to involve several functional and job roles. The panel of SMEs identified over 100 situations in which such roles may be involved and how their individual responsibilities related to each other throughout the work practice. A rich description of the three targeted job roles emerged from this preliminary work, based on an innovative process of job model elicitation using vignettes to capture exemplary performance or mis-use cases involving errors or omissions. Thus, another important contribution of JPMs may be the development of team assessments. These models may also foster better understanding of the role of soft skills necessary to initiate, manage, and excel in collaborative problem-solving activities typical of smart grid cybersecurity. Finally, the catalog of the fundamental and differentiating job tasks across multiple job roles may foster the creation of shared libraries for curricula, assessments, and lab exercises that will help develop an adaptive and versatile workforce and identify career path options for individuals based on their competency profile.

The next step will be to conduct a practice analysis in Phase II of the project to guide selection from the list of fundamental and differentiating tasks. These tasks will then be further elaborated using cognitive task and protocol analysis. The primary outcome from this effort should be the development and validation of a set of proficiency and situational judgment item pools, as well as simulation configurations that may be used to validate the construct and predictive validity of these items. The confirmatory analysis performed during this phase will prepare the material necessary to develop a PPA that can distinguish the contribution of knowledge, skill, and ability factors in producing effective smart grid cybersecurity job performance.

15.1 Implications for Workforce Development

The preliminary results of the JAQ suggest that the design of smart grid cybersecurity development interventions would benefit from a focus on critical incidents (Flanagan 1954). Unlike the traditional definition of incidents in the cybersecurity domain, a critical incident is a defining moment in which the differences in skill level are notable in clearly identifiable outcomes of action taken. By integrating assessments, further defined below, which capture the progress against the job mission, modules can be designed which produce development that uniquely assesses the discrete contribution of knowledge, skill and ability in producing performance outcomes.

Our results suggest that in developing smart grid cybersecurity education and training courses or cyber competition content the focus should be directed toward the methods or behavioral sequences explicit or implicit in the responsibilities and tasks to be performed. Moreover, an important outcome that emerged from this study is the importance of focusing on the *right* tasks and the *right* learning objectives—those that are fundamental or differentiating—based on assessment data that indicates the positioning of an individual along the progression from novice to master. Our SME panels informed us that while a single task may occur across multiple vignettes and multiple job roles, the sequence and

method of task execution may be substantially altered by context. Thus, an important implication of our initial study for workforce development is the need for situational judgment tests that may assess whether an individual has selected the right task, using the right method, at the right time. During the next phase of the project we will elaborate on the normative models developed in the current study. We will ask the SME panels to also identify the mis-use cases that can form a set of distractor choices to make sure that the test taker has developed sufficient understanding, or is able to demonstrate skilled performance when faced with the distraction or distress that accompanies simulated or real-world smart grid cybersecurity activities.

Perhaps most important, the research on developing JPMs has shown the value of deliberate practice for accelerating proficiency. Thus, training or future development of assessment instruments should be designed as small, interchangeable modules that increase understanding in performing a single task, allowing modules to be combined in varying ways to target specific areas of responsibility associated with each job role. Practice exercises and assessment instruments should be aligned with each training module to facilitate deliberate practice. Studies have found deliberate practice is essential to accelerate proficiency across a broad range of expertise domains (Ericsson, 1996; Hoffman & Feltovich, 2010). Finally, both proficiency (knowledge) and performance (skill) tests should be included that test not only for understanding but the ability to apply the new knowledge in familiar and unfamiliar settings. In so doing, the course will support the progression of competency from novice to master in the least time possible.

15.2 Implications for Future Research

This has been a preliminary study intended to describe the tasks that indicate performance in three job roles involved in smart grid cybersecurity: Security Operations, Intrusion Analysis, and Incident Response. Our intent was to establish the foundation for expanding research into developing a holistic approach to cybersecurity workforce development. We have previously proposed a model for accelerating expertise development described as Ground Truth Expertise Development (Assante and Tobey 2011).

Future research is needed to develop a more complete and predictive model of both potential performance and competence development. This will require factor analysis of the data collected through the JAQ to produce a construct and measurement model that demonstrates convergent and discriminant validity. The resulting factor model will then need to be confirmed through critical-incident studies. The results of these studies should inform the development of new proficiency and performance assessments aligned with the tasks found to be strong indicators of job performance. Finally these assessments should be validated as predictors of scores in cyber challenges, competitions, and simulations in which the indicator tasks are being performed. Figure 15.1 summarizes these steps and suggests both individual and organizational benefits that may be derived from completion of this framework.

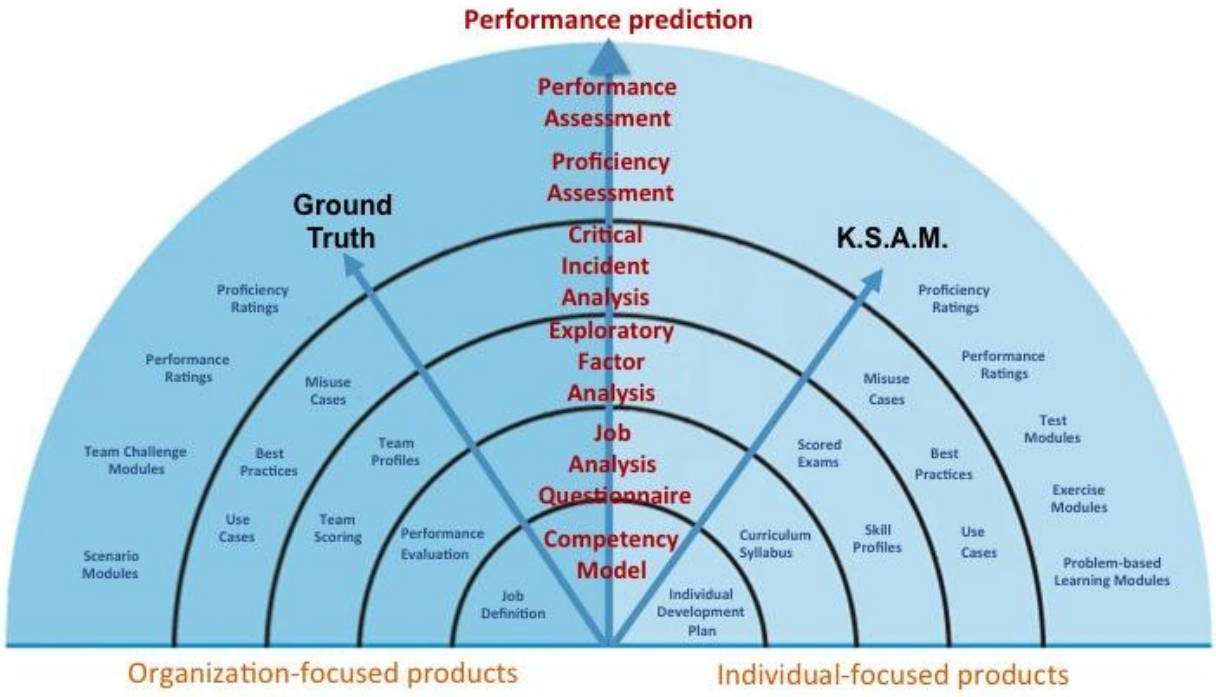


Figure 15.1. Future Research Program

Additionally, since the JAQ was altered significantly during the pilot process, making it inappropriate for comparison with the final JAQ responses, it may be valuable to administer the questionnaire to the SME panel assembled in the second phase of the project. The comprehensive elicitation of tasks during the initial phase of the project resulted in a very lengthy questionnaire. A smaller group of SMEs might produce a comparable response to the public survey which would significantly reduce the effort and shorten the time required to develop a JPM. This second sample should be analyzed to make sure the data would not be biased by non-independence (Kenny et al. 2002) and that it demonstrates sufficient within-group agreement and reliability to support aggregation (Bliese 2000; Klein et al. 2000). Finally, a power analysis should be conducted to determine the response necessary for distinguishing the critical and differentiating tasks.

Future research is also needed regarding how JPMs can be maintained over time, incorporating changes in ground truth on a recurring basis. We need to better understand the dynamics of cybersecurity and its implications for smart grid deployment and operation. Future research should study the diffusion of knowledge related to new threats, vulnerabilities, and best practices. We need to better understand the factors that facilitate broad dissemination, reduce sharing of ineffective practices that may lead to maladaptive skill development, and encourage adoption across the affected organizations.

Perhaps most important is the need to better understand the dynamics of movement within the Competency Box. Future research should include experimental and field studies to identify benchmarks and factors influencing the shapes, slopes, and lengths of learning curves. We need better understanding of how learning curves might differ between and among fundamental and differentiating tasks, and therefore across job roles.

We need better understanding of team competence. Future research might therefore seek to answer questions such as:

- How do the factors that influence team competence differ from those that influence development of individual competence?
- How do varying configurations of team member competence profiles affect team performance?
- How is team performance affected by variance in knowledge, skill, and ability of team members collaborating in accomplishing a task?

Finally, future research may want to explore the role of motivation, arousal, and the configuration of skills that are labeled as traits in producing individual performance and affecting team outcomes.

These, and many more questions, become possible to answer with discrete measurement of the three core dimensions of competence: knowledge, skill, and ability.

15.3 Limitations of the Study

Due to the preliminary nature of the study findings, there are many limitations which could be addressed by future phases of the project or through other research. We cannot possibly review in the space provided a comprehensive list of limitations. However, three limitations are notable, involving cautions on making inferences from our small sample to date, lessons learned from SME panel participation, and coordination requirements for obtaining broader industry support.

First, and perhaps most important, a sufficient sample to support inferential analysis has yet to be obtained. Therefore, no conclusions should be drawn regarding the definition of fundamental or differentiating tasks, JPM factors, or ratings of specific task statements. Lacking an evidence-based list of fundamental and differentiating tasks, future panel activity will need to consider a broader list of tasks in determining the focal areas for conducting a critical-incident analysis. Critical-Incident Analysis is defined as intensive, in-depth interviews with SMEs to document what the experts were thinking, feeling, and doing during a critical incident. A critical incident is a characteristic and challenging event that embodies the most important aspects of the job.

In order to make these panel sessions most effective we strongly encourage continued diligence in obtaining responses to the JAQ, and production of incremental updates to the CDM analysis as the panel progresses. It may prove valuable to have other cybersecurity experts who may not have extensive control-systems experience respond to the JAQ, as many of the tasks are not specific to smart grid deployments and therefore an adequate sample may be obtained quickly.

Second, SME panel participation as discussed in several progress reports has not met our expectations.[4] Consequently, the elicitation of information on the job context, description, and development of the JAQ may have been biased by an insufficiently representative group of SMEs. During the next phase of the project it is imperative that we create a longer list of prospective panel members so

[4] Additional information is available from the author upon request

that replacements can be readily made for panel members who cannot fulfill their participation commitments. We should consider assigning a person with strong connections to the participant pool the specific role of recruitment coordinator, with a quota established for obtaining and maintaining SME participation rates in panel sessions and activities. Further, while anonymity is essential for public surveys, future panel activities, where appropriate, should be attributed in order to facilitate tracking progress and sending reminders to members who have not completed their assignments.

Third, the experience in gathering data from the JAQ suggests that unless more resources and time are allocated to coordination, results may be biased by skewed participation rates across industry groups. The initial wave of JAQ invitations was appropriately broad and comprehensive but produced an insufficient participation rate. Accordingly, two additional waves were initiated that targeted invitations to utility organizations which had provided much higher participation and response rates. However, this purposive sampling approach may bias the results by overweighting responses obtained through disproportionate participation from a few organizations in the sample. During Phase II industry participation will be needed in validating panel opinions (similar to but with much reduced content than the JAQ), forming a subject pool for the experimental studies of work practices, and forming a subject pool for a field study of work practices. The experience in Phase I suggests that recruitment of these participants should begin well in advance of their being needed, a much larger group than needed should be identified, and any and all factors that could inconvenience a participant should be addressed if possible. Additionally, recruitment of participants should be broadened to: 1) include members of other NBISE panels with smart grid experience; 2) expand the distribution channels for recruiting, including LinkedIn® and other social networks; and 3) engage panel chairs and members in recruiting qualified participants. Finally, a project resource with strong ties to the industry (perhaps a PNNL representative) should be accountable to the research team for developing the recruitment plan and managing a quota for participation that provides a sufficient and representative sample for each activity.

Fourth, as briefly discussed in the implications for future research, the comprehensive nature of the task elicitation may have led to the creation of an onerous questionnaire design. Further, the method used to identify the critical and differentiating tasks by adding separate ratings for novice, intermediate, and expert to each judgment of frequency and importance may be more complicated than necessary. Although the preliminary data seems to provide support for this approach in producing expected and significant differences in ratings of tasks across the levels of expertise, it may be productive to consider how the same information may be more efficiently obtained while maintaining the validity and reliability of this important new method for composing a predictive JPM as a replacement for descriptive task analyses and competency models.

Fifth, this study has focused primarily on addressing three key technical gaps in credentialing smart grid cybersecurity professionals:

- competency measurement gap (what competencies should be tested?)
- training gap (transferring training/knowledge to real world)
- certification gap (defining certification framework that integrates knowledge and skill to facilitate predicting operational performance).

However, this phase of the study has not contributed to understanding two additional important deficiencies: the assessment gap and the support gap. The guided process framework for this study, the

Ground Truth Expertise Development model (Assante and Tobey 2011), suggests that these two gaps are essential near-term and long-term workforce development tools, respectively.

The importance of addressing these gaps in the second or third phase of the project should be well understood. Throughout this project and reflected without due acknowledgement throughout this report, we have greatly benefitted from the critical guidance provided by the research team at PNNL, especially the thoughtful review and advice provided by Dr. Frank Greitzer. In closing this report, there is no better way to illuminate the limitations of the current study in addressing the technical needs of the smart grid cybersecurity profession than to quote the insightful comments provided by Dr. Greitzer in his review of an earlier draft of this report:

> ***Assessment gap:*** *A major challenge for assessment is to construct tests that accurately differentiate between simple declarative knowledge versus skilled performance. Assessment and performance measures/metrics are key to the development of an effective certification process. It is clear that certification is the primary focus of work on this project to date. My previous critique of the project plans and approach suggested that it is premature to judge the project's potential for addressing the assessment gap. The report clearly identifies previous research and technical issues surrounding this need—it is by no means a problem that has been solved in current practice. As the scenarios become specified in more detail, the challenge will be to specify KSAs in a sufficient level of detail to yield operational definitions of expected behavior, with associated performance measures, to inform this analysis. I have previously stated that this is the most difficult challenge facing the program. The report alludes to the relevance of the recognition-primed decision making (RPDM) framework (Gary Klein's work)—this should offer some help in structuring an approach to the problem, particularly with regard to inferring mental models that may be useful to help distinguish varying levels of understanding (Greitzer, Podmore, Robinson & Ey, 2009).*
>
> ***Support gap****: As noted in my previous reviews, the documentation of the methodology to date does not provide a specific description of how the approach will address the* ***Support gap*** *by identifying potential decision support tools to enhance performance. Nevertheless, the systematic approach being used to break down tasks into lower-level constructs appears to offer good potential to address the support gap, since the identification of KSA requirements and learning objectives that inform an accelerated learning paradigm can also be examined as possible requirements or objectives that may be applied to tool and/or enhanced visualization development. To date, the concepts and requirements derived through the interactions and knowledge engineering activities with SMEs have <u>not</u> been specifically applied to inform tool development (decision support).*

As I said in previous Notes, the devil is in the details—but given the work to date I would say that the potential for addressing the support gap has improved based on the work described, even though there has not yet been a sufficiently detailed description of assessment methods and metrics that can inform certification methods and metrics.

16.0 References

Aarts H and A Dijksterhuis. 2000. "Habits as knowledge structures: Automaticity in goal-directed behavior." *Journal of Personality and Social Psychology*, 78(1)53-63.

Ackerman, PL. 1996. "A theory of adult intellectual development: Process, personality, interests, and knowledge." *Intelligence*, 22(2)227–257.

Anderson LW, DR Krathwohl, and BS Bloom. 2001. "A taxonomy for learning, teaching, and assessing: A revision of Bloom's taxonomy of educational objectives." (Complete ed.) New York: Longman.

Arvey RD, TE Landon, SM Nutting, and SE Maxwell. 1992. "Development of physical ability tests for police officers: A construct validation approach." *Journal of Applied Psychology*, 77(6)996-1009.

Assante MJ and DH Tobey. 2011. "Enhancing the cybersecurity workforce." *IEEE IT Professional*, 13(1)12-15.

Bassett, DS., & E Bullmore. 2006. "Small-world brain networks." *The Neuroscientist*, 12:512–523.

Behrens JT, T Collison, and S DeMark. 2006. "The seven Cs of a comprehensive assessment: Lessons learned from 40 million classroom exams in the Cisco Networking Academy Program." In SL Howell and M Hricko (eds.), *Online assessment and measurement: Case studies from higher education, K-12, and corporate* (pp. 229-245). Hershey, PA: Information Science Publication.

Behrens JT, RJ Mislevy, KE DiCerbo, and R Levy. 2010. *An evidence centered design for learning and assessment in the digital world* (CRESST Report 778). Los Angeles: University of California, National Center for Research on Evaluation, Standards, and Student Testing (CRESST).

Berk RA. 1980. *Criterion-referenced measurement: The state of the art*. Baltimore: John Hopkins University Press.

Binde BE, R McRee, and TJ O'Connor. 2011. *Assessing Outbound Traffic to Uncover Advanced Persistent Threat* (p. 34): SANS Technology Institute.

Bliese PD. 2000. "Within-group agreement, non-independence, and reliability: Implications for data aggregation and analysis." *Multilevel Theory, Research, and Methods in Organizations: Foundations*, extensions and new directions (pp. 349-381). San Francisco: Jossey-Bass.

Bloom BS. 1956. *Taxonomy of educational objectives: The classification of educational goals*. (1st ed.) New York: Longmans, Green.

Bodeau DJ, R Graubart, and J Fabius-Greene. 2010. "Improving Cyber Security and Mission Assurance via Cyber Preparedness (Cyber Prep) Levels." In *Proceedings of the 2010 IEEE Second International Conference on Social Computing*, 1147-1152.

Boje DM. 1991. "The storytelling organization: A study of story performance in an office-supply firm." *Administrative Science Quarterly*, 36:106-126.

Boje DM. 1995. "Stories of the storytelling organization: A postmodern analysis of Disney as Tamara-land." *Academy of Management Journal*, 38(4):997-1035.

Boje DM. 2001. *Narrative Methods for Organizational and Communication Research*. London: Sage Publications.

Boje DM. 2008. *Storytelling Organizations*. London: Sage Publications.

Boyatzis, RE. 1982. *The competent manager: A model for effective performance*. New York: Wiley.

Boyatzis, RE. 2008. "Competencies in the 21st century." *Journal of Management Development*, 27(1):5–12.

Brannick MT and EL Levine. 2002. *Job analysis: Methods, research, and applications for human resource management in the new millennium*. Thousand Oaks, CA: Sage Publications.

Brannick MT, EL Levine, and FP Morgeson. 2007. *Job and work analysis: Methods, research, and applications in human resource management*. Los Angeles: Sage Publications.

Briggs RO, G-Jd Vreede, and JFJ Nunamaker. 2003. "Collaboration engineering with ThinkLets to pursue sustained success with group support systems." *Journal of Management Information Systems*, 19(4)31-64.

Briggs RO, G-Jd Vreede, JFJ Nunamaker, and DH Tobey. 2001. "ThinkLets: Achieving predictable, repeatable patterns of group interaction with group support systems (GSS)." In *Proceedings of the 34th Annual Hawaii International Conference on System Sciences*, 1057-1065.

Brown RD and NMA Hauenstein. 2005. "Interrater agreement reconsidered: An alternative to the rwg indices." *Organizational Research Methods*, 8(2)165-184.

Brown TA. 2006. *Confirmatory Factor Analysis for Applied Research*. New York: Guilford Press.

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(1)225-262.

Carroll, JB. 1993. *Human Cognitive Abilities: A survey of factor-analytic studies*. Cambridge: Cambridge University Press.

Cattell, RB. 1943. "The measurement of adult intelligence." *Psychological Bulletin*, 40(3):153–193.

Cattell, RB. 1963. "Theory of fluid and crystallized intelligence: A critical experiment." *Journal of Educational Psychology*, 54(1):1–22.

Cattell, RB. 1971. *Abilities: Their structure, growth, and action*. Boston: Houghton Mifflin.

Cattell, RB. 1987. *Intelligence: Its structure, growth, and action*. Amsterdam: North-Holland.

Chi MTH, R Glaser, and MJ Farr. 1988. *The Nature of Expertise*. Hillsdale, NJ: Lawrence Erlbaum Associates.

Crandall B, GA Klein, and RR Hoffman. 2006. *Working Minds: A Practitioner's Guide to Cognitive Task Analysis*. Cambridge, MA: MIT Press.

Cropanzano RS, K James, and M Citera. 1993. "A goal hierarchy model of personality, motivation and leadership." *Research in Organizational Behavior*, 15:1267-1322.

Czarniawska B. 1997. *Narrating the Organization: Dramas of Institutional Identity*. Chicago: University of Chicago Press.

Dainty ARJ, M-I Cheng, and DR Moore. 2005. "Competency-based model for predicting construction project managers' performance." *Journal of Management in Engineering*, 21(1):2-9.

Ellis JA. 1996. "Prospective memory or the realization of delayed intentions: A conceptual framework for research." In M Brandimonte, GO Einstein, and MA McDaniel (eds.), *Prospective memory: Theory and applications* (pp. 1–22). Mahwah, NJ: Lawrence Erlbaum Associates.Ericsson, KA. 1996. *The road to excellence: The acquisition of expert performance in the arts and sciences, sports, and games*. Mahwah, NJ: Lawrence Erlbaum Associates.

Ericsson KA. 2004. "Deliberate practice and the acquisition and maintenance of expert performance in medicine and related domains." *Academic Medicine*, 79(10):S70-S81.

Ericsson KA. 2006. "Protocol analysis and expert thought: Concurrent verbalizations of thinking during experts' performance on representative tasks." In KA Ericsson, N Charness, PJ Feltovich, and RR Hoffman (eds.), *The Cambridge Handbook of Expertise and Expert Performance* (pp. 223-241). Cambridge, UK: Cambridge University Press.

Ericsson KA and N Charness. 1994. "Expert performance: Its structure and acquisition." *American Psychologist* 49(8):725-747.

Ericsson KA, N Charness, PJ Feltovich, and RR Hoffman. 2006. *The Cambridge Handbook of Expertise and Expert Performance*. Cambridge, UK: Cambridge University Press.

Ericsson KA and HA Simon. 1980. "Verbal reports as data." *Psychological Review*, 87(3):215-251.

Ericsson KA and HA Simon. 1993. *Protocol Analysis: Verbal Reports as Data*, Revised edition. Cambridge, MA: MIT Press.

Evans K and F Reeder. 2010. *A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters*. Washington, D.C.: Center for Strategic and International Studies.

Flanagan JC. 1954. "The critical incident technique." *Psychological Bulletin*, 51(4):327-358.

Frincke DA and R Ford. 2010. "Building a better boot camp." *IEEE Security & Privacy*, 8(1):68-71.

Gibson SG, RJ Harvey, and ML Harris. 2007. "Holistic versus decomposed ratings of general dimensions of work activity." *Management Research News*, 30(10):724-734.

Goleman, D. 1995. *Emotional Intelligence*. New York: Bantam Books.

Goleman, D. 2006. *Social intelligence: The new science of human relationships*. New York: Bantam Books.

Greitzer FL, R Podmore, M Robinson, and P Ey. 2009. *Naturalistic Decision Making For Power System Operators*. Naturalistic Decision Making Conference, June 2009. PNNL-SA-62694. Pacific Northwest National Laboratory, Richland, Washington. Also published in the *International Journal of Human Computer Interaction* (Special issue on Naturalistic Decision Making with Computers) 2010, 26(2), 278-291. PNNL-SA-64674.

Guynn MJ. 2003. "A two process model of strategic monitoring in event-based prospective memory: Activation/retrieval mode and checking." *International Journal of Psychology*, 38:245-256.

Guynn MJ, MA McDaniel, and GO Einstein. 2001. "Remembering to perform actions: A different type of memory?" In HD Zimmer, RL Cohen, MJ Guynn, J Engelkamp, R Kormi-Nouri, and MA Foley (eds.), *Memory for Action: A distinct form of episodic memory?* (pp. 25–48). New York: Oxford University Press.

Hoffman RR. 1992. *The psychology of expertise: Cognitive research and empirical AI*. New York: Springer-Verlag.

Hoffman RR and PJ Feltovich. 2010. *Accelerated Proficiency and Facilitated Retention: Recommendations Based on an Integration of Research and Findings from a Working Meeting*. (p. 377) Mesa, AZ: Air Force Research Laboratory.

Hoffmann MHW. 2011. *Fairly certifying competences, objectively assessing creativity*. Paper presented at the Global Engineering Education Conference (EDUCON), April 4-6, Amman, Jordan.

Jeanneret PR, WC Borman, UC Kubisiak, and MA Hanson. 1999. "Generalized work activities." N Peterson and MD Mumford (eds.). In *An occupational information system for the 21st Century: The development of O*NET* (pp. 101-121). Washington, D.C.: American Psychological Association.

Joel, D. 1999. "The limbic basal-ganglia-thalamocortical circuit and goal-directed behavior: Commentary on Depue and Collins (1999) Neurobiology of the structure of personality." *Behavioral and Brain Sciences*, 22:525–526.

Kenny DA, L Mannetti, A Pierro, S Livi, and DA Kashy. 2002. "The statistical analysis of data from small groups." *Journal of Personality and Social Psychology*, 83(1)126-137.

Kim, Y-J., D Zitman, CG Galizia, K-H Cho, & ME Adams. 2006. "A command chemical triggers an innate behavior by sequential activation of multiple peptidergic ensembles." *Current Biology*, 16:1395–1407.

Klein GA, R Calderwood, and D MacGregor. 1989. "Critical decision method for eliciting knowledge." *IEEE Transactions on Systems, Man & Cybernetics*, 19:462-472.

Klein KJ, PD Bliese, SWJ Kozlowski, F Dansereau, M Gavin, MGriffin, D Hofmann, et al. 2000. "Multilevel analytical techniques: Commonalities, differences, and continuing questions." *Multilevel theory, research, and methods in organizations* (pp. 512-553). San Francisco: Jossey-Bass.

Le Deist FD and J Winterton. 2005. "What is competence?" *Human Resource Development International*, 8(1):27-46.

LeBreton JM and JL Senter. 2008. "Answers to 20 questions about interrater reliability and interrater agreement." *Organizational Research Methods*, 11(4),815-852.

Lievens, F., CL Reeve. 2012. "Where I–O psychology should really (re) start its investigation of intelligence constructs and their measurement." *Industrial and Organizational Psychology*, 5(2):153–158.

Lievens F, JI Sanchez, and W De Corte. 2004. "Easing the inferential leap in competency modeling: The effects of task related information and subject matter expertise." *Personnel Psychology*, 57(4):881-904.

Locke EA, KN Shaw, LM Saari, and GP Latham. 1981. "Goal setting and task performance: 1969-1980." *Psychological Bulletin*, 90:125-152.

Long JS. 1983. *Confirmatory Factor Analysis: A preface to LISREL*. Beverly Hills, CA: Sage.

Mansfield, RS. 1996. "Building competency models: Approaches for HR professionals." *Human Resource Management Journal*, 35:7–18.

Markowitsch, HJ. 2000. "Neuroanatomy of memory." *The oxford handbook of memory* (pp. 465–484). New York: Oxford University Press.

McDaniel MA and GO Einstein. 2000. "Strategic and automatic processes in prospective memory retrieval: A multiprocess framework." *Applied Cognitive Psychology*, 14:S127–S144.

McDaniel, MA., FP Morgeson, EB Finnegan, MA Campion, & EP Braverman. 2001. "Use of situational judgment tests to predict job performance: A clarification of the literature." *Journal of Applied Psychology*, 86:730–740.

McDaniel, MA. & DL Whetzel. 2005. "Situational judgment test research: Informing the debate on practical intelligence theory." *Intelligence*, 33:515–525.

McCormick EJ. 1979. *Job analysis: Methods and Applications*. New York: AMACOM Books.

Miller GA, E Galanter, and KH Pribram. 1960. *Plans and the Structure of Behavior*. New York: Henry Holt and Company.

Mislevy RJ. 1994. "Evidence and inference in educational assessment." *Psychometrika*, 59(4):439-483.

Mislevy RJ. 2006. "Cognitive psychology and educational assessment." In RL Brennan (ed.), *Educational measurement* (4th ed., pp. 257-305). Westport, Ct.: Praeger Publishers.

Mislevy RJ and R Bock. 1983. *BILOG: Item and test scoring with binary logistic models*. Mooresville, IN: Scientific Software.

Mislevy RJ, LS Steinberg, and RG Almond. 1999. *On the roles of task model variables in assessment design*. Los Angeles: National Center for Research on Evaluation, Standards, and Student Testing, Center for the Study of Evaluation.

Morgeson FP and EC Dierdorff. 2011. "Work analysis: From technique to theory." In S Zedeck (ed.), *APA handbook of industrial and organizational psychology* (1st ed., pp. 3-41). Washington, D.C.: American Psychological Association.

NICE Cybersecurity Workforce Framework. 2011. Retrieved October 30, 2011, (September 20, 2011) from http://csrc.nist.gov/nice/framework/

Nunamaker JFJ, RO Briggs, DD Mittleman, DR Vogel, and PA Balthazard. 1997. "Lessons from a dozen years of group support systems research: A discussion of lab and field findings." *Journal of Management Information Systems*, 13(3):163-207.

Offermann L and M Gowing. 1993. "Personnel selection in the future: The impact of changing demographics and the nature of work." In N Schmitt and WC Borman (eds.), *Personnel selection in organizations* (1st ed., pp. 385-417). San Francisco: Jossey-Bass.

Parry S. 1996. "The quest for competencies." *Training*, 33:48-54.

Powers WT. 1973. *Behavior: The control of perception*. Chicago: Aldine.

Proctor, RW. & KPL Vu. 2006. "Laboratory studies of training, skill acquisition, and retention of performance." *The Cambridge Handbook of Expertise and Expert Performance* (pp. 265–286). Cambridge, UK: Cambridge University Press.

Ree, MJ. JA & Earles. 1991. "Predicting training success: Not much more than g." *Personnel Psychology*, 44:321–332.

Ree, MJ. & JA Earles, J. A. 1993. "g is to psychology what carbon is to chemistry: A reply to Sternberg and Wagner, McClelland, and Calfee." *Current Directions in Psychological Science*, 2:11–12.

Ree, MJ, JA Earles, & MS Teachout. 1994. "Predicting job performance: Not much more than g." *Journal of Applied Psychology*, 79:518.

Reiter-Palmon R, M Brown, DL Sandall, C Buboltz, and T Nimps. 2006. "Development of an O* NET web-based job analysis and its implementation in the US Navy: Lessons learned." *Human Resource Management Review*, 16(3):294-309.

Ryan JJCH. 2011. "Cyber security: The mess we're in and why it's going to get worse." In L Hoffman (ed.), *Developing cyber security synergy* (pp. 37-45). Washington, D.C.: Cyber Security Policy and Research Institute, The George Washington University.

Sanchez JI and EL Levine. 2001. "The analysis of work in the 20th and 21st centuries." In N Anderson, DS Ones, H Sinangil, and C Viswesvaran (eds.), *Handbook of Industrial, Work, and Organizational Psychology* (pp. 70-90). London: Sage.

Sanchez JI and EL Levine. 2009. "What is (or should be) the difference between competency modeling and traditional job analysis?" *Human Resource Management Review*, 19(2):53-63.

Scherbaum, CA, HW Goldstein, KP Yusko, R Ryan & PJ Hanges. 2012. "Intelligence 2.0: Reestablishing a research program on g in I–O psychology." *Industrial and Organizational Psychology*, 5(2):128–148.

Schmidt FL. 1993. "Personnel psychology at the cutting edge." In N Schmitt and WC Borman (eds.), *Personnel Selection in Organizations* (1st ed.). San Francisco: Jossey-Bass.

Schraagen JM. 2006. "Task analysis." In KA Ericsson, N Charness, PJ Feltovich, and RR Hoffman (eds.), *The Cambridge Handbook of Expertise and Expert Performance* (pp. 185-201). Cambridge, UK: Cambridge University Press.

Schuler H. 1989. "Some advantages and problems of job analysis." In M Smith and IT Robertson (eds.), *Advances in selection and assessment* (pp. 31-42). Oxford: John Wiley & Sons.

Schultheiss, OC & JC Brunstein. 2005. "An implicit motive perspective on competence." In A. J. Elliot & C. S. Dweck (Eds.), *The handbook of competence and motivation* (pp. 31–52). New York: John Wiley & Sons.

Scullin, MK, MA McDaniel & GO Einstein. 2010. "Control of cost in prospective memory: Evidence for spontaneous retrieval processes." *Journal of Experimental Psychology: Learning, Memory, and Cognition*, 36:190–203.

Senge, PM. 1990. *The Fifth Discipline: The art and practice of the learning organization*. New York: Doubleday.

Shippmann JS, RA Ash, M Batjtsta, L Carr, LD Eyde, B Hesketh., J Kehoe, K Pearlman, EP Prien, and JI Sanchez. 2000. "The practice of competency modeling." *Personnel Psychology*, 53(3):703-740.

Smit-Voskuijl O. 2005. "Job analysis: Current and future perspectives." In A Evers, N Anderson, and O Smit-Voskuijl (eds.), *The Blackwell handbook of personnel selection* (pp. 27-46). MA Malden: Blackwell Publishing.

Spearman, CE. 1904. "General intelligence, objectively determined and measured." *American Journal of Psychology*, 15:201–293.

Spencer, LM and SM Spencer. 1993. *Competence at work: Models for superior performance*. New York: John Wiley & Sons.

Sternberg, RJ. 1996. *Successful intelligence*. New York: Simon & Schuster.

Tobey, DH. 2010. *Prosodic forecasts: Emotive language shifts as a predictor of shifts in investor sentiments*. Las Cruces: New Mexico State University.

Tobey, DH & PG Benson. 2009. "Aligning performance: The end of personnel and the beginning of guided skilled performance." *Management Revue*, 20:70–89.

Tobey, DH & MR Manning. 2009. "Melting the glacier: Activating neural mechanisms to create sustainable large-scale organizational change." *Research in Organizational Change and Development*, 17:175–209.

Tobey DH. 2001. *COTS-Based Systems: Automating Best Practices*. Paper presented at the "USC Center for Software Engineering Annual Research Review," Los Angeles, CA.

Tobey DH. 2007. *Narrative's Arrow: Story sequences and organizational trajectories in founding stories*. Paper presented at the "Standing Conference on Management and Organizational Inquiry," Las Vegas, NV.

Tobey, DH. 2008. *Storying crisis: What neuroscience can teach us about group decision making*. Paper presented at the "Southwest Academy of Management," San Antonio, TX.

Tobey, DH (forthcoming). *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, R Reiter-Palmon, and A Callens. (forthcoming). *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, I Wanasika, and CI Chavez. 2007. *PRISMA: A goal-setting, alignment and performance evaluation exercise*. Paper presented at the Organizational Behavior Teachers Conference, Pepperdine, CA.

Trafimow D and S Rice. 2008. "Potential Performance Theory (PPT): A general theory of task performance applied to morality." *Psychological Review*, 115(2):447-462.

Trafimow D and S Rice. 2009. "Potential performance theory (PPT): Describing a methodology for analyzing task performance." *Behavior Research Methods*, 41(2):359-371.

White RW. 1959. "Motivation reconsidered: The concept of competence." *Psychological Review*, 66:297–333.

Wicker FW, FB Lambert, FC Richardson, and J Kahler. 1984. "Categorical goal hierarchies and classification of human motives." *Journal of Personality*, 52(3):285-305.

Williamson DM, M Bauer, LS Steinberg, RJ Mislevy, JT Behrens, and SF DeMark. 2004. "Design rationale for a complex performance assessment." *International Journal of Testing*, 4(4):303-332.

Yerkes RM and JD Dodson. 1908. "The relation of strength of stimulus to rapidity of habit-formation." *Journal of Comparative Neurology and Psychology*, 18(5):459–482.

Appendix A – Panel Roster

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

Appendix B – Job Analysis Questionnaire
Demographic Questions

1. [R0-001] How many employees work at your facility?
   Please choose only one of the following:

   ○ Less than 10
   ○ 10-99
   ○ 100-999
   ○ 1,000-4,999
   ○ 5,000-9,999
   ○ 10,000 or more

2. [R0-002] What job title best describes you?
   Please choose all that apply:

   ☐ Control systems engineer
   ☐ Control systems operator
   ☐ Control systems manager
   ☐ Training specialist
   ☐ IT Executive
   ☐ IT manager
   ☐ IT professional
   ☐ IT systems administrator
   ☐ Network engineer
   ☐ Intrusion analysis staff
   ☐ Intrusion analysis manager
   ☐ Incident handling staff
   ☐ Incident handling manager
   ☐ Cyber security analyst
   ☐ Cyber security operations staff
   ☐ Cyber security operations manager
   ☐ Cyber security manager
   ☐ Cyber security executive
   ☐ Other:

3. [R0-003] How long have you held this position? (Years):
   Please write your answer here:

4. [R0-004] How many people report directly to you?
   Please choose all that apply:

   ☐ No direct reports
   ☐ 1-5
   ☐ 6-30
   ☐ More than 30

5. [R0-005] What job title best describes the position you had prior to your current job?
   Please choose all that apply:

   ☐ Control systems engineer
   ☐ Control systems operator
   ☐ Control systems manager
   ☐ Training specialist
   ☐ IT executive
   ☐ IT manager
   ☐ IT professional
   ☐ IT systems administrator
   ☐ Network engineer
   ☐ Intrusion analysis staff
   ☐ Intrusion analysis manager
   ☐ Incident handling staff
   ☐ Incident handling manager
   ☐ Cyber security analyst
   ☐ Cyber security operations staff
   ☐ Cyber security operations manager
   ☐ Cyber security manager
   ☐ Cyber security executive
   ☐ Other:

6. [R0-006] How would you classify your level of expertise in the cybersecurity field?
   Please choose only one of the following:

   ○ Novice: minimal knowledge, no connection to practice
   ○ Beginner, working knowledge of key aspects of practice
   ○ Competent: good working and background knowledge of the area
   ○ Proficient: depth of understanding of discipline and area of practice
   ○ Expert: authoritative knowledge of discipline and deep tacit understanding across area of practice

7. [R0-007] What level of familiarity do you have with smart grid operations?
   Please choose only one of the following:

   ○ Novice: minimal knowledge, no connection to practice
   ○ Beginner, working knowledge of key aspects of practice
   ○ Competent: good working and background knowledge of the area
   ○ Proficient: depth of understanding of discipline and area of practice
   ○ Expert: authoritative knowledge of discipline and deep tacit understanding across area of practice

8. [R0-008] What level of familiarity do you have with smart grid cybersecurity?
   Please choose only one of the following:

   ○ Novice: minimal knowledge, no connection to practice
   ○ Beginner, working knowledge of key aspects of practice
   ○ Competent: good working and background knowledge of the area
   ○ Proficient: depth of understanding of discipline and area of practice
   ○ Expert: authoritative knowledge of discipline and deep tacit understanding across area of practice

9. [R0-009] What is your gender?
   Please choose only one of the following:

   ○ Female
   ○ Male

10. [R0-010] What is your age?
    Please choose only one of the following:

    ○ Under 20
    ○ 21-30
    ○ 31-40
    ○ 41-50
    ○ 51-60
    ○ Over 60

Appendix C – Revised Job Analysis Questionnaire Task List Based on Pilot Test

The JAQ is the primary data collection method for developing a theoretical model of job performance in three smart grid cybersecurity roles: Security Operations, Incident Response, and Intrusion Analysis. The task statements below were contained in the JAQ that was evaluated by nominated SMEs to determine those tasks that are most critical to perform and those tasks which best differentiate between the performance of individuals possessing basic, intermediate, and advanced skills.

Task	Task Statement
9638	Collect all data necessary to support incident analysis and response.
9818	Map activities observed in the network to systems to help establish the baseline.
9186	Review event correlation (for example look at baseline data to determine the type and frequency of events during normal operations).
9640	Analyze the intrusion by looking for the initial activity and all follow-on actions of the attacker.
9637	Assign an incident response manager for all incidents.
9641	Collect images of affected system for further analysis before returning the system to an acceptable operational state.
9639	Communicate incident information and updates to affected users, administrators, and security staff and request additional information that may support analysis and response actions.
9642	Establish or update a repository for all incident-related information and index and catalog this information with assigned incident numbers for easy retrieval.
9643	Test incident storage repository to make sure it is functioning properly and can only be accessed by authorized personnel.
9644	Verify incident or case files are complete and managed properly by the assigned incident manager.
9137	Analyze individual threat activity by correlating with other sources to identify trends.
9819	Analyze the security incident and identify defining attriubutes [sic].
9709	Protect classified or proprietary information related to the event, but release general incident information to stakeholders.
9825	Report security incident classification (category selected) to management and record in incident management system.
9770	Communicate incident response plan and team member roles to stakeholders and team members to ensure that they understand commitment and responsibilities when team is stood up.
9364	Communicate with other analysts to work as a team on larger incidents.
9579	Coordinate notification strategies with other units, such as Compliance.
9180	Coordinate reactive and proactive responses.
9613	Coordinate with compliance to make all regulator required security incident reports in compliance with the standards.
9772	Develop an incident response program / plan.
9768	Develop a detailed incident response action plan and team roles.
9697	Document call trees and reporting and coordinating procedures to all parties.
9779	Document stakeholders that must be contacted for each affected system in an incident.
9109	Identify known information to include event details and an accurate sequence of events.
9876	Maintain a single sequence of events with change control throughout the incident investigation.
9771	Identify people resources by skills, expertise, and roles to support analytical efforts.

Task	Task Statement
9780	Maintain knowledge of professional resources within the organization.
9777	Maintain professional credentials and networking relationships with professional organizations.
9122	Prioritize alerts into predefined categories.
9778	Recognize dissenting opinions among analysts.
9769	Establish a team of internal intrusion detection experts for second-tier incident response.
9775	Test the incident response program / plan.
9774	Train staff on the incident response program / plan.
9776	Update the incident response program/plan based on testing results.
9706	Identify the source of infections or successful attacks.
9701	Monitor all systems that were suspected or confirmed as being compromised during an intrusion/incident.
9704	Report incident response status to management, including confidence levels for eradication actions.
9703	Review running processes to determine if incident response successfully removed malware.
9707	Train users in phishing identification and malware distribution methods.
9686	Analyze incident response team actions and performance of team members against the incident response plan.
9684	Develop a response plan for the incident and assign actions and deadlines.
9688	Identify impacts occurring from response actions and consider timeliness of response efforts.
9685	Monitor incident response performance and actions and compare them to the incident response plan.
9687	Understand necessary deviations or unanticipated actions from the incident response plan.
9830	Analyze reoccurring activity that is not flagged as a security event and troubleshoot likely cause.
9832	Coordinate watch rotation turnover so that no active event analysis is dropped between team changes.
9829	Review event logs and alerts to ensure as much as possible that they have been processed and categorized.
9361	Review log files for signs of intrusions and security events.
9259	Assess whether network scan results are real or false positives.
9206	Communicate with external agencies such as law enforcement, ICS-CERT, and DOE regarding incident reports.
9849	Report the time of discovery for all reportable events and incidents and the time of notification.
9621	Develop escalation process and procedures for network activity that has not been shown to be authorized.
9430	Verify all devices are being submitted to Security Information and Event Management for full network visibility.
9696	Collect necessary information for inclusion in the communications plan.
9694	Communicate with business management to identify additional parties that should be included in communication and response plans.
9700	Review the communication plan and make changes as appropriate.
9695	Understand changes to organizations and the business to identify stakeholders to be included in the communications plan.
9699	Verify communication plan and contact information with all parties at an appropriate frequency.
9169	Test the SIEM (Security Information and Event Management) implementation with a alert triggers based on how the monitor has been configured.
9591	Test incident response system and planning remains effective against the latest attacker methodologies and tools.
9412	Test IR (Information Response) specialists to verify they maintain a current understanding of threats and how to analyze.
9676	Test remediated systems and the effectiveness of containment measures.

Task	Task Statement
9592	Test to verify that there is a correct flow of intrusion events to incident cases and that there is a coordinated response between Incident Response Specialist, Intrusion Analyst, and System Operations Specialist stakeholders.
9873	Analyze actions indicating malicious events may be spreading or providing opportunities for an attacker to move.
9874	Analyze actions indicating malicious events that provide opportunities for an attacker to close down command and control channels.
9875	Analyze actions indicating malicious events to determine strategy for blocking outside IPs to contain an incident.
9666	Analyze logs and system information to determine which systems have been affected by an attacker and what actions were taken by the attacker.
9677	Analyze the incident's technical and business impacts.
9670	Assign response team members to collect data for analysis from systems within the containment boundary.
9668	Communicate the boundary around affected systems being contained.
9187	Coordinate with the Help Desk to identify user complaints that may be related to the investigated event.
9680	Coordinate with outside parties to determine if containment efforts are successful (for example, call FBI and confirm the Command and Control channel has been closed).
9673	Coordinate containment with system owners and determine impact of proposed actions after identifying affected system.
9675	Assess if the incident needs to be re-rated and re-evaluate the response plan based on containment efforts.
9667	Define the boundary around suspect systems to minimize the spread and impact of an identified security incident.
9674	Document all actions taken to contain systems.
9683	Document all external communications.
9877	Minimize spread of the incident by ensuring contaminated systems are monitored.
9878	Minimize spread of the incident by ensuring contaminated systems cannot communicate to systems outside of the network boundary.
9671	Establish boundaries or shut down infected systems.
9679	Identify appropriate parties to participate in the incident response including legal, communications, and others.
9682	Maintain asset management information during containment process.
9681	Monitor performance of incident response staff.
9678	Report business and technical impacts of the incident and response activities.
9672	Report to security management and system owners when systems have been successfully contained.
9856	Conduct security drills that incorporate the latest threats and vulnerabilities in the scenarios.
9128	Alert operators to events occurring so that they may increase system logging or retain logs where normally such logs may be simply lost due to system storage constraints.
9401	Analyze test results to ensure systems are functioning nominally.
9397	Develop a schedule for testing elements of the incident response plan and organizations involved in the process.
9407	Develop incident report template to be used when reporting the final status of an incident response.
9214	Develop incident response scenarios.
9622	Develop schedule, test plans, evaluation criteria, and sign-off for evaluating test success and/or failure.
9398	Document all incident response exercises and tests.

Task	Task Statement
9409	Document gaps and outcomes to multiple parties to improve process and procedures.
9400	Document shortcomings and lessons learned from Incident Response exercises and formulate action plans to ensure they're corrected as rapidly as possible.
9126	Escalate analysis findings in accordance with defined plan.
9405	Maintain a set of packaged scenarios with injects and data to exercise the response process.
9139	Maintain documented procedures for analyzing logs and handling log archive.
9343	Maintain technical competence using industry tools for attacks (i.e., backtrack).
9408	Report to internal and external incident stakeholders involved during and after incident response.
9403	Report status to management at defined stages of response per procedure.
9116	Understand incident response process and initiate incident handling according to documented policies and procedures.
9191	Understand incident response, notification, and log handling requirements of business.
9239	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.
9106	Analyze logs by correlating all suspect systems.
9354	Analyze compromised system's configuration by determining if the Intrusion Detection System alert is real.
9134	Report what was analyzed and the list of flagged events, key findings, issues, actions taken.
9351	Review logs, network captures, and traces.
9240	Update security tools (Security Event and Information Management, Intrusion Detection/Prevention System, Firewalls) with information pertinent to network tools or attacks.
9565	Configure alerts to monitor for old signatures and failed updates.
9248	Collect data from proxies and e-mail systems to profile events involving malicous [sic] links or attachments and try to correlate to business process and assets.
9204	Decide on a subjective and/or objective measure to determine the likelihood that an event is an incident. (i.e., a confidence factor).
9284	Develop correlation methods to associate identified vulnerabilities with events identified by security monitoring solutions (Intrusion Detection System, Security Event and Information Management, etc).
9135	Develop procedures for addressing anomalous events in the logs that cannot be immediately identified as known threats, etc.
9121	Prioritize suspect log entries and preserve on master sequence of events list.
9124	Identify systems not logging or components that are blind spots.
9184	Collect a sequence of events and continue to add information based in the investigation process.
9607	Verify that alert thresholds and incident response procedures result in capturing enough data to support incident analysis and response efforts.
9658	Assign the incident to a category or type if possible.
9659	Assess an incident rating calculated on the potential severity and impact of the incident.
9657	Assess if an event meets the criteria to be investigated and opened as an incident.
9655	Assess if the event is applicable to your organization.
9660	Document closure of all incidents.
9656	Document that no action will be taken for events that have been logged but do not meet incident response criteria.
9662	Document the activity being evaluated as an event.
9665	Report all events being investigated to security management.
9663	Review incident criteria.
9654	Verify that the event has occurred.

Task	Task Statement
9664	Verify that the event meets the criteria for further investigation.
9356	Assess whether all necessary expertise is available to address the problem (in one physical or virtual room).
9189	Develop an incident tracking mechanism to classify and track all security incidents.
9190	Open an event ticket to track the potential incident.
9113	Open event tickets and notify interested parties when a probable event occurs and track the event as it unfolds.
9136	Identify and properly respond to situations in which log management applications may be attacked or compromised.
9588	Test the incident response procedure/plan to ensure correct workflow and functionality.
9192	Understand the basic components of an incident response process (Prepare, Identify, Contain, Eradicate, Recover, Lessons Learned).
9203	Establish clear metrics that distinguish types of incidents. Users can then correctly categorize incidents.
9589	Document updates to incident response procedure/plan.
9808	Communicate warning signs of security events to internal stakeholders.
9802	Define security events and incidents with evaluation criteria.
9803	Develop procedures to escalate an event to an incident.
9785	Maintain a current list of stakeholders' contact information and link this information to notification requirements.
9806	Test security staff with drills to determine if events and incidents are being properly characterized.
9708	Develop and publicize ways to distinguish between routine system errors and malicious activities.
9826	Document logic behind why an event was determined to be false.
9831	Escalate findings to appropriate personnel to review event and ensure accuracy of false-positive findings.
9117	Identify and filter out false positives; if determined to be an incident, assign to incident handler.
9719	Monitor all logs associated with third party accessing your systems; this may require a manual review against historic use profiles.
9327	Implement penetration testing and vulnerability assessments to improve incident identification.
9318	Understand environment (culture, staff) to create a better relationship for transmitting delicate and sometimes poorly understood information.
9814	Escalate vendor breach of contract to management and legal team.
9786	Develop role-based access control matrix.
9783	Maintain knowledge of reporting requirements associated with systems.
9200	Identify repeat incidents involving the same person or persons, systems, or adversaries.
9604	Maintain incident data repository and analyze data and metrics regarding types of incidents, frequency, and systems impacted.
9605	Review incidents over time to determine lessons learned or how to better align security tools.
9857	Develop a standardized process to ensure appropriate steps are taken during and after an event occurs.
9711	Monitor systems that were affected and the entire sub-network for activity associated with the attack.
9712	Report closing of the incident and all incident response processes that were followed.
9710	Review incident response actions to ensure actions were taken properly.
9791	Monitor for unauthorized access to tools and data.
9610	Report the attack Tactics, Techniques, and Procedures (used in the last 6months against the organization).
9181	Develop working theories of the attack and look for correlated evidence to support or reject the working theories.

Task	Task Statement
9202	Document the incident response activities to determine positive and negative results from actions and security controls. These should be the starting point for Lessons Learned discussions and follow-on preparation activities.
9129	Review known intrusion Tactics, Techniques, and Procedures and observables to assist in profiling log events and capture event information that may relate to known signatures.
9304	Understand how phishing attacks can adversely impact web-based management applications.
9119	Verify log analysis findings through alternate means such as local log storage or affected system state/configuration.
9634	Define how systems were initially compromised and how the attack progressed and what observables were available for detection and response.
9633	Develop mitigations based on incidents analyzed and recommend improvements in security capabilities or tools as appropriate.
9632	Identify security incidents that require training or awareness for users and security staff.
9635	Implement lessons learned from the analysis of material incidents.
9636	Test the security staff and deployed solutions against scenarios developed from incidents with significant lessons learned.
9114	Maintain chain of custody and integrity of log files if they are to be used by law enforcement at a later date.
9197	Develop a chain-of-custody process and consider forensic images if needed as the investigation progresses.
9232	Identify third-party vendors who specialize in remediation of security penetrations and forensics.
9112	Maintain access control permissions to log files.
9797	Collect proper approvals before individuals are granted access to tools and data.
9796	Define authorized staff for specific security tools and data sources.
9800	Develop roles and responsibilities that can be implemented through Roles Based Access Controls and authorization group memberships.
9789	Establish process to provide authorization for tool use and credentials to access tools.
9790	Maintain centralized Roles Based Access Controls lists for all security tools.
9299	Access a current smart grid inventory and asset list.
9822	Collect change management information to automatically update baseline.
9526	Collect existing device configurations.
9110	Develop base scenario and publish results to show what the log files would/should look like without attack or compromise.
9702	Test all security controls or changes that were implemented during a response.
9827	Verify that security monitoring systems and management systems are working and providing expected coverage.
9178	Analyze security device and application configurations for technical impacts (e.g., network congestion).
9151	Configure system in compliance with the baseline configuration manual.
9152	Coordinate with network operations and system adminstrators [sic] to plan for the implementation and scheduling of required outages or notifications during the deployment.
9159	Coordinate with other departments to properly prepare for additional resources required by the security monitoring solution (i.e., network, database, access management, etc).
9550	Coordinate with project managers to understand current and future projects that will install systems.
9166	Coordinate with system administrators to reboot hosts or restart necessary processes after the software or device has been installed to ensure the monitoring solution is online and functioning.
9620	Develop an approval workflow for accountability, traceability, and reporting.

Task	Task Statement
9434	Develop configuration manuals on all custom solutions.
9551	Document certification and accreditation (baseline configuration, vulnerability assessment, authorization to operation).
9175	Document deployment information in company asset management systems.
9332	Identify deployment risks including technological, geographic, and privacy related.
9543	Review checklist for implementing a device or system for necessary approvals.
9552	Review deployment plans and as planned configurations.
9545	Schedule implementation with affected business owners and IT support staff.
9546	Test implementation with planned configurations to determine any deployment issues.
9176	Test the installation against the functional and performance requirements.
9541	Verify health status of host security tools.
9441	Verify that operating systems, services, and applications are hardened in compliance with regulatory guidance.
9549	Verify that operator and implementer procedures require acknowledgment of authorization prior to implementing.
9630	Update all asset management systems with deployed mitigations, configuration changes, or patches and versions.
9296	Assess if solutions that cannot handle abnormal network traffic should be retired.
9612	Review closed tickets for false positives for unacceptable results.
9844	Review network topologies, composition, and activity to determine security tool needs.
9645	Test security operations staff in the planning and execution of security operations and tools.
9845	Test tools against existing operational environments to determine ability to handle stress and loads, and operate as advertised.
9795	Test that security tool systems and data cannot be accessed by unauthorized internal or external entities.
9341	Maintain a security configuration/coverage map of tools used across the enterprise.
9173	Analyze monitoring solution to determine if newer technology better accomplishes the mission.
9278	Analyze which systems are being scanned and which systems are being missed.
9433	Assign significance to custom Security Event and Information Management rules for unknown event types.
9352	Configure alert rules for Security Event and Information Management solution to automate alerts.
9255	Configure assets IP address and pertinent metadata.
9105	Configure rules for Security Event and Information Management tools to capture and flag events known to be intrusion indicators.
9131	Configure Security Event and Information Management rules and alerts for unsupported devices such as those used in the smart grid and Advanced Metering Infrastructure.
9156	Configure system technical policies that set thresholds and parameters for monitoring.
9432	Develop custom Security Event and Information Management parsers for unknown event types.
9345	Establish a test lab where tools can be practiced and learned.
9593	Maintain an asset inventory of both hardware and software. Link this inventory to other security tools.
9431	Review healthy log collection metrics to understand baseline from which to measure normal performance.
9429	Review Service Level Agreements/Operating Level Agreements to understand expected thresholds.
9348	Understand how to run wireshark [sic] and tcpdump.
9150	Understand the selected Security Event and Information Management tool.
9293	Understand the effort required to plug the solution into custom or specific software and hardware.
9111	Verify that all systems are logging to a central location.

Task	Task Statement
9103	Analyze available logs and note gaps and time periods.
9420	Analyze system logs for Network Time Protocol synchronization anomaly messages.
9104	Configure your security log management tool to sort and filter data in a manner that is best suited for the event being analyzed.
9428	Implement a Datum Secure/Network Time Protocol capability for environments where a secure connection to a root time stamp authority is required.
9531	Maintain change management records for systems that are operational.
9108	Maintain log file storage and archive older events.
9527	Update database of device configurations upon changes to configurations.
9421	Verify Network Time Protocol server is using Universal Time Code format to avoid time zone issues.
9359	Decide where to install security monitoring solutions such that the overall expense is minimized and the coverage is maximized.
9566	Develop procedure to perform manual updates.
9568	Develop procedure to respond to failed alerts.
9569	Document procedures for configuring monitoring solutions to correctly obtain vendor software and signature updates.
9562	Monitor the monitoring solution to ensure vendor software and signature updates are being downloaded correctly.
9567	Monitor vendor notifications for updates to software and signatures and compare against deployed versions.
9563	Review daily, weekly and monthly reports for systems that are not updating or out of baseline with the rest of the system population.
9325	Review system security architecture and governance for new system extensions.
9558	Review updates and version and confirm with vendor.
9559	Schedule update timelines for existing and new solutions.
9557	Subscribe to vendor publications relevant to the product line at hand.
9560	Test functionality after update to ensure system is operating.
9571	Test to ensure that automatic updates occur securely.
9570	Train staff on the procedures for configuring monitoring solutions to correctly obtain vendor software and signature updates.
9564	Manually update monitoring solution with vendor software and signature updates.
9561	Verify configuration against procedures.
9618	Convert (and parse) unknown asset log formats to compatible log format for given monitoring solution.
9574	Define which devices require logging and what level of detail logs need to be configured for.
9142	Develop a centralized logging system.
9619	Develop a periodic verification process to ensure that the assets are logging in alignment with the intended operational architecture.
9363	Develop and/or procure a data logging and storage architecture that scales and is fast enough to be useful for analysis.
9573	Develop a procedure to categorize systems for monitoring.
9422	Identify holes in Network Time Protocol structure system-wide.
9342	Identify sources of targets to scan.
9572	Implement solution to identify new devices connecting to the network(s).
9145	Maintain a list of components that can direct logs to a central logging system, and components that cannot. Configure a method of collecting forensic data from systems that cannot.

Task	Task Statement
9263	Test all vulnerability scanners for modes or configurations that would be disruptive to the communication paths and networks being tested and host communication processing looking for possible con(f)licts that may result in negative operational impacts.
9418	Test server to make sure Network Time Protocol service is operating.
9581	Coordinate with administrators from other departments (i.e., networking, operating systems, servers) to identify strengths and weaknesses in the organization's logging implementations.
9157	Develop reporting logic and work with security operations staff to configure how often, what information, and what priorities are sent from monitoring tool alerts.
9580	Develop standard communication procedure to use when writing rules.
9587	Establish baselines for setting incident alert levels in Security Event and Information Management systems and periodically review and adjust the levels to ensure optimal monitoring.
9582	Test system for performing according to desired functionality and configured policies.
9583	Verify that configuration alert types and alerts are working.
9585	Coordinate periodic testing of alerting mechanisms to ensure the methodology is functioning as expected.
9280	Develop baseline scanning as a part of Configuration Management policies and procedures.
9161	Develop custom internal network monitoring tools (non-vendor solution) to detect anomalies that vendor tools would not be able to identify.
9288	Develop custom scan rules to provide deeper scans or avoid problematic checks.
9163	Develop management interface view to maintain situational awareness of the monitoring tools' or agents' health and operating conditions.
9258	Identify metrics by which tools will be measured against to ensure they are still meeting requirements and goals.
9149	Implement intrusion prevention/detection solution.
9289	Implement secondary scanner should the initial scanner experience usage issues.
9143	Implement web content filtering.
9606	Review past incidents to determine if host security solutions and logs are providing data that can identify an event.
9270	Develop a scanning plan and make sure all network operations staff and key stakeholders are consulted and notified about the timing of test initiation.
9295	Communicate timing and schedule of scans.
9807	Develop Security Event and Information Management rule sets to detect documented event classes for each monitored system.
9538	Communicate changes to user security tools and information regarding identified events and incidents.
9828	Change existing system logic to prevent the same false positive from occurring.
9611	Review tool configurations and target configurations to reduce false positives based on historic information.
9725	Access company policies to verify that the software being downloaded is allowed.
9734	Establish a sandbox in which experimental software may be installed and analyzed for malevolent behavior.
9736	Implement technology that will create inventories/database of the software installed for offline analysis.
9729	Scan systems in an attempt to detect the use of unacceptable software.
9723	Search existing list of acceptable software prior to installing.
9722	Understand company policies and procedures for downloading and installing third-party software.
9715	Search asset management system to collect a list of all system vendors for prioritized technology.
9720	Decide what mitigations should be implemented on remote connections.

Task	Task Statement
9268	Coordinate assessment of any target systems with System Owners ahead of time.
9273	Develop a deconfliction profile for company planned and executed scans with log analysis.
9597	Maintain or be able to access a list of assigned system owners.
9254	Configure vulnerability scanners to operate safely and effectively in the targeted environment.
9858	Review best practices and standards documentation to determine appropriate configuration settings.
9860	Test the vulnerability assessment solution in a development environment to see if desired results are achieved.
9859	Understand desired outcome as well as purpose of assessment so that the solution can be configured appropriately.
9748	Configure security tools to automatically apply patches and apply updates.
9754	Configure signatures for host and network based IPS to ensure optimal configuration and reduce likelihood of business disruption.
9746	Create policy/procedures for how to patch tools.
9744	Define criticality levels for all tool types and identify security tools as among the most critical security tools that need to be patched and updated properly.
9750	Define reports on the current patch and update status of all security tools and identify any variances against vendor releases.
9755	Document current patch levels and updates before use in critical situations.
9751	Establish a systems and tools patching program and schedule.
9739	Identify current patch level of security tools.
9740	Identify primary support resources for each of the production tools to ensure team members understand their responsibilities.
9757	Implement replica production (i.e., LAB) environment for testing of patches prior to production release.
9749	Maintain a list of approved security tools and their approved patch levels.
9649	Monitor security tool providers for updates and patches for tools that are in use.
9738	Monitor security tool vendors for updates and patches.
9745	Monitor vendor feeds for published patches.
9213	Review latest penetration test tools.
9752	Review signatures (for the tools that use them) to determine applicability once implemented.
9756	Schedule periodic reviews to determine when patches and updates are required.
9781	Sign up for vendor notifications and alerts.
9782	Test toolset upgrades against old version to ensure new patches don’t adversely affect results or impair performance.
9742	Understand the process by which security tools are updated before use.
9747	Verify versions of security tools against vendors latest release version or review exception for not updating the software.
9690	Assess what configuration settings result in capturing the required information for monitoring.
9689	Identify logging and monitoring capability of deployed devices.
9426	Implement a reference time source to remove external dependencies for Network Time Protocol.
9861	Implement monitoring system that meets design criteria.
9691	Implement necessary communications and repository to receive data.
9834	Implement procedural and technical controls to ensure logs are maintained for expected period of time per policy.
9523	Prioritize critical systems for monitoring.
9693	Test the data repository to ensure it remains online and is available to receive data.

Task	Task Statement
9692	Verify that the system is reporting the expected information based on the configurations.
9599	Coordinate with system owners to modify schedule based on work or operational changes that affect security scanning.
9260	Define scope of systems and system exclusions for vulnerability testing.
9598	Review scanning schedule results for anomalies.
9609	Coordinate with smart grid suppliers to confirm settings and scans for their equipment.
9279	Coordinate with vendors running scanners on their equipment to develop your scanning program.
9144	Understand the resources and processes used by the security monitoring tool; and identify constraints, impacts to host or network systems, and required configurations to develop an implementation plan.
9601	Verify with the vendor the system processes or states that are authorized for smart grid components.
9765	Configure the security monitoring solution so that it provides a list of hosts that are being monitored and cross-reference that with the asset inventory in place.
9763	Coordinate an assessment of the current monitoring solutions coverage with a third party.
9760	Coordinate an assessment to test the effectiveness and coverage of security monitoring tools.
9140	Coordinate with administrators from other departments (i.e., networking, operating systems, servers) to identify strengths and weaknesses in the organization's logging implementations.
9160	Identify metrics that will be used to show performance of monitoring solution.
9766	Implement a process and technology to re-test effectiveness after each system update.
9837	Configure log management systems and other log repositories to maintain logs for documented period of time per policy.
9833	Document in policy the appropriate length of time to store documents.
9835	Review security operating procedures and policy for data storage requirements.
9839	Schedule log management system and other log repositories to purge data that is older than the documented retention period.
9228	Test in a sandbox new and potentially malicious tools appropriately.
9838	Test storage periods by calling up events and incidents logged by the security operations team.
9836	Verify event/incident categorization to make sure associated data is being stored for the appropriate period.
9146	Implement application (layer 7) firewalls.
9798	Implement Data Leakage Prevention system for security tool systems and data.
9302	Implement penetration tests on deployed components.
9439	Implement the multiple (layered) solution control options for mitigation.
9256	Implement vulnerability scan.
9437	Document any changes made to the operating system or other components to trace possible causes of a system malfunction.
9792	Document system configuration and access control.
9794	Implement controls to prevent unauthorized access tools and data.
9321	Develop an asset inventory of both hardware and software. Link this inventory to other security tools.
9315	Develop technical libraries for all protocols in use and note security issues.
9172	Establish Operational Level Agreements and/or Service Level Agreements where appropriate.
9148	Identify business, contractual, Service Level Agreements and legal requirements that can be met by monitoring solution.
9344	Understand how specific tools (e.g., nmap, nessus, metasploit [sic]) accomplish their results (i.e., what methods and protocols are used).
9320	Understand the ANSI C12 Standards (i.e., C12.18, C12.19, C12.21, C12.22).

Task	Task Statement
9292	Update network deployments to segregate systems that cannot handle vulnerability scans.
9335	Identify the inter-dependencies between the data network and the power system, including fault isolation and protection.
9155	Identify stakeholders who would be users of monitoring solution and their unique requirements.
9648	Document procedures for the successful and proper use of all security tools with a special attention to constraints.
9650	Review security operations procedures for tool use and current versions.
9847	Maintain a list of all required reporting requirements to include what is reported, how it is to be reported, and when it is to be reported (e.g., within 24 hours).
9850	Verify that all reported events and incidents were handled in compliance with the reporting requirements.
9339	Communicate risks to internal stakeholders.
9313	Document risk and impact analysis, including business impact, of smart grid components for management.
9338	Understand NERC CIP and audit requirements.
9525	Implement policy enforcement tool.
9530	Report exceptions to company configuration management policy and standards.
9805	Review a sampling of events to determine if they were properly characterized.
9731	Monitor software installed on end-points for compliance with the company policy.
9726	Monitor software used in the infrastructure and correlate it to a list of acceptable software.
9716	Verify that contracts require vendors to provide proper notice of a security breech or incident that may affect the security of your organization's systems.
9493	Report risk in accordance with defined risk categorization model.
9310	Inventory the component supply chain pipeline process and document it for suppliers.
9813	Review contracts to ensure vendors will notify you if they are breached, their system or solutions are compromised, and/or they have a significant security issue that could directly affect you.
9812	Establish metrics for vendors to assess compliance with notification requirements in the contract.
9767	Communicate results of independent security review to system stakeholders.
9762	Report findings of the independent review to management.
9764	Schedule an independent [sic] review and verification after the security monitoring solution has been implemented.
9209	Communicate with external stakeholders (Law Enforcement Organizations, Public Relations, Legal, IT, Marketing) when necessary to understand regulatory requirement and breach notifications.
9793	Coordinate with internal audits to audit security tool use.
9788	Review access rights to tools and data on a defined frequency to ensure access is appropriate.
9799	Verify access control privileges are working as designed.
9787	Verify tool access and logs for authorized use.
9842	Test security staff on access procedures, company policies, and technical standards for accessing systems.
9714	Verify that staff have read and understand how to access policies and standards for refresher.
9578	Develop policy to determine which critical systems are to be monitored and at what level.
9576	Develop policy to ensure critical systems are monitored.
9577	Understand data classification levels and how to identify such levels with assets.
9575	Understand the data classification strategies that are in place.
9728	Communicate company policy for downloading and installing third-party software.

Task	Task Statement
9721	Develop a policy that requires system administrators to follow company procedures for downloading and installing third-party software.
9732	Establish a basis or requirement for third-party software before use (e.g., what business purpose does it satisfy, why is it needed, etc.).
9848	Develop a process by which staff must acknowledge they have read and understand all applicable policies and procedures.
9713	Review policies and standards that apply to work area.
9522	Analyze cost of monitoring solution vs. features of each solution to ensure maximum Return on Investment.
9226	Establish a budget to handle the scope of an incident that might have the worst possible impact on your infrastructure and ensure that it is available in case an incident occurs.
9141	Analyze market options for Security Event and Information Management tools.
9761	Develop relationships with vendor partners who specialize in this testing.
9758	Define scope of an independent review and budget necessary resources.
9647	Collect information about the security tools employed by the organization.
9646	Review security operations staff performance in the execution of their duties.
9817	Scan systems to establish baseline.
9410	Identify training materials and information sources regarding cyber attacks and techniques.
9220	Identify training opportunities that teach methodologies associated with current attack tools.
9810	Analyze attacker Tactics, Techniques, and Procedures and deconstruct in order to evaluate the effectiveness of protective measures.
9809	Collect observed attacker Tactics, Techniques, and Procedures from available sources to include Information Sharing and Awareness Councils, peer utilities, government sources.
9306	Collect the most recent (or predicted future) threats into a comprehensive list to disseminate to all employees.
9305	Collect vendor knowledge bases and DOE / DHS generated testing reports of known vulnerabilities to specific smart grid components. Supplement that information with open source reporting and internal red teaming or tabletop assessments.
9820	Develop a heat map to illustrate current high-level security posture for executive consumption.
9811	Identify observables that flow from particular attacker Tactics, Techniques, and Procedures to optimize your security monitoring capabilities.
9547	Identify external scanning needs that an internal scanner may not be able to adequately assess.
9544	Monitor for new systems installed on the network.
9402	Report summary of test results to management.
9425	Scan for configuration anomalies.
9444	Scan for gaps in system configuration against a benchmark configuration manual.
9555	Scan internal and external networks for new and unauthorized systems.
9624	Assign a technical point of contact for vulnerability remediation and assistance.
9625	Assess the risk ratings of the vulnerability based on the technical information and how the technology is deployed and the importance of the systems.
9626	Consult with vendor or integrators and internal system owners to develop appropriate mitigations.
9623	Document all vulnerability information alerts or disclosures that apply to deployed technology and note the time and responsible party to develop the risk picture and initiate workflow.
9627	Implement vulnerability mitigations in accordance with the plan to include patches or additional security controls.
9628	Scan all affected systems to ensure the patch or mitigations are present and the risk associated with the vulnerability has been reduced as expected.

Task	Task Statement
9629	Test all identified mitigations or patches to make sure they remove or mitigate the vulnerability as expected with no negative impacts.
9326	Analyze vulnerabilities for business impact.
9603	Develop a method to characterize vulnerabilities that includes risk scores.
9294	Develop a process for scoring the risk associated with identified vulnerabilities to support prioritization of mitigation recommendations.
9229	Develop a process to create and prioritize job tickets for analysis and distribution of information to specific recipients.
9314	Alert end users of potential risks and vulnerabilities that they may be able to mitigate.
9399	Coordinate with other departments to ensure that routine business operations are not affected during testing.
9404	Develop a RACI (Responsible, Accountable, Consulted, Informed) matrix to ensure all roles clearly understand their responsibilities in the testing process.
9406	Identify all systems that may be affected by testing.
9331	Identify threat actors.
9244	Report vulnerabilities to staff and stakeholders.
9298	Coordinate efforts with the vendor to develop an understanding of the component and security implications.
9596	Coordinate with external governments on threat intelligence.
9853	Communicate new threats or newly discovered vulnerabilities to the entire security operations staff.
9614	Develop threat awareness content that can be included in security awareness and outreach efforts.
9319	Monitor industry groups and forums to stay up to date on the latest security vulnerabilities related to smart grid components.
9815	Monitor intelligence sources for information that indicates that a vendor you are working with may have been compromised.
9852	Test security to staff to assess understanding of current threats and vulnerabilities.
9854	Train security operations staff when significant changes in threat or vulnerability have occurred.
9416	Alert external government entities with new intelligence.
9252	Develop a threat analysis testing environment and sandbox where Tactics, Techniques, and Procedures can be analyzed and considered.
9333	Develop attack trees of attack vectors against vulnerable systems.
9225	Develop possible attack techniques against specific technologies and implementations in your smart grid deployments.
9413	Identify sources of intelligence to use for threat analysis.
9615	Review threat tables and conduct analysis of existing incident response data.
9267	Develop a prioritized list of critical resources.
9205	Analyze events against industry sharing initiatives to identify anomalies/possible events.
9489	Analyze vendor Knowledge Bases and DOE and DHS generated testing reports of known vulnerabilities to specific smart grid components.
9265	Analyze vulnerability reports.
9491	Monitor vulnerability reports.
9262	Review vulnerability scan results.
9595	Maintain a prioritized list of critical resources.
9307	Collect issues to identify trends with particular vendors or manufacturers.
9556	Communicate with the vendor to ensure you are registered to receive updates.

Task	Task Statement
9201	Prioritize systems within your network to determine which ones are of the High, Moderate, or Low impact value.
9276	Review assessment results in accordance with defined risk categorization model.
9718	Communicate with vendors about a vulnerability or incident in order to understand risk and devise a mitigation strategy.
9717	Monitor security news and intelligence sources to include vendor webpages for vulnerability disclosures, incident announcements, and knowledge briefs.
9230	Communicate with research firms to keep abreast of new changes and methodologies.
9301	Identify methods to detect vulnerabilities in smart grid components with help from industry groups and thought leaders.
9215	Identify sources for information regarding attacks, exploit capability and tools, and newly discovered vulnerabilities.
9346	Review ICS-Cert, NERC, and other source reports of attacks and develop understanding of how the threats actually work against specific vulnerabilities.
9211	Subscribe to appropriate industry security mailing lists.
9219	Subscribe to intelligence services and open source information subscriptions to be aware of events.
9222	Subscribe to various information-sharing portals relevant to the content.
9316	Subscribe to vulnerability feeds and maintain information-sharing subscriptions.
9608	Verify that assessment tool outputs contain all necessary data elements for vulnerability analysis and risk determination.
9492	Prioritize vulnerability scan results.
9600	Analyze vulnerabilities to determine risk based on how you have deployed the technology and the likelihood for exploitation.
9243	Develop contract language that requires your technology vendors and service providers to provide information about vulnerabilities and threats to the technology you purchase.
9816	Map newly discovered vulnerabilities to equipment and vendors to track compliance.
9759	Hire independent third-party auditor to assess/audit toolset coverage and effectiveness.
9602	Maintain a table of attack techniques that align with your deployed technology and business processes.
9253	Implement a honeypot and research the attacks it collects.
9631	Analyze all intrusions to determine lessons learned and identify requires changes to security procedures, technology, or training.
9616	Develop an attack technique table.
9415	Coordinate presentations on latest threats to management and senior management.
9411	Develop schedule to have all Incident Response specialists complete training to refresh and keep knowledge current.
9414	Review all internal incidents for the purposes of staying current in threats and how to to stay up to date on current threats and determine the best way to analyze them, review all internal incidents.
9235	Train information collection, analysis, and dissemination.
9286	Train staff on Train staff on requirements and procedures for using vulnerability scanning.
9217	Develop various security/attack monitoring courses and require all employs to attend training to ensure widespread understanding of baseline requirements.
9590	Train non-security team members (CXO, Legal, etc.) on how to follow incident response procedure/plans.
9183	Understand the company's incident response process and procedures .
9536	Analyze user behavior in stopping security services or use of the tools and services.
9617	Train Incident Response Team on the usage of the attack technique table.

Task	Task Statement
9652	Train new security staff and provide refresher training at required intervals.
9653	Verify all security staff have the necessary training and required certifications or qualifications to operate tools.
9241	Communicate with new staff or external stakeholders.
9727	Review and familiarize new staff with company policies and procedures for downloading and installing third-party software.
9497	Develop training sessions about attack techniques.
9245	Develop training sessions about attack tools.
9496	Train other departments on attack tools.
9498	Train other departments on attack techniques.
9350	Develop training materials for other team members about current attack tools, technologies, and techniques to compromise systems and intrude upon systems and networks.
9237	Review past events and lessons learned within your organization and develop a plan based on those insights.
9651	Develop training for new operators and refresher training for previously trained staff.
9840	Train security staff on accessing policies and standards and topics addressed.

Appendix D – Literature Review Bibliography

Anderson R and S Fuloria. 2010. *"Who Controls the off Switch?"* Paper presented at the *2010 1st IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Gaithersburg, MD.

Bartels G. 2011. "Combating smart grid vulnerabilities." *Journal of Energy Security*.

Baumeister T. 2010. *Literature Review on Smart Grid Cyber Security*, at http://csdl.ics.hawaii.edu/techreports/10-11/10-11.pdf

Boyer WF and SA McBride. 2009. *Study of Security Attributes of Smart Grid Systems-Current Cyber Security Issues.* (U.S. Department of Energy Office of Electricity Delivery and Energy Reliability, Trans.). Idaho Falls, ID: Idaho National Laboratory Critical Infrastructure Protection/Resilience Center.

Cavoukian A, P Jules, and W Christopher. 2009. *SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation*. Toronto, Ontario: Information and Privacy Commissioner, Ontario, Canada.

Cyber Security Coordination Task Group. 2009. *Smart Grid Cyber Security Strategy and Requirements*, (Draft. ed.). Gaithersburg, MD: U.S. Dept. of Commerce, National Institute of Standards and Technology.

Dagle J. 2009. *Summary of Cyber Security Issues in the Electric Power Sector*. Ft. Belvoir: Defense Technical Information Center.

Dan G and H Sandberg. 2010. "Stealth Attacks and Protection Schemes for State Estimators in Power Systems." Paper presented at the *2010 1st IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Gaithersburg, MD.

Davis CM, JE Tate, H Okhravi, C Grier, TJ Overbye, and D Nicol. 2006. "SCADA Cyber Security Testbed Development." Paper presented at the *38th North American Power Symposium (NAPS 2006)*, Sept. 2006, Carbondale, IL.

Depuru SSSR, L Wang, and V Devabhaktuni. 2011. "Smart meters for power grid: Challenges, issues, advantages and status." *Renewable & Sustainable Energy Reviews*, 15(6):2736-2742. doi: 10.1016/j.rser.2011.02.039.

Dong W, L Yan, M Jafari, P Skare, and K Rohde. 2010. "An Integrated Security System of Protecting Smart Grid against Cyber Attacks." Paper presented at the *2010 Innovative Smart Grid Technologies* (ISGT), Gaithersburg, MD.

Fadlullah ZM, MM Fouda, N Kato, S Xuemin, and Y Nozaki. 2011. "An early warning system against malicious activities for smart grid communications." *Network, IEEE*, 25(5):50-55. doi: 10.1109/MNET.2011.6033036

Fouda MM, ZM Fadlullah, N Kato, L Rongxing, and S Xuemin. 2011. "Towards a light-weight message authentication mechanism tailored for Smart Grid communications." Paper presented at the *IEEE Conference on Computer Communications Workshops*, Shanghai, China.

Gustavsson R and B Stahl. 2010. "The empowered user-The critical interface to critical infrastructures." Paper presented at the *2010 5th International Conference on Critical Infrastructure* (CRIS), Beijing, China.

Hamlyn A, H Cheung, T Mander, L Wang, C Yang, and R Cheung. 2008. "Computer Network Security Management and Authentication of Smart Grids Operations." Paper presented at the *2008 IEEE Power and Energy Society General Meeting*, Pittsburgh, PA. http://ieeexplore.ieee.org/ielx5/4584435/4595968/04596900.pdf?tp=&arnumber=4596900&isnumber=4595968

Hiskens IA and M Akke. 1999. "Analysis of the Nordel power grid disturbance of January 1, 1997 using trajectory sensitivities." *IEEE Transactions on Power Systems*, 14(3):987-994.

Holmgren AJ, E Jenelius, and J Westin. 2007. "Evaluating strategies for defending electric power networks against antagonistic attacks." *IEEE Transactions on Power Systems*, 22(1):76-84. doi: 10.1109/TPWRS.2006.889080.

Idaho National Laboratory. 2011. *Vulnerability Analysis of Energy Delivery Control Systems*. Idaho Falls, ID: U.S. Department of Energy.

Inc. K. 2010. "The U.S. smart grid revolution: Smart grid workforce trends 2011." *The GridWise Alliance*, pp. 37

Iyer S. 2011. "Cyber security for smart grid, cryptography, and privacy." *International Journal of Digital Multimedia Broadcasting, 2011*. doi: 10.1155/2011/372020

Kim TT and HV Poor. 2011. "Strategic protection data injection attacks on power grids." *IEEE Transactions on Smart Grid*, 2(2):326-333. doi: 10.1109/TSG.2011.2119336

Kosut O, J Liyan, RJ Thomas, and T Lang. 2010. "On Malicious Data Attacks on Power System State Estimation." Paper presented at the *2010 45th International Universities Power Engineering Conference* (UPEC 2010), Cardiff, Wales.

Ling APA and M Masao. 2011. "Selection of Model in Developing Information Security Criteria on Smart Grid Security System." Paper presented at the *2011 IEEE 9th International Symposium on Parallel and Distributed Processing with Applications Workshops* (ISPAW), Los Alamitos, CA.

Naone E. 2010. "Hacking the Smart Grid." *Technology Review*, August 2.

National SCADA Test Bed. 2009. *Study of security attributes of smart grid systems: Current cyber security issues*. Idaho Falls, ID: INL Critical Infrastructure Protection/Resilience Center.

Office of the Information & Privacy Commissioner of Ontario, Hydro One, GE, IBM, & TELVENT. 2011. *Operationalizing privacy by design the Ontario smart grid case study*. Toronto, Ontario: Information and Privacy Commissioner of Ontario.

Pearson ILG. 2011. "Smart grid cyber security for Europe." *Energy Policy*, 39(9):5211-5218. doi: 10.1016/j.enpol.2011.05.043.

Qian H and RS Blum. 2011. "New hypothesis testing-based methods for fault detection for smart grid systems." Paper presented at the *2011 45th Annual Conference on Information Sciences and Systems* (CISS 2011), Baltimore, MD.

Reddi RM. 2010. *Real time test bed development for power system operation, control and cybersecurity.* Master's thesis, Mississippi State University, Mississippi State, MS Retrieved from http://library.msstate.edu/etd/show.asp?etd=etd-11112010-175544 available from OCLC WorldCat database.

Robles RJ and K Tai-hoon. 2010. "Communication Security for SCADA in Smart Grid Environment." Paper presented at the *9th WSEAS International Conference on Data Networks, Communications, Computers* (DNCOCO 2010), Athens, Greece.

Salmeron J, K Wood, and R Baldick. 2004. "Analysis of electric grid security under terrorist threat." *IEEE Transactions on Power Systems, 19*(2):905-912.

Scarfone K, T Grance, and K Masone. 2008). *Computer security incident handling guide: Recommendations of the National Institute of Standards and Technology*. (800-61 Revision 1). Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology Retrieved from http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf.

Sheldon FT and H Okhravi. 2010. *Data Diodes in Support of Trustworthy Cyber Infrastructure*. Oak Ridge National Laboratory. Oak Ridge, TN.

Simmhan Y, AG Kumbhare, C Baohua, and V Prasanna. 2011. "An Analysis of Security and Privacy Issues in Smart Grid Software Architectures on Clouds." Paper presented at the *2011 IEEE 4th International Conference on Cloud Computing* (CLOUD 2011), Los Alamitos, CA.

Smart Grid Information Clearinghouse. 2011. *Deployment Experience*, from http://www.sgiclearinghouse.org/Deployment.

So HKH, SHM Kwok, EY Lam, and L King-Shan. 2010. "Zero-configuration Identity-based Signcryption Scheme for Smart Grid." Paper presented at the *2010 1st IEEE International Conference on Smart Grid Communications* (SmartGridComm), Gaithersburg, MD.

Sugwon H and L Myongho. 2010. "Challenges and Direction toward Secure Communication in the SCADA System." Paper presented at the *2010 8th Annual Communication Networks and Services Research Conference* (CNSR), 11-14 May 2010, Los Alamitos, CA.

Ten C-W, C-C Liu, and M Govindarasu. 2008. "Cyber-vulnerability of power grid monitoring and control systems." Paper presented at the *Proceedings of the Fourth Annual Workshop on Cyber Security and Information Intelligence Research*, Oak Ridge, TN. http://powercyber.ece.iastate.edu/publications/CSIIR-extended.pdf

The Energy Sector Control Systems Working Group. 2011. *Roadmap to Achieve Energy Delivery Systems Cybersecurity* (p. 80).

The Smart Grid Interoperability Panel – Cyber Security Working Group. 2010. *Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements*. (NISTIR 7628). Gaithersburg, MD: National Institute of Standards and Technology Retrieved from https://www.evernote.com/shard/s66/res/307ff759-2782-4e63-990a-2b438a01574b/nistir-7628_vol1.pdf.

The Smart Grid Interoperability Panel – Cyber Security Working Group. 2010. *Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid*. (NISTIR 7628). Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from https://www.evernote.com/shard/s66/res/307ff759-2782-4e63-990a-2b438a01574b/nistir-7628_vol1.pdf.

The Smart Grid Interoperability Panel – Cyber Security Working Group. 2010. *Guidelines for Smart Grid Cyber Security: Vol. 3, Supportive Analyses and References*. (NISTIR 7628). Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf.

United States Government Accountability Office. 2011. *Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed*. (GAO-11-117). Retrieved from http://www.gao.gov/products/GAO-11-117.

Wang T-K and F-R Chang. 2011. "Network Time Protocol Based Time-Varying Encryption System for Smart Grid Meter." Paper presented at the *2011 Ninth IEEE International Symposium on Parallel and Distributed Processing with Applications Workshops* (ISPAW), 26-28, May 2011, Busan, South Korea.

Wang Y. 2011. "sSCADA: securing SCADA infrastructure communications." *International Journal of Communication Networks and Distributed Systems,* 6(1):59-78. doi: 10.1504/ijcnds.2011.037328.

Wang Y, D Ruan, J Xu, M Wen, and L Deng. 2010. "Computational Intelligence Algorithms Analysis for Smart Grid Cyber Security." In Y Tan, SYH and TKC (eds.), *Advances in Swarm Intelligence, Pt 2, Proceedings*, 6146:77-84.

Zhuo L, L Xiang, W Wenye, and C Wang. 2010. "Review and evaluation of security threats on the communication networks in the smart grid." Paper presented at the *Military Communications Conference* (MILCOM 2010), Oct. 31 2010-Nov. 3 2010, San Jose, CA.

Appendix E – Job Descriptions

Job descriptions are an excellent source of job classification data. Accordingly, this appendix will include sample job descriptions from recruitment advertisements across the industries that are involved in the smart grid. These advertisements were collected from firms in the energy industry, profession services firms, and technology vendors. Further information on the selection of these descriptions may be obtained from Pacific Northwest National Laboratory.

accenture

Security Technology - Smart Grid Consultant

Job Location: CA - San Francisco; GA - Atlanta; IL - Chicago; NJ - Florham Park; NY -New York; TX - Dallas; VA - Reston
Job Number: 00136772

Schedule: Full-time
Organization: **Technology Growth Platform**
Location: **Location Negotiable**
Travel: **100% (Monday - Friday)**

Accenture's Technology Growth Platform (TGP) offers a full range of global delivery services-from enterprise solutions, system integration, technical architectures, business intelligence, infrastructure consulting, and technology research/development.

Accenture's Security Practice helps organizations work through complex business and technology issues to provide innovative and holistic approaches for dynamic cyber defense, enterprise risk management, information assurance and information security. Our security professionals bring deep technology skills and industry knowledge to any organization and work closely with clients to design and implement a security solution closely tied to enterprise objectives.

Smart Grid Security Consultant:

Our professionals deliver innovative security solutions and provide expertise in all aspects of cyber security for our utility client's smart grid security challenges. Our consultants identify and evaluate security gaps and will help to create and implement security strategies and plans to address. They also anticipate security requirements and identify sound security controls for applications, systems, processes, and organizations. Our consultants work on dedicated security projects, and well as with cross disciplinary teams to integrate security controls on projects.

We are currently looking for consultants for our Security Practice with experience in Smart Grid Security technologies.

Key Responsibilities may include one or more of the below:

- Working directly with clients and Accenture teams to design and implement security solutions for smart grid projects, across platforms and vendors
- Developing smart grid security strategy for clients
- Performing risk assessments of smart grid infrastructure and/or applications
- Assisting client teams in implementing security solutions for their existing or new applications/infrastructure, including advanced metering infrastructure (AMI) and meter data management (MDM)
- 100% Travel

Basic Qualifications:

- Minimum 3 years experience in Information Technology
- Minimum 3 years hands-on experience implementing security solutions and/or security assessments (e.g. certification and accreditation, risk assessments)
- Minimum 1 year experience in smart grid security
- Minimum Bachelor's degree

Preferred Skills:

- Familiar with smart grid vendors such as SSN, OPower, Ambient, Trilliant, GE Meters, Oracle MDM, Oracle CC&B, etc.
- Expertise with smart grid security frameworks such as NISTIR 7628, NERC- CIP, or NIST SPs.
- Strongly prefer industry-adopted security certification(s) (e.g. Security+, CISSP, CISA, CISM, CEH)
- Knowledge of computer networking and standard protocols (e.g. TCP/IP)
- Knowledge of wireless technologies (e.g. Cellular, Wi-Fi, Bluetooth, ZigBee)
- Electric power/gas/water utility or energy industry experience

Professional Skill Requirements:

- Eagerness to contribute in a team-oriented environment
- Ability to work creatively and analytically in a problem-solving environment
- Desire to work in an information systems environment
- Excellent communication (written and oral) and interpersonal skills

accenture

Security Technology - Smart Grid Senior Manager

Job Location: CA - San Francisco; GA - Atlanta; IL - Chicago; NJ - Florham Park; NY -New York; TX - Dallas; VA - Reston
Job Number: 00136778

Schedule: Full-time
Organization: Technology Growth Platform
Location: Location Negotiable
Travel: 100% (Monday - Friday)

Accenture's Technology Growth Platform (TGP) offers a full range of global delivery services-from enterprise solutions, system integration, technical architectures, business intelligence, infrastructure consulting, and technology research/development.

Accenture's Security Practice helps organizations work through complex business and technology issues to provide innovative and holistic approaches for dynamic cyber defense, enterprise risk management, information assurance and information security. Our security professionals bring deep technology skills and industry knowledge to any organization and work closely with clients to design and implement a security solution closely tied to enterprise objectives.

Smart Grid Security Senior Managers:
Our Senior Managers assist clients with the identification and evaluation of holistic security gaps with a focus on the infrastructure and business applications layer.
They also anticipate security requirements and identify sound security controls for applications, systems, processes and organizations. Our senior managers can easily work with non-security teams to integrate security controls on projects.

Key Responsibilities may include one or more of the below:

- Working within Utility Industry compliance frameworks, specifically FERC, NERC CIP and recently released NIST Smart Grid security requirements
- Defining Security & Control capabilities of Accenture Smart Grid offerings
- Working with Oracle, EMC, RSA, Cisco, Symantec and Silver Springs Networks as part of a Smart Grid Solution
- Developing and presenting at industry conferences as an expert in the Utilities Security and Smart Grid field
- Play substantive or lead role in establishing Accenture's presence within the Utilities/Smart Grid field

- Business development responsibilities
- Demonstrate ability to create and direct proposal efforts
- Ability to travel 100%

Basic Qualifications:

· Minimum 5 years experience in Information Technology
· Minimum 5 years hands-on experience implementing security solutions and/or security assessments (e.g. certification and accreditation, risk assessments)
· Minimum 1 year experience in smart grid security
· Minimum 3 years consulting sales experience.
· Minimum 2 years experience with developing and communicating proposals for security and privacy services
· Minimum Bachelor's degree

Preferred Skills:

· Familiar with smart grid vendors such as SSN, OPower, Ambient, Trilliant, GE Meters, Oracle MDM, Oracle CC&B, etc.
· Expertise with smart grid security frameworks such as NISTIR 7628, NERC- CIP, or NIST SPs.
· Strongly prefer industry-adopted security certification(s) (e.g. Security+, CISSP, CISA, CISM, CEH)
· Knowledge of computer networking and standard protocols (e.g. TCP/IP)
· Knowledge of wireless technologies (e.g. Cellular, Wi-Fi, Bluetooth, ZigBee)
· Electric power/gas/water utility or energy industry experience

Professional Skill Requirements:

· Eagerness to contribute in a team-oriented environment
· Ability to work creatively and analytically in a problem-solving environment
· Desire to work in an information systems environment
· Excellent communication (written and oral) and interpersonal skills
· Proven track record with client facing presentations and business development activities
· Needs analysis, positioning, business justification and closing skills
· Ability to effectively lead/ manage large teams (often global in location)

Information Security Risk Analyst III 104293

Posted: October 15, 2011

Job Code:	104293
Company Name:	Constellation Energy
Job Level:	Experienced (non-manager)
Position Type:	Full Time
Salary Range:	Not Specified
Location:	Baltimore, MD
Job Type:	Information Technology (IT)

Constellation Energy
The way energy works.

APPLICATION INFORMATION

https://careers.constellation.com/psp/careers/EMPLOYEE/HRMS/c/HRS_HRAM.HRS_CE.GBL?Page=HRS_CE_HM_PRE&Action=A&SiteId=3

View All Job Opportunities for this Employer

Job Description:

Responsibilities
Job Summary:

The Information Security Risk Analyst III (ISRA III) provides cyber and information security expertise in the analysis, assessment, development, and evaluation of security solutions and architectures to secure applications, operating systems, databases, and networks. The ISRA III develops security requirements, conducts security risk assessments, designs security solutions, evaluates application and system architectures, and develops and reviews security policies and standards. The ISRA provides cyber and information security risk consulting to business units, information technology (IT) organizations, and support and operational functions. The ISRA III leads the cyber and information security aspects of business initiatives and IT projects to assist in mitigating security risks for information, business, and operational applications and systems across the company. This role serves as a senior staff member of the Information Risk (IR) team with technical cyber and information security expertise to mitigate cyber security risks to the company, including its stakeholders and customers.

Senior Software Security Analyst Job

Apply now »

Date: Sep 19, 2011
Location: Glen Allen, VA, United States

Job Number:	1438707
Business	GE Corporate
Business Segment:	Corporate Initiatives Group
About Us:	At GE, ensuring the security of our data is, and always will be, a top priority. That's why we hire the best and brightest experts in the information security field. If you are looking for a challenging career on the cutting edge of security and technology, with an opportunity to be a part of a diverse, dynamic and global team, then GE's Information Security Technology Center in Glen Allen, VA is the place for you! Join our GE team today, where you'll find endless learning opportunities to make the most of your talents. Our culture of innovation and imagination, coupled with industry leaders who will inspire you, make GE an exciting place to grow your career. To stay connected with news and hot jobs at GE's Information Security Technology Center, follow us on Twitter: @geinfosec or visit ge.com/infosec.
Posted Position Title:	Senior Software Security Analyst
Career Level:	Experienced
Function	Information Technology
Function Segment:	Information Security
Location:	United States
U.S. State, China or Canada Provinces:	Virginia
City:	Glen Allen
Postal Code:	23060-9297
Relocation Assistance	No
Role Summary/Purpose:	The Senior Software Security Analyst will serve as a technical software security resource responsible for identifying software vulnerabilities and working with development teams to design / implement solutions to ensure and protect the safety and security of all information systems; Assess GE applications and software products across all businesses and provide guidance / direction for the protection of information systems and intellectual property assets.

SCADA Protocol Engineer

Computers/Software | Livermore, CA

Send Jobvite

Environmentally sustainable power systems—meet the challenge. Creativity/imagination required. Provide software development expertise: research, analyze, develop cyber security solutions for critical infrastructure industry with a focus on SCADA/DCS and the emerging Smart Grid. Help industry meet the challenges of developing environmentally sustainable power systems that integrate intermittent wind/solar generation, plug-in electric vehicles, energy storage, and innovative market designs that provide a high degree of consumer choice. Advanced planning and operating tools required. Rapidly decreasing costs/increasing capabilities of sensors, communication systems, and computers offer unprecedented opportunities for deployment of advanced technologies for grid management. Join our team in developing nation's most advanced modeling, simulation, and optimization tools to provide insight and actionable information to key decision makers.

What You Will Do

- Analyze critical infrastructure security architectures/protocols/technologies for vulnerabilities.
- Conduct vulnerability assessments and penetration testing (field/lab, wired/wireless, hardware/software/network).
- Research/develop secure technologies/architectures for existing power and gas architectures.
- Design, implement, deploy, and maintain software systems using object-oriented analysis, design, and programming techniques.
- Collaborate to develop innovative methods; fulfill deliverables as a team.
- Serve as the primary technical contact on specific projects.
- Brief sponsors on the results and impact of research accomplishments.
- Travel to support project needs/deadlines or to attend job related conferences and workshops.

Careers

- Career Opportunities
- Internships + Co-Ops
- Scholarships
- Recruiting Events
- Compensation + Benefits
- Contact Talent Acquisition
- Careers FAQs

Career Opportunities

Network Security Analyst- 1100607- Regular

USA-WA-Spokane/Liberty Lake

Description

As the alternative energy industry continues to grow, the "smart grid" sector continues to be of particular interest to security protection due to the demand for wireless data accessibility. Itron's growth has presented an opportunity for a solid IT Security Analyst to join the growing team to lead the US side of the business focusing on network security and compliance.

Itron has an immediate opening for an IT Network Security Analyst with a knack for breaking and fixing network security. This individual will execute security controls to prevent hackers from infiltrating company information or jeopardizing e-commerce programs and research attempted efforts to compromise security protocols. Maintain and Monitor security relevant infrastructure components and collaborate with IT operations. Administers security policies to control access to systems including the company's firewalls. Uses applicable encryption methods. Provides information to management regarding the negative impact on the business caused by violation of confidentiality, integrity or availability of information and information systems.

Duties and Responsibilities:

- Implement centralized logging for network and security infrastructure
- Audits user and system security configurations for compliance with internal and external requirements
- Recommends process improvement
- Understands ISO27000 series of standards and Sarbanes Oxley rules surrounding IT
- Understands the application of security concepts across a broad scope of information technology areas including data communications, network design, operations, database structures, operating systems, application development, security risk assessment, and disaster recovery
- Understands security/controls risk vs. business impact in decision making
- Perform audits and follow-up on corrective actions

If you would like to learn more about the Spokane area, please click on this link.

Qualifications

Preferred Skills & Experience: This position requires a minimum of 5 years of Security related experience

Smart-Grid Cyber Security Engineer in Ohio United States

Req ID 208296BR
Industry Job Title Smart-Grid Cyber Security Engineer
Standard Job Code/Title E2543:Info Assurance Engineer Sr
Required skills -Ability to design and/or architect end-to-end secure solutions for one or more of the following: network-centric systems, secure wireless mesh networking and embedded systems, large IT systems and internet security

-Security Policy and Standards development experience

-Security Risk Assessment experience

-Security operations experience including IDS/IPS, log management, incident detection and response

-Familiarity with the software development, testing and maintenance

-Strong interpersonal and communication skills
Desired skills -Electrical Utility working experience

-CISSP

-Previous consulting experience

-Software Development experience
Specific Job Description Energy and Cyber Services is seeking a cyber architect with a broad range of skills including information assurance, security engineering, systems architecture and SDLC experience. The role will include leadership and/or support of client facing consulting engagements. Successful applicant will need to be interviewed and accepted by the client.

Successfull applicant will need to be interviewed and accepted by the client.
Standard Job Description Provides security engineering designs and implementation in all aspects of Information Assurance and Information Security (InfoSec) Engineering. Assesses and mitigates system security threats/risks throughout the program life cycle; validates system security requirements definition and analysis; establishes system security designs; implements security designs in hardware, software, data, and procedures; verifies security requirements; performs system certification and accreditation planning and testing and liaison activities, and supports secure systems operations and maintenance.
Security Clearance None
Typical Minimums Bachelors degree from an accredited college in a related discipline, or equivalent experience/combined education, with 5 years of professional experience; or 3 years of professional experience with a related Masters degree.

Share

Current Search Criteria

Smart-Grid Cyber Security Engine...
Ohio
Clear All

Related Job Titles

Info Assurance Engineer Sr Stf (35)
Info Assurance Engineer Asc (32)
Info Assurance Engineer Stf (15)
Info Assurance Engineer (11)
Info Assurance Engineer Sr (10)
Information Assurance Specialist... (9)
Information Assurance Specialist... (9)
Information Assurance Specialist... (9)
Information Assurance Profession... (4)
Information Assurance Engineer A... (4)

Substation SCADA Integration Engineer

Category: Telecommunications

Type: Contract

Description: SCADA engineer responsible for assisting with the integrated design, programming, installation, and testing of with various substation integration/automation and Smart Grid projects. Experience required in SCADA and substation design, programming and installation.

Responsibilities include conceptual and detailed design creating/modifying/reviewing substation schematic drawings, wiring diagrams, one/three line drawings, and point lists. Responsibilities also include communication network design (Ethernet LAN and WAN), serial point-to-point communications, multi-drop networks, time synchronization design, device configurations, cyber security requirements and documentation.

Experience with standard industry substation wiring practices, instrumentation, protection, and controls required. Experience with programming, configuring and testing modern substation RTUs, Intelligent Electronic Devices (IEDs), and HMIs is required. Candidate must have basic understanding of protocols such as DNP3 and Modbus

Smart Grid Security Engineer - Westminster, CA

Southern California Edison
SCE - NB61727528EA - Smart Grid Security Engineer
Work Location: CA-Westminster

Basic Qualifications
Must have experience designing and/or architecting end-to-end secure solutions for one of more the following: network-centric systems, secure wireless mesh networking and embedded systems, large IT systems and internet security.

Core Competencies
- Bachelor's Degree in Electrical or Computer Engineering or a related field, or an equivalent combination of education, training, and work experience.
- Typically possesses three or more years of experience in Information Technology security, including communications and network security, performing analysis and providing recommendations.
- Demonstrated experience performing analysis, developing specifications, designing, constructing, testing and implementing secure solutions designs (i.e. red team analysis, penetration testing).
- Demonstrated experience with network management, performance monitoring and optimization.
- Demonstrated ability to abstract the solution architecture into different views and domains, apply critical thinking skills, technical ingenuity, creativity, and resourcefulness to ensure the security will continue to be viable.
- Demonstrated knowledge of security standards and testing tools and methods (i.e. NIST800-53, PKI).
- Demonstrated strong oral and written communication skills, and be customer focused to understand and appropriately respond to business requirements.
- Demonstrated experience interfacing and collaborating with clients, peers, and management to develop solutions.
- Demonstrated proficiency with PC applications, including Microsoft Word, Excel, Access, PowerPoint and Visio.
- Must demonstrate the ability to integrate work across relevant areas, develop the business and services to enhance customer satisfaction and productivity, manage risks and safety appropriately, develop and execute business plans, manage information, and provide exceptional service to internal and external customers.
- Must demonstrate effective resource and project planning, decision making, results delivery, team building, and staying current with relevant technology and innovation.
- Must demonstrate strong ethics, influence and negotiation, leadership, interpersonal skills, communication, the ability to effectively manage stress and engage in continuous learning.

Engineer - Protection Emphasis (Government Services)

Location: Pullman, WA
Date: 10/25/2011
Categories: Engineering
Biomedical Engineering
Education
Electronics Engineer
Quality Control
Robotics

SCHWEITZER ENGINEERING LABORATORIES

Schweitzer Engineering Laboratories, Inc.

Job Details

Engineer - Protection Emphasis (Government Services)

Job Description:

The Opportunity:
Schweitzer Engineering Laboratories, Inc. (SEL) seeks two Protection Engineers for our Government Engineering Solutions team to design and develop advanced power system solutions for military installations across the country. The positions will work out of our Pullman, Washington offices.

Are you ready to develop state-of-the-art monitoring, control, and automation equipment for distribution power systems? Would you like to work for a company that continuously invests in new product development and truly values the contributions of smart, dedicated engineers like yourself? Our products protect, monitor, and control transmission lines, transformers, bus bars, capacitor banks, distribution feeders, generators, and motors worldwide. If you are an engineer with demonstrated experience in application, support, and development of transmission or distribution systems, we invite you to consider joining our team.

SELs corporate office is located in Eastern Washington where you'll enjoy an unmatched quality of life. Enjoy the smaller town life: country space, freedom from traffic, easy access to recreational activities in nearby mountains, rivers, and forests, as well as great schools and universities.

Engineer - Protection Emphasis (Government Services)
Responsibilities:

- Develop and maintain an acceptable/moderate/high level of technical expertise in electric power system protection and/or automation.
- Work within the project team to develop project deliverables.
- Train and assist customers with the installation, commissioning and operation of automation and/or protection systems, both on-site and from SEL offices.

Appendix F – National Initiative for Cybersecurity Education Framework

Securely Provision – Specialty areas concerned with conceptualizing, designing, and building secure information technology (IT) systems, with responsibility for some aspect of the system's development.

Table F.1 NICE Framework: Securely Provision

SGC Job Role	NICE Specialty Area Label	NIST Sample Job Title
Smart Grid Risk & Vulnerability Analyst	Information Assurance Compliance – oversees, evaluates, and supports the documentation, validation, and accreditation process necessary to assure that new IT systems meet organization's IA requirements. Ensures compliance from internal and external perspectives.	Risk/Vulnerability Analyst
Smart Grid Security Architect	Systems Requirements Planning – Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions. Provides guidance to customers about applicability of information systems to meet business needs.	Solutions Architect, Systems Engineer, Systems Consultant, etc.

Operate and Maintain – Specialty areas responsible for providing the support, administration, and maintenance necessary to provide effective and efficient IT system performance and security.

Table F.2. NICE Framework: Operate and Maintain

SGC Job Role	NICE Specialty Area Label	NIST Sample Job Title
Smart Grid Risk & Vulnerability Analyst	Information Assurance Compliance – oversees, evaluates, and supports the documentation, validation, and accreditation process necessary to assure that new IT systems meet organization's IA requirements. Ensures compliance from internal and external perspectives.	Risk/Vulnerability Analyst
Smart Grid Security Architect	Systems Requirements Planning – Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions. Provides guidance to customers about applicability of information systems to meet business needs.	Solutions Architect, Systems Engineer, Systems Consultant, etc.

Protect and Defend – Specialty areas responsible for the identification, analysis, and mitigation of threats to internal IT systems or networks.

Table F.3. NICE Framework: Protect and Defend

SGC Job Role	NICE Specialty Area Label	NIST Sample Job Title
Network Security Specialist	Computer Network Defense – Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.	Network Defense Technician
Security Operations Specialists	Computer Network Defense & Computer Network Defense Infrastructure Support – Tests, implements, deploys, maintains, and administers the infrastructure hardware and software that are required to effectively manage the computer network defense service provider network and resources. Monitors network to actively remediate unauthorized activities.	Security Operator, IDS Technician, Network Security Specialists
Incident Response Specialists	Incident Response – Responds to crisis or urgent situations within pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.	Incident Handler, Incident Responder, Computer Crime Investigator
Intrusion Analyst	Incident Response – above	Intrusion Analyst
Penetration Tester/Red Team Technician	Vulnerability Assessment and Management – Conducts assessments of threats and vulnerabilities, determines deviations from acceptable configurations, enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.	Penetration Tester, Red Team Technician, Ethical Hacker, Blue Team Technician
Reverse Engineer	Vulnerability Assessment and Management – above	Reverse Engineer

Appendix G– Operational Excellence Vignettes

Item	Description
1	Grid operating in a known non-secure mode when operators believed it to be running securely.
2	Request to operator to disable a security component where security infrastructure is believed to be confusing to a normal systems task.
3	Usage of administrator or original user profile on a network-linked computer. (Far easier to be hacked than a non-administrator user profile.)
4	Improper or incomplete testing of application code causes master system to fail once code is rolled into production.
5	Insufficient separation of communication functions between a general-purpose information technology (IT) network/system and a control system network (via Internet Protocol or Ethernet).
6	Impetus to centralize or simplify existing network architecture.
7	Lack of patching of a general-purpose operating system (Microsoft Windows, Linux, Unix, etc.) (lack of operational control) used for control systems.
8	Unknown vendor or third-party service organization engineering level (back door) access to various systems and devices that get published and abused.
9	New threat issued against a specific piece of hardware (HW) or software (SW).
10	Utilizing unvalidated or untested third-party components (RNG, IC) or third-party software in your meter, product, platform.
11	Control system vendors shipping products with insecure web or other internet services running.
12	Provisioning and de-provisioning of users and access control - (employee terminations and hires, etc.)
13	RCE of various utility and vendor internal engineering/configuration tools to discover embedded credentials or methods of access to system and devices that would bypass established security controls.
14	System categorization changes, e.g., high system connects to medium system and is detected. Need to redefine architecture or revisit system.
15	New data point, new data is requested from a smart grid device that has not been yet been used.
16	Vendor source code shows up at DEFCON.
17	Share account usage on ICS/Line devices - no centralized authentication.
18	System and/or device disposal/retirement.
19	Mandate to submit annual reports to governing body detailing compliance of cybersecurity measures.
20	Field device aggregation point configured to allow remote administration of the cellular modem via multiple management interfaces.
21	Misconfiguration of field network device allowing network leakage.
22	Arbitrary electrical usage increases.
23	When attempting to send a disconnect command to a smart meter, you do not get confirmation that the disconnect switch was tripped.
24	Frequency hopping (FHSS) sequence vulnerable to hardware bus sniffing.
25	Misconfiguration or inadequate security controls implemented based on false sense of security of closed system.
26	Default SNMP (Simple Network Management Protocol) community strings used on internal and/or field devices.
27	Poor vendor participation in deployment and security assessments.
28	Inadequate security control management due to lack of policy and procedure development.
29	Lack of an incident response process.
30	Risk-based decision making that balances business, compliance, safety, and security.
31	You want to get more out of less, and want to do so by investigating any possible opportunities to centralize.
32	Signatures and responding to what matters to eliminate the noise from the field and enterprise.
33	Running security tests on equipment and software that might brick, reset, or crash a system.

Item	Description
34	When to start and document the chain of custody of digital evidence and maintain it during an investigation.
35	My honeynet is fulfilling its operational function, how far do I let this activity continue?
36	Neighborhood network usage spikes exceed normal or expected network traffic. Authorized meter traffic does not account for the increased usage.
37	Strategic decision making around the purchasing, timing, cost, and placement of security.
38	Field network goes down for 24 hours and no visibility into devices and no logs. Do we trust them?
39	How to effectively scan the network and produce actionable reports to find and monitor all active and known devices?
40	Supply chain security and trust thereof.
41	From my evidence pattern, can I distinguish what my adversary is, a who, what, when, and why? Nation state - trusted insider- criminal activist.
42	A series of field walk-downs has identified unaccounted-for devices and connections in substations and field sites associated with the new smart grid technology being deployed. Your policy calls for strong asset management and security has been tasked to identify any unauthorized connections or devices.
43	Project manager wants to deploy, however, significant security risks are present -- how to effectively and logically communicate and drive change that makes business sense?
44	My historical event data is mined, and correlated into a real-time engine, providing predictive events, critical functions are mapped into this engine, allowing immediate impact analysis to determine appropriate response action.
45	Define a plan to allow for routine updates of firmware for security fixes, etc.
46	How to effectively deal with any shared accounts on devices, especially when employees are term.
47	Some systems do not support centralized key management and/or easy key rotation. Could be an issue if a key is compromised.
48	Distribution Automation Control remote terminal unit (RTU) firmware snippets are being reported by NESCO as being recovered from two underground webpages associated with hacking research. The firmware snippets are being reported as belonging to equipment that you have recently deployed.
49	Seed value generation and nonce composition during key derivation.
50	HW and SW vendor selection – with respect to security functionality.
51	Senior management has been warned that employees are using personal e-mail accounts (e.g., gmail, yahoo) to mail company documents that may include sensitive info. Privacy and internal audit want to talk with security about technical options for discouraging if not stopping this behavior.
52	Vendor management and related procurement language.
53	Out-of-band networking is utilized for security activities; one may also be used for enterprise social media as a sandbox.
54	Internal guidance discouraging the use of Universal Serial Bus (USB) sticks in IT and particularly OT systems do not seem to be working. What can be done to protect equipment from malware using this vector? What are the options?
55	A regional NERC auditor asked for artifacts of security vulnerability assessments covering your phasor data concentrators and phasor measurement units communication network.
56	What are the criteria to establish one as a Qualified Witness in a legal process?
57	Receive a vulnerability alert impacting a deployed smart grid device.

Appendix H– Threat or Vulnerability Response Vignettes

Item	Description
58	Smart-meter electronic tampering (electricity theft).
59	Resource depletion through flooding.
60	Command set or data interception.
61	DNS Spoofing Portals and Gateway Devices.
62	Smart-meter wireless carrier distributed denial of service (DDOS).
63	Individual smart meter denial of service (DOS).
64	MiM attack to capture new encryption keys.
65	Worm enables code execution on a deployed utility meter.
66	Poisoned timing data input to disrupt synchronization.
67	False data input into power system state estimation model.
68	Loss of business-sensitive or personally identifiable information (PII) data.
69	Suspected or actual intrusion into or capture of operator public key infrastructure.
70	Disruption of information flow between different operational systems used in utility operations with the intent to destabilize the power system.
71	Remote access methods through an Internet Protocol network with the intent to escalate privileges and gain control over control systems management computers.
72	Capture of confidential information through unmonitored external storage device (USB, CD, etc.).
73	Denial-of-service attack on utility communications network to disrupt system control.
74	Phishing attack directed toward an entry-level position/new account in an effort to obtain valuable login/network access to various systems and devices that get published and abused.
75	Rogue device attached to secure network, grabbing IP address of authorized device, generating security event management alerts.
76	Introduction of unauthorized content (e.g. PDFs, images, executables, etc.) with embedded malware/advanced threats through local and privileged access ports (e.g. USB ports and devices).
77	Smart meter optical port password (c12.18 master password) for an entire utility territory is posted to the internet along with instructions on how customers can reconfigure their meter to decrease actual consumption readings. This information is actively being used by customers.
78	Creation of DOS conditions in power system components through gaming or abuse of poorly implemented security controls.
79	Discovery or suspicion of a cloned device (e.g. alert of a device operating on the network in a way that no one device could, such as same device ID appearing in two service territories.)
80	Reported theft of a hand-held or mobile terminal that can access the smart grid.
81	Gaming/excessive generation of intrusion detection/prevention events in order to blind a system to a real attack, or have defenders loosen rules to facilitate a real attack.
82	Unauthorized access to a network or system (same for unauthorized data manipulation).
83	Rogue devices with wireless communications enabled are being placed in multiple substations and accessed remotely by attacker to probe the substation infrastructure and communications links back to the utility. It is unknown how many substations are affected.
84	Targeted resource exhaustion (e.g., packets of death, message floods, bad configuration states, etc.) of critical control/monitoring devices in order to disable power or information system protections.
85	It was recently discovered that a rogue communications tunnel was set up between the control center network and the internet using a corporate machine as an intermediate proxy. Upon further investigation, it is realized that firewall rules between the control center and corporate network have been changed to enable this tunnel.
86	Introduction of viruses/malware into control system computers via smart grid operators' use of removable media (e.g., USB thumb drives).
87	Malware infects hybrid vehicles (causing explosive battery overcharging).

Item	Description
88	Social engineering of utility and vendor personnel to discover undocumented accesses to various systems and devices that get published and abused.
89	You learn that a specific field device you recently deployed uses non-secure wireless communications and is being attacked by unknown persons.
90	Unencrypted memory storage components in meters that contain C12.18 security codes.
91	You learn that the vendor that processes your meter data has been compromised via news wire.
92	Unencrypted C12.18 communications allowed for the interception of the C12.18 security code.
93	Several customers call into your help desk and report their power out and there are no known natural incidents (such as lightning strikes, snow storms, etc.) that have been detected in the area.
94	Loss or unauthorized access/release of PII data.
95	You believe an opponent has gained access to your network, and you want to detect where.
96	Your PKI (public key infrastructure) has been compromised and you want to react.
97	A rogue device is introduced to the AMI network.
98	Compromised device has maliciously embedded hardware or chipset.
99	Mobile radio frequency (RF) jamming is detected through node outages, can I overlay these to geographical information system (GIS) mapping?
100	Same meter password is used on all meters and is now posted on a public website.
101	An e-mail has been sent to key project team leaders associated with smart grid deployments. The e-mail referenced a presentation provided by one of the company's executives and contained a .pdf document. The document was found to contain code that executed.
102	The security desk receives a call from the local FBI field office requesting information about the type of smart meters your utility is deploying. An active criminal investigation has led to a warrant search that turned up several smart meters at a warehouse suspected of criminal activity.
103	Hostile malware has affected my systems. Is this local or are neighboring entities affected (my vendors/partners/other neighboring utilities)?
104	A message from “anonymous” was posted on a community message board warning of a campaign against your company for failing to address meter billing problems and your company’s decision to build a new advanced light water reactor at one of your existing nuclear power plant sites.
105	Use advanced visual analytics to rapidly find the outlier of events in big data as an investigation technique. Or, mine deeply to find the imbedded event that wishes to cloak its activities.
106	A member of the public utility commission e-mailed a complaint received from a customer that suggested an employee of the company was providing information about individual customer electricity usage on Facebook.

Appendix I – Master Vignettes

Data Leakage/Theft
Loss of business sensitive or PII data.
Capture of confidential information through unmonitored external storage device (USB, CD, etc.).
Reported theft of a hand-held or mobile terminal that can access the smart grid.
Misconfiguration of field network device allowing network leakage.
Loss or unauthorized access/release of PII data.
The security desk receives a call from the local FBI field office requesting information about the type of smart meters your utility is deploying. An active criminal investigation has led to a warrant search that turned up several smart meters at a warehouse suspected of criminal activity.
Senior management has been warned that employees are using personal email accounts (e.g. Gmail, yahoo) to mail company docs that may include sensitive info. Privacy and internal audit want to talk with security about technical options for discouraging if not stopping this behavior.
A member of the public utility commission e-mailed a complaint received from a customer that suggested an employee of the company was providing information about individual customer electricity usage on Facebook.
Network Attacks
Resource Depletion through Flooding.
Command set or data interception.
DNS Spoofing Portals and Gateway Devices.
Smart Meter Wireless Carrier DDOS.
MiM attack to capture new encryption keys.
Disruption of information flow between different operational systems used in utility operations with the intent to destabilize the power system.
Denial of service attack on utility communications network to disrupt system control.
Rogue device attached to secure network, grabbing IP address of authorized device, generating SEM alerts.
Creation of DoS conditions in power system components through gaming or abuse of poorly implemented security controls.
Gaming/excessive generation of intrusion detection/prevention events in order to blind a system to a real attack, or have defenders loosen rules to facilitate a real attack.
Targeted resource exhaustion (e.g. packets of death, message floods, bad configuration states, etc) of critical control/monitoring devices in order to disable power or information system protections.
You learn that a specific field device you recently deployed uses insecure wireless communications and is being attacked by unknown persons.
Frequency hopping (FHSS) sequence vulnerable to hardware bus sniffing.
Signatures and responding to what matters to eliminate the noise from the field and enterprise.
Man in the middle attack detected - sensitive information/ PII data between the head end systems and the data collector has been compromised.
Security Testing
Improper or incomplete testing of application code causes master system to fail once code is rolled into production.
Unknown vendor/3rd party service organization engineering level (back door) access to various systems and devices that get published and abused.
Utilizing unvalidated or untested third party components (RNG, IC) or third-party software in your meter, product, or platform.
Substation/SCADA Attacks
Poisoned Timing Data Input to Disrupt Synchronization.
False data input into power system state estimation model.

Rogue devices with wireless communications enabled are being place in multiple substations and accessed remotely by attacker to probe the substation infrastructure and communications links back to the Utility. It is unknown how many substations are affected.
Compromised device has maliciously embedded hardware or chipset.
“Zero Day” attack - new malware detected on control system components.
Physical security vulnerability: LAN ports in common areas in Office premises/ Sub-stations/ Datacenter allow access to anyone connecting to that port.
AMI Attacks
Smart Meter Electronic Tampering (Electricity Theft).
Worm enables code execution on a deployed utility meter.
Smart meter optical port password (c 2 8 master password) for an entire utility territory is posted to the Internet along with instructions on how customers can reconfigure their meter to decrease actual consumption readings This information is actively being used by customers.
A rogue device is introduced to the AMI network.
Same meter password is used on all meters and is now posted on a public website.
Client Side Attacks
Introduction of unauthorized content (e.g. PDFs, Images, Executable, etc.) with embedded malware/advanced threats through local and privileged access ports (e.g. USB ports and devices).
Usage of administrator or original user profile on a network-linked computer (Far easier to be hacked than a non-administrator user profile).
Unauthorized access to a network or system (same for unauthorized data manipulation).
It is recently discovered that a rogue communications tunnel was set up between the control center network and the Internet using a corporate machine as an intermediate proxy. Upon further investigation, it is realized that firewall rules between the control center and corporate network have been changed to enable this tunnel.
Introduction of viruses/malware into control system computers via smart grid operator’s use of removable media (e.g. USB thumb drives).
Internal guidance discouraging the use of USB sticks in IT and particularly OT systems doesn't seem to be working. What can be done to protect equipment from malware using this vector? What are the options?
Phishing Incidents
Phishing attack directed toward an entry-level position/new account in an effort to obtain valuable login/network access to various systems and devices that get published and abused.
Social engineering of utility and vendor personnel to discover undocumented accesses to various systems and devices that get published and abused.
An e-mail has been sent to key project team leaders associated with smart grid deployments. The e-mail referenced a presentation provided by one of the company's executives and contained a PDF document. The document was found to contain code that executed.
Risk management, compliance and audit
Mandate to submit annual reports to governing body detailing compliance of cybersecurity measures.
Risk-based decision making that balances business, compliance, safety, and security.
Strategic decision making around the purchasing, timing, cost, and placement of security.
Project manager wants to deploy, however, significant security risks are present -- how to effectively and logically communicate and drive change that makes business sense?
HW and SW vendor selection – W. R. T. security functionality.
Network Separation and Attack Paths
Remote access methods through an Internet Protocol network with the intent to escalate privileges and gain control over control systems management computers.
Insufficient separation of communication functions between a general-purpose IT network/system and a control system network (via Internet Protocol or Ethernet).
Impetus to centralize or simplify existing network architecture.
System categorization changes, e.g., high system connects to medium system and is detected. Need to redefine architecture or revisit system.

Field device aggregation point configured to allow remote administration of the cellular modem via multiple management interfaces.
Incident Response Process & Log Management
Grid operating in a known non-secure mode when operators believed it to be running securely.
New data point, new data is requested from a Smart Grid device that has not been yet been used.
Lack of an incident response process.
You believe your an opponent has gained access to your network, and you want to detect where.
When to start and document the "chain of custody" of digital evidence and maintain it during an investigation.
My honeynet is fulfilling its operational function, how far do I let this activity continue?
Neighborhood network usage spikes exceed normal or expected network traffic. Authorized meter traffic does not account for the increased usage.
Field network goes down for 2 hours and no visibility into devices and no logs. Do we trust them?
Hostile malware has affected my systems. Is this local or are neighboring entities affected (my vendors/partners/other neighboring utilities)?
Use advanced visual analytics to rapidly find the outlier of events in big data as an investigation technique. Or, mine deeply to find the imbedded event that wishes to cloak its activities.
Encryption Attacks
Suspected or actual intrusion into or capture of operator public key infrastructure.
Your PKI has been compromised and you want to react.
Some systems don't support centralized key management and/or easy key rotation. Could be an issue if a key is compromised.
Seed value generation and nonce composition during key derivation.
Control system vendors shipping products with non-secure web or other Internet services running.
Poor vendor participation in deployment and security assessments.
Inadequate security control management due to lack of policy and procedure development.
Running security tests on equipment and software that might brick, reset, or crash a system.
How to effectively scan the network and produce actionable reports to find and monitor all active and known devices?
Threat & Vulnerability Management
Lack of patching of a general-purpose operating system (Microsoft Windows, Linux, Unix, etc.) (lack of operational control) used for control systems.
New threat issued against a specific piece of HW/SW.
Vendor source code shows up at DEFCON.
You learn that the vendor that processes your meter data has been compromised via news wire.
Misconfiguration or inadequate security controls implemented based on false sense of security of closed system.
Default SNMP community strings used on internal and/or field devices.
Supply chain security and trust thereof.
A series of field walk-downs has identified unaccounted-for devices and connections in substations and field sites associated with the new smart grid technology being deployed. Your policy calls for strong asset management and security has been tasked to identify any unauthorized connections or devices.
Define a plan to allow for routine updates of firmware for security fixes, etc.
Distribution Automation Control RTU firmware snippets are being reported by NESCO as being recovered from two underground webpages associated with hacking research. The firmware snippets are being reported as belonging to equipment that you have recently deployed.
Remote Code Execution vulnerability detected on several AMI components - smart meter, data collector, etc. due to patch related issue.
Access Control Maintenance
Provisioning and de-provisioning of users and access control - (employee terminations and hires, etc).
Share account usage on ICS / Line devices - no centralized authentication.
How to effectively deal with any shared accounts on devices, especially when employees are terminated.

Appendix J – Master Vignettes Process Stages

Data Leakage / Theft
Preconditions
Onset
Analysis of information and risk
Actively test or assess networks for evidence of leakage or misconfigurations
Asset management inventory and review of known good configuration files
Observable identified by organization through user reports or security alert
Observe artifacts of data leakage, theft, misconfigured devices
Identify suspicious activity or suspect configurations and analyze
Security Group/Help Desk initiates Incident Response process
Contain the incident
Eradication and ongoing mitigations
Collect and gather information and evidence to support analysis
Develop after-action report and assess loss if any
Correct any misconfigurations or findings
Validate mitigations and assess policy/strategy
Root cause analysis as to why configurations were not as planned or expected
Conclusions
Network Attacks
Preconditions
Onset
Observable identified by organization through user reports or security alert
Security Group/Help Desk initiates Incident Response process
Contain the incident
Analysis of information and risk
Eradication and ongoing mitigations
Collect and gather information and evidence to support analysis
Notify users whose information has been compromised
Develop after-action report and assess loss if any
Validate mitigations and assess policy/strategy
Conclusions
Substation / SCADA Attacks
Preconditions
Onset
Observable identified by organization through user reports or security alert
Analysis of information and risk
Contain the incident
Security Group/Help Desk initiates Incident Response process
Collect and gather information and evidence to support analysis
Validate mitigations and assess policy/strategy
Develop after-action report and assess loss if any
Eradication and ongoing mitigations
Conclusions
AMI Attacks
Preconditions
Onset
Design and implement or update the policies of implemented Security Incident and Event Management (SIEM) to make sure that such breaches are detected, alerted, ticket created and response provided.
Create or update the security incident detection and response framework
Observable identified by organization through user reports or security alert
Contain the incident

Analysis of information and risk
Security Group/Help Desk initiates Incident Response process
Collect and gather information and evidence to support analysis
Eradication and ongoing mitigations
Validate mitigations and assess policy/strategy
Develop after-action report and assess loss if any
Conclusions
Client-Side Attacks
Preconditions
Onset
Observable identified by organization through user reports or security alert
Security Group/Help Desk initiates Incident Response process
Contain the incident
Collect and gather information and evidence to support analysis
Analysis of information and risk
Eradication and ongoing mitigations
Validate mitigations and assess policy/strategy
Develop after-action report and assess loss if any
Notify users whose information has been compromised
Asset Management: Ensure that all the IT assets are accounted for within in the infrastructure and they are monitored.
Electronic Perimeter: define the perimeter and the information exit points in the infrastructure and implement appropriate controls like firewall, IDS/ IPS. Data Loss Prevention, etc
Conclusions
Phishing Incidents
Preconditions
Onset
Observable identified by organization through user reports or security alert
Security Group/Help Desk initiates Incident Response process
Contain the incident
Collect and gather information and evidence to support analysis
Analysis of information and risk
Eradication and ongoing mitigations
Validate mitigations and assess policy/strategy
Develop after-action report and assess loss if any
Conclusions
Network Separation and Attack Paths
Preconditions
Onset
Identify attack routes.
Observable identified by organization through user reports or security alert
Security Group/Help Desk initiates Incident Response process
Contain the incident
Identify Purpose of Network Connection (e.g. why is the network configured this way.)
Collect and gather information and evidence to support analysis
Analysis of information and risk
Eradication and ongoing mitigations
Validate mitigations and assess policy/strategy
Develop after-action report and assess loss if any
Observable identified by organization through user reports or security alert
Conclusions
Incident Response Process & Log Management
Preconditions
Onset

Identify stakeholders and incident response parties internal to the organization
Educate all employees and stakeholders on the process and program
Identify parties to coordinate with and notify external to the organization
Design and implement security information management tools, platforms, and alert logic
Observable identified by organization through user reports or security alert
Security Group/Help Desk initiates Incident Response process
Contain the incident
Collect and gather information and evidence to support analysis
Analysis of information and risk
Eradication and ongoing mitigations
Validate mitigations and assess policy/strategy
Review risk management, Business Impact, and risk registry information to incorporate into Incident Response
Conclusions
Encryption Attacks
Preconditions
Onset
Observable identified by organization through user reports or security alert
Security Group/Help Desk initiates Incident Response process
Contain the incident
Collect and gather information and evidence to support analysis
Analysis of information and risk
Eradication and ongoing mitigations
Validate mitigations and assess policy/strategy
Develop after-action report and assess loss if any
Conclusions
Security Testing
Preconditions
Onset
Establish testing program requirements and resources
Establish rules of engagement
Identify Vendor Security Contacts
Develop Site Acceptance Testing Procedure that will identify insecure or unnecessary services
Set testing targets and timeline
Test equipment during SAT
Develop exploit or custom code to evaluate possible vulnerabilities if required
Chose and train security tools
Develop schedule and test plans based on risk
Conduct test - evaluate attack surface and scan for vulnerabilities
Record findings and prioritize based on risk
Present findings and recommendations
Act on findings and update programs/policy as required
Work with vendor to solve the problem or develop working mitigations
Test mitigations and develop a security operations plan to monitor remaining weaknesses/attack scenarios
Conclusions
Threat & Vulnerability Management (patching, hardening)
Preconditions
Onset
Monitor open source information and vendors for vulnerability and threat information
Analyze vulnerability reports, alerts, and exploit tools or code
Conduct inventory of software, hardware, technology and map to business process
Determine risk, mitigation options, investment, and action plan
Review Risk Map and Risk Assessments and map to vulnerability management process

Deploy mitigations and or additional controls, reduce access, heighten monitoring
Work with vendor and internal teams to plan, test, and deploy patches
Update risk assessments and risk registry based on analysis
Update audit playbook and plans
Update education programs such as awareness and training
Validate mitigations and assess policy/strategy
Conclusions
Access Control Maintenance
Preconditions
Onset
Take inventory of devices and systems that use shared accounts
Review authorization and provisioning process for users that have shared access
Conduct risk assessment based on results of inventory and reviews
Consider mitigation options and present risk reduction ROI to management
Implement mitigations if any
Prepare security operations, incident response, and intrusion detection
Test shared user accounts for exploitable process and weaknesses
Conclusions
Risk Management, Compliance and Audit
Preconditions
Onset
Identify all compliance requirements
Analyze risk and obligations against current state (investments, controls, risk/rewards)
Identify decision points and business process (like budgeting)
Conduct a strategic risk assessment for the organization
Define overarching security policy
Link efforts to governance process and enterprise risk management process
Audit and test decisions, fielded controls/mitigations, and investments
Conclusions

Appendix K – Nominal Number of Job Roles

Job Roles	Access Control Maintenance	AMI Attacks	Client-Side Attacks	Data Leakage/Theft
Security Operations Specialists	2	9	9	11
Chief Security Operations Manager		5	7	5
Incident Response Specialist/Analyst	1	7	6	7
Manager of Technology	7	4	4	6
Security Administrator	8	5	6	5
Intrusion Analyst	2	6	6	5
Control System Engineer	6	3	4	8
Advanced Meter Security Specialist	6	4	3	9
Cyber Threat Analysis	5	3	4	4
Hardware Support Specialist	6	3	4	9
Meter or Field Device Technician	5	3	3	9
Network Security Analyst	3	3	3	7
Telecommunications Engineer	1	4	3	9
Information Security Risk Analyst III	4	3	3	3
Smart Grid Security Engineer	5	3	3	6
Exploitation Analysis	3	4	4	3
Security Investigator		5	5	4
Substation SCADA Integration Engineer		3	3	6
Network Security Specialists	2	3	2	6
SCADA Protocol Engineer		2	1	5
Protection Emphasis Engineer	2	2	2	4
All Source Intelligence		3	2	2
Risk/Vulnerability Analyst	4	1	1	2
Privacy Analyst		2	3	4
Penetration Tester/Red Team Technician	2	1	1	2
Legal Advice and Advocacy		1	2	1
Operational Security Testing Professional	3	1	1	2
Reverse Engineer		2	2	2
Utility Chief Operating Officer		1	2	1
Education and Training		1	2	
Strategic Planning and Policy Development	4	1	1	1
Senior Software Security Analyst	2	1	1	1
Security Architect	4			
Smart Grid Operations Engineer		2	1	3
Information Security Analyst	4			1
Enterprise Architect	3			
IT Auditor				3
IT Development Supervisor				
Smart Grid Architect				
Data/Information Quality Analyst	1			4
Integrative Security Assessment Researcher				1

Job Roles	Access Control Maintenance	AMI Attacks	Client-Side Attacks	Data Leakage/Theft
Smart Grid Sr. Manager – Professional Services	1			2
Provisioning Specialist	1			
Smart Grid Consultant				
Security Operations Specialists	10	11	9	9
Chief Security Operations Manager	5	9	8	5
Incident Response Specialist/Analyst	8	11	7	9
Manager of Technology	4	7	4	5
Security Administrator	6	5	5	8
Intrusion Analyst	6	6	7	8
Control System Engineer	4	3	4	4
Advanced Meter Security Specialist	4	3	3	4
Cyber Threat Analysis	4	4	6	5
Hardware Support Specialist	4	3	3	3
Meter or Field Device Technician	4	3	3	4
Network Security Analyst	4	4	5	7
Telecommunications Engineer	4	3	5	4
Information Security Risk Analyst III	4	3	3	5
Smart Grid Security Engineer	3	3	4	3
Exploitation Analysis	3	3	5	5
Security Investigator	5	6	5	5
Substation SCADA Integration Engineer	4	3	3	3
Network Security Specialists	2	3	4	4
SCADA Protocol Engineer	2	2	3	4
Protection Emphasis Engineer	3	2	2	3
All Source Intelligence	2	2	3	3
Risk/Vulnerability Analyst	2	2	2	2
Privacy Analyst	2	3	3	1
Penetration Tester/Red Team Technician	1	2	1	3
Legal Advice and Advocacy	1	4	2	2
Operational Security Testing Professional		2	1	1
Reverse Engineer	2	2	2	3
Utility Chief Operating Officer	1	4	2	1
Education and Training	3	2	2	2
Strategic Planning and Policy Development	1	1	1	2
Senior Software Security Analyst		2	1	2
Security Architect		3		4
Smart Grid Operations Engineer			1	
Information Security Analyst		2		
Enterprise Architect		2		1
IT Auditor		1		
IT Development Supervisor				1
Smart Grid Architect		2		1
Data/Information Quality Analyst				
Integrative Security Assessment Researcher				2
Smart Grid Sr. Manager – Professional				1

Job Roles		Access Control Maintenance	AMI Attacks	Client-Side Attacks	Data Leakage/Theft
Services					
Provisioning Specialist					
Smart Grid Consultant					1

Job Roles	Phishing Incidents	Risk Management	Security Testing	Substation/ SCADA Attacks	Threat & Vulnerability Management
Security Operations Specialists	10	1	3	8	4
Chief Security Operations Manager	6	8	11	5	10
Incident Response Specialist/Analyst	8			7	
Manager of Technology	4	4	7	4	7
Security Administrator	6	1	2	5	4
Intrusion Analyst	6		2	6	5
Control System Engineer	4	1	3	4	6
Advanced Meter Security Specialist	4		3	4	6
Cyber Threat Analysis	4	1	3	4	5
Hardware Support Specialist	4		3	3	6
Meter or Field Device Technician	4		3	4	6
Network Security Analyst	4		2	3	6
Telecommunications Engineer	4		3	4	5
Information Security Risk Analyst III	4	4	4	2	5
Smart Grid Security Engineer	3		3	3	5
Exploitation Analysis	3	1	2	4	4
Security Investigator	5			4	
Substation SCADA Integration Engineer	4		3	4	5
Network Security Specialists	2		1	3	3
SCADA Protocol Engineer	2		3	3	6
Protection Emphasis Engineer	3		3	2	4
All Source Intelligence	2	2	2	3	5
Risk/Vulnerability Analyst	2	4	3	1	5
Privacy Analyst	2	4	1	2	4
Penetration Tester/Red Team Technician	1	2	11	1	1
Legal Advice and Advocacy	1	5	3	1	4
Operational Security Testing Professional	1	2	11	1	1
Reverse Engineer	2		2	2	3
Utility Chief Operating Officer	1	7	1	1	1

Job Roles		Access Control Maintenance	AMI Attacks	Client-Side Attacks	Data Leakage/Theft
Education and Training	3	1	1	1	2
Strategic Planning and Policy Development	1	3	1	1	1
Senior Software Security Analyst	1		1	1	5
Security Architect		1	2		1
Smart Grid Operations Engineer			1	2	3
Information Security Analyst			1		5
Enterprise Architect		1	2		3
IT Auditor		3			2
IT Development Supervisor		2	3		2
Smart Grid Architect		1	2		2
Data/Information Quality Analyst					1
Integrative Security Assessment Researcher			1		2
Smart Grid Sr. Manager – Professional Services					1
Provisioning Specialist					2
Smart Grid Consultant					

Appendix L – Percent of Role Involvement

Table L.1. Percent of Role Involvement in Access Control Maintenance, AMI Attacks, Client-Side Attacks, and Data Leakage/Theft

A frequency distribution of roles across vignettes were used to assist in determining which job roles are the most critical, and consequently which vignettes (that heavily involve these job roles) are most relevant for further analysis. Accordingly, we calculate the percentage of steps in which a job role is involved for each of the master vignettes. Those roles which have the broadest involvement (sorted by rows with greatest number of green cells below) across the vignettes will be candidates for selection.

Job Roles	Access Control Maintenance	AMI Attacks	Client-Side Attacks	Data Leakage/Theft
Security Operations Specialists	**20.00%**	**69.23%**	**64.29%**	**64.71%**
Incident Response Specialist/Analyst	**10.00%**	**53.85%**	**42.86%**	**41.18%**
Chief Security Operations Manager		**38.46%**	**50.00%**	**29.41%**
Intrusion Analyst	**20.00%**	**46.15%**	**42.86%**	**29.41%**
Security Administrator	**80.00%**	**38.46%**	**42.86%**	**29.41%**
Manager of Technology	70.00%	30.77%	28.57%	35.29%
Security Investigator		38.46%	35.71%	23.53%
Advanced Meter Security Specialist	60.00%	30.77%	21.43%	52.94%
Hardware Support Specialist	60.00%	23.08%	28.57%	52.94%
Meter or Field Device Technician	50.00%	23.08%	21.43%	52.94%
Network Security Analyst	30.00%	23.08%	21.43%	41.18%
Control System Engineer	60.00%	23.08%	28.57%	47.06%
Cyber Threat Analysis	50.00%	23.08%	28.57%	23.53%
Telecommunications Engineer	10.00%	30.77%	21.43%	52.94%
Information Security Risk Analyst III	40.00%	23.08%	21.43%	17.65%
Smart Grid Security Engineer	50.00%	23.08%	21.43%	35.29%
Substation SCADA Integration Engineer		23.08%	21.43%	35.29%
Exploitation Analysis	30.00%	30.77%	28.57%	17.65%
Network Security Specialists	20.00%	23.08%	14.29%	35.29%
SCADA Protocol Engineer		15.38%	7.14%	29.41%
Protection Emphasis Engineer	20.00%	15.38%	14.29%	23.53%
Information Security Analyst	40.00%			5.88%
Privacy Analyst		15.38%	21.43%	23.53%
All Source Intelligence		23.08%	14.29%	11.76%
Security Architect	40.00%			
Risk/Vulnerability Analyst	40.00%	7.69%	7.14%	11.76%
Legal Advice and Advocacy		7.69%	14.29%	5.88%
IT Auditor				17.65%
Reverse Engineer		15.38%	14.29%	11.76%
Operational Security Testing Professional	30.00%	7.69%	7.14%	11.76%
Penetration Tester/Red Team Technician	20.00%	7.69%	7.14%	11.76%
Utility Chief Operating Officer		7.69%	14.29%	5.88%
Enterprise Architect	30.00%			
IT Development Supervisor				

Job Roles	Access Control Maintenance	AMI Attacks	Client-Side Attacks	Data Leakage/Theft
Education and Training		7.69%	14.29%	
Data/Information Quality Analyst	10.00%			23.53%
Smart Grid Operations Engineer		15.38%	7.14%	17.65%
Senior Software Security Analyst	20.00%	7.69%	7.14%	5.88%
Strategic Planning and Policy Development	40.00%	7.69%	7.14%	5.88%
Provisioning Specialist	10.00%			
Smart Grid Architect				
Integrative Security Assessment Researcher				5.88%
Smart Grid Sr. Manager – Prof. Services	10.00%			11.76%
Smart Grid Consultant				

Table L.2. Percent of Role Involvement in Encryption Attacks, Incident Response Process, Network Attacks, and Network Separation and Attack Paths

Job Roles	Encryption Attacks	Incident Response Process	Network Attacks	Network Separation and Attack paths
Security Operations Specialists	**90.91%**	**73.33%**	**75.00%**	**64.29%**
Incident Response Specialist/Analyst	**72.73%**	**73.33%**	**58.33%**	**64.29%**
Chief Security Operations Manager	**45.45%**	**60.00%**	**66.67%**	**35.71%**
Intrusion Analyst	**54.55%**	**40.00%**	**58.33%**	**57.14%**
Security Administrator	**54.55%**	**33.33%**	**41.67%**	**57.14%**
Manager of Technology	36.36%	46.67%	33.33%	35.71%
Security Investigator	45.45%	40.00%	41.67%	35.71%
Advanced Meter Security Specialist	36.36%	20.00%	25.00%	28.57%
Hardware Support Specialist	36.36%	20.00%	25.00%	21.43%
Meter or Field Device Technician	36.36%	20.00%	25.00%	28.57%
Network Security Analyst	36.36%	26.67%	41.67%	50.00%
Control System Engineer	36.36%	20.00%	33.33%	28.57%
Cyber Threat Analysis	36.36%	26.67%	50.00%	35.71%
Telecommunications Engineer	36.36%	20.00%	41.67%	28.57%
Information Security Risk Analyst III	36.36%	20.00%	25.00%	35.71%
Smart Grid Security Engineer	27.27%	20.00%	33.33%	21.43%
Substation SCADA Integration Engineer	36.36%	20.00%	25.00%	21.43%
Exploitation Analysis	27.27%	20.00%	41.67%	35.71%
Network Security Specialists	18.18%	20.00%	33.33%	28.57%
SCADA Protocol Engineer	18.18%	13.33%	25.00%	28.57%
Protection Emphasis Engineer	27.27%	13.33%	16.67%	21.43%
Information Security Analyst		13.33%		
Privacy Analyst	18.18%	20.00%	25.00%	7.14%
All Source Intelligence	18.18%	13.33%	25.00%	21.43%
Security Architect		20.00%		28.57%
Risk/Vulnerability Analyst	18.18%	13.33%	16.67%	14.29%

Job Roles	Encryption Attacks	Incident Response Process	Network Attacks	Network Separation and Attack paths
Legal Advice and Advocacy	9.09%	26.67%	16.67%	14.29%
IT Auditor		6.67%		
Reverse Engineer	18.18%	13.33%	16.67%	21.43%
Operational Security Testing Professional		13.33%	8.33%	7.14%
Penetration Tester/Red Team Technician	9.09%	13.33%	8.33%	21.43%
Utility Chief Operating Officer	9.09%	26.67%	16.67%	7.14%
Enterprise Architect		13.33%		7.14%
IT Development Supervisor				7.14%
Education and Training	27.27%	13.33%	16.67%	14.29%
Data/Information Quality Analyst				
Smart Grid Operations Engineer			8.33%	
Senior Software Security Analyst		13.33%	8.33%	14.29%
Strategic Planning and Policy Development	9.09%	6.67%	8.33%	14.29%
Provisioning Specialist				
Smart Grid Architect		13.33%		7.14%
Integrative Security Assessment Researcher				14.29%
Smart Grid Sr. Manager – Prof. Services				7.14%
Smart Grid Consultant				7.14%

Table L.3. Percent of Role Involvement in Phishing Incidents, Risk Management, Security Testing, Substation/SCADA Attacks, and Threat and Vulnerability Management

Job Roles	Phishing Incidents	Risk Management	Security Testing	Substation/ SCADA Attacks	Threat & Vulnerability Management
Security Operations Specialists	**90.91%**	**10.00%**	**16.67%**	**72.73%**	28.57%
Incident Response Specialist/Analyst	**72.73%**			**63.64%**	
Chief Security Operations Manager	**54.55%**	**80.00%**	**61.11%**	**45.45%**	71.43%
Intrusion Analyst	**54.55%**		**11.11%**	**54.55%**	35.71%
Security Administrator	**54.55%**	**10.00%**	**11.11%**	**45.45%**	28.57%
Manager of Technology	36.36%	40.00%	38.89%	36.36%	50.00%
Security Investigator	45.45%			36.36%	
Advanced Meter Security Specialist	36.36%		16.67%	36.36%	42.86%
Hardware Support Specialist	36.36%		16.67%	27.27%	42.86%
Meter or Field Device Technician	36.36%		16.67%	36.36%	42.86%
Network Security Analyst	36.36%		11.11%	27.27%	42.86%
Control System Engineer	36.36%	10.00%	16.67%	36.36%	42.86%
Cyber Threat Analysis	36.36%	10.00%	16.67%	36.36%	35.71%
Telecommunications Engineer	36.36%		16.67%	36.36%	35.71%
Information Security Risk Analyst III	36.36%	40.00%	22.22%	18.18%	35.71%
Smart Grid Security Engineer	27.27%		16.67%	27.27%	35.71%
Substation SCADA Integration Engineer	36.36%		16.67%	36.36%	35.71%
Exploitation Analysis	27.27%	10.00%	11.11%	36.36%	28.57%
Network Security Specialists	18.18%		5.56%	27.27%	21.43%
SCADA Protocol Engineer	18.18%		16.67%	27.27%	42.86%
Protection Emphasis Engineer	27.27%		16.67%	18.18%	28.57%

Job Roles	Phishing Incidents	Risk Management	Security Testing	Substation/ SCADA Attacks	Threat & Vulnerability Management
Information Security Analyst			5.56%		35.71%
Privacy Analyst	18.18%	40.00%	5.56%	18.18%	28.57%
All Source Intelligence	18.18%	20.00%	11.11%	27.27%	35.71%
Security Architect		10.00%	11.11%		7.14%
Risk/Vulnerability Analyst	18.18%	40.00%	16.67%	9.09%	35.71%
Legal Advice and Advocacy	9.09%	50.00%	16.67%	9.09%	28.57%
IT Auditor		30.00%			14.29%
Reverse Engineer	18.18%		11.11%	18.18%	21.43%
Operational Security Testing Professional	9.09%	20.00%	61.11%	9.09%	7.14%
Penetration Tester/Red Team Technician	9.09%	20.00%	61.11%	9.09%	7.14%
Utility Chief Operating Officer	9.09%	70.00%	5.56%	9.09%	7.14%
Enterprise Architect		10.00%	11.11%		21.43%
IT Development Supervisor		20.00%	16.67%		14.29%
Education and Training	27.27%	10.00%	5.56%	9.09%	14.29%
Data/Information Quality Analyst					7.14%
Smart Grid Operations Engineer			5.56%	18.18%	21.43%
Senior Software Security Analyst	9.09%		5.56%	9.09%	35.71%
Strategic Planning and Policy Development	9.09%	30.00%	5.56%	9.09%	7.14%
Provisioning Specialist					14.29%
Smart Grid Architect		10.00%	11.11%		14.29%
Integrative Security Assessment Researcher			5.56%		14.29%
Smart Grid Sr. Manager – Prof. Services					7.14%
Smart Grid Consultant					

Appendix M – Primary Goals

Goals
Maintain understanding of current attack tools, technologies, and techniques to compromise systems and intrude upon systems and networks.
Analyze log files for signs of an attack or compromise.
Successful deployment of new monitoring tool to scan smart grid deployment for intrusion attempt indicators. New tool is scanning and reporting, initial configuration stabilized and exceptions flagged for analysis. Simulated attack shows system highlighted the situation.
Investigate security events and analyze if they are incidents.
Analyze system logs for intrusions and security events.
Understand the security vulnerabilities of the smart grid components; meters, headend, etc.
Install security monitoring solutions.
Respond to security alerts generated by security systems.
Notify the appropriate parties to security incidents and actions taken or current situation and risk associated with intrusions, policy violations, unknown activity causing technical impacts, threats, alarms, or events that require deviation from normal operating protocols.
Contain known devices that are suspected to be compromised or to possess unauthorized executables and software.
Identify and classify technology to include hardware, software, systems, and data by their importance or overall risk to the organization (e.g. critical systems and data).
Maintain situational awareness of operating conditions for the business process or system (e.g. maintain level of awareness of the distribution system's status, outages, major evolutions, constraints, or current operating conditions).
Perform a penetration test of a system.
Identify the impact of security efforts to operational risk. Security efforts sometimes create operational risks; we need to understand what these impacts are so that we can approach the implementation of security efforts in a manner that minimizes operational impact.
Evaluate system aspects to arrive at a security posture.
Develop a sustainable cybersecurity program.
Maintain awareness of current cybersecurity threat and vulnerability environment.
Develop a cybersecurity awareness, training, and education program for the utility and its customers.
Implement specific security requirements within the operational system.
Evaluate alerts and advisories as applicable when released to determine overall risk/exposure and next steps.
Lead a cross-functional team incident response process.
Conduct routine assessments of networks and underlying infrastructure.
Determine system baseline configuration to meet security requirements.
Develop policy, standards and guidelines for others to follow.
Apply security policies to meet security objectives of the system.
Conduct pre-deployment cybersecurity testing on new equipment. Certify hardware and firmware versions for deployment, compatibility and interoperability.
Project management including the identification and prioritization of goals to balance business and security objectives.

Appendix N – Important Goals

Goal	Network Attacks	Substation & SCADA Attacks	AMI Attacks	Client-Side Attacks	Phishing Incidents	Network Separation and Attack Paths	Incident Response & Log Mgt	Encryption Attacks
Maintain understanding of current attack tools, technologies, and techniques to compromise systems and intrude upon systems and networks.	59%	55%	55%	55%	50%	59%	59%	55%
Analyze log files for signs of an attack or compromise.	60%	50%	50%	60%	30%	30%	70%	40%
Successful deployment of new monitoring tool to scan smart grid deployment for intrusion attempt indicators. New tool is scanning and reporting, initial configuration stabilized and exceptions flagged for analysis. Simulated attack shows system highlighted the situation.	60%	60%	60%	60%	20%	30%	70%	40%
Investigate security events and analyze if they are incidents	63%	58%	58%	58%	54%	33%	96%	58%
Analyze system logs for intrusions and security events.	50%	40%	50%	40%	20%	20%	100%	20%
Understand the security vulnerabilities of the smart grid security components; meters, headend, etc.	48%	48%	61%	43%	22%	48%	43%	48%
Install security monitoring solutions	48%	48%	48%	48%	35%	48%	78%	39%

Appendix O – PRISM Definition for Important Goals

Goal	Objective Measure	Premier	Robust	Improved	Satisfactory	Moot
Understand current attack tools, technologies, and techniques to compromise systems.	Percentage of employees and contractors passing the annual or semi-annual security quiz.	100% of employees and contractors attended and passed the quiz.	80% of employees and contractors attended and passed the quiz.	60% of employees and contractors attended and passed the quiz.	40% of employees and contractors attended and passed the quiz.	30% of employees and contractors attended and passed the quiz.
Analyze log files for signs of an attack or compromise.	Percentage of logs reviewed; time to review each source.	> 98% log coverage in less than 8 hours	> 90% log coverage within 24 hours	> 90% log coverage within 48 hours	> 80% log coverage within 48 hours	Less than 75% log coverage or greater than 72 hours
Apply new monitoring tools to scan smart grid system for security incident indicators.	Percent of smart grid system components being monitored. Percent of smart grid system baseline established. Event detection effectiveness.	Monitoring 100%; 100% of baseline configuration identified; simulated attack shows system affected; exceptions flagged for analysis.	Monitoring 75%; 75% of baseline configuration identified; simulated attack shows system affected; exceptions flagged for analysis.	Monitoring 50%; 50% of baseline configuration identified; simulated attack shows system affected; exceptions flagged for analysis.	Monitoring 50%; 25% of baseline configuration identified; simulated attack shows system affected; exceptions not yet identified.	Monitoring 50%; 0% of baseline configuration identified; simulated attack does not show system affected; exceptions not yet identified.
Evaluate security events and analyze if they are incidents	Number of events analyzed. Timeliness of analysis.	Security events (telemetry: syslog, snmp...) are automatically correlated with vulnerabilities and normal system activity to determine whether a security event is an Incident and automatically provide recommended mitigation.	Security events (telemetry: syslog, snmp...) are sent to a centralized log management system. Non-real-time scripts review old logs for events and send alerts/reports.	Security events (telemetry: syslog, snmp...) are sent to a centralized log management system. Log review is manual.	All security events are collected and forensically recorded.	Security events are not collected.

Goal	Objective Measure	Premier	Robust	Improved	Satisfactory	Moot
Analyze system logs for intrusions and security events.	Percentage of logs reviewed, time to review each log source.	> 98% log coverage in less than 8 hours	> 90% log coverage within 24 hours	> 90% log coverage within 48 hours	> 80% log coverage within 48 hours	Less than 75% log coverage or greater than 72 hours
Understand the security vulnerabilities of the smart grid components; meters, headend, etc.	Comprehensive list of security components (perhaps ordered by vulnerability) including specific risks to each; steps to mitigate these vulnerabilities or reduce risk	Gather a list of components involved; identify security mechanisms and audit mechanisms; carry out audit across system; collect data; collect mitigation steps.			Make a comprehensive list of all security components, with specific vulnerabilities of each highlighted.	
Install security monitoring solutions.	How much of the entire network is covered or how many devices out of all devices are being actively monitored.	If you are able to demonstrate that every cyber asset is being monitored by a security monitoring solution, then this is the premier state.	If you are able to demonstrate that 75% or more of every cyber asset is being monitored by a security monitoring solution, then this is the robust state.	If you are able to demonstrate that 50% – 75% or more of every cyber asset is being monitored by a security monitoring solution, then this is the improved state.	If you are able to demonstrate that 25% – 50% or more of every cyber asset is being monitored by a security monitoring solution, then this is the satisfactory state.	If you are able to demonstrate that less than 25% of every cyber asset is being monitored by a security monitoring solution, then this is the moot state.

o.

Appendix P – Distribution of Respondents

Age Group	Percentage of Respondents
21–30	9%
31–40	27%
41–50	28%
51–60	22%
Over 60	4%
Not reported	10%

Appendix Q – Size of Respondent Organization

Number of Employees	Percentage of Respondents
Less than 10	2%
10–99	11%
100–999	15%
1,000–4,999	16%
5,000–9,999	5%
10,000+	43%
Unreported	8%

Appendix R – Job Titles of Respondents

Respondents were asked to identify their job title (or titles) from a list of 19 titles, including an "Other" option. A total of 129 responses were received to this question with the distribution indicated below. Note that this question entitled the respondent to select multiple categories, thus the total will exceed 100%.

Job Title	Percentage of Respondents
Control systems engineer (CT01)	5.84%
Control systems operator (CT02)	0.73%
Control systems manager (CT03)	1.46%
Training specialist (CT04)	2.19%
IT Executive (CT18)	2.19%
IT manager (CT05)	4.38%
IT professional (CT06)	16.06%
IT systems administrator (CT07)	3.65%
Network engineer (CT08)	9.49%
Intrusion analysis staff (CT11)	5.84%
Intrusion analysis manager (CT12)	2.19%
Incident handling staff (CT13)	5.11%
Incident handling manager (CT14)	2.92%
Cybersecurity analyst (CT15)	28.47%
Cybersecurity operations staff (CT09)	10.22%
Cybersecurity operations manager (CT10)	5.11%
Cybersecurity manager (CT16)	10.95%
Cybersecurity executive (CT17)	6.57%
Other	20.44%

Appendix S – Levels of Experience

How would you classify your level of expertise in the cybersecurity field?	Percentage
Novice: minimal knowledge, no connection to practice (LE1)	2.92%
Beginner, working knowledge of key aspects of practice (LE2)	14.60%
Competent: good working and background knowledge of the area (LE3)	24.09%
Proficient: depth of understanding of discipline and area of practice (LE4)	24.82%
Expert: authoritative knowledge of discipline and deep tacit understanding across area of practice (LE5)	23.36%
No answer	10.22%
What level of familiarity do you have with smart grid operations?	Percentage
Novice: minimal knowledge, no connection to practice (LE1)	19.71%
Beginner, working knowledge of key aspects of practice (LE2)	26.28%
Proficient: good working and background knowledge of the area (LE3)	26.28%
Competent: depth of understanding of discipline and area of practice (LE4)	10.22%
Expert: authoritative knowledge of discipline and deep tacit understanding across area of practice (LE5)	8.03%
No answer	9.49%

Appendix T – Preliminary Fundamental Tasks

Task	Task Description
9103	Analyze available logs and note gaps and time periods.
9111	Verify that all systems are logging to a central location.
9116	Understand incident response process and initiate incident handling according to documented policies and procedures.
9117	Identify and filter out false positives; if determined to be an incident, assign to incident handler.
9137	Analyze individual threat activity by correlating with other sources to identify trends.
9149	Implement intrusion prevention/detection solution.
9150	Understand the selected Security Event and Information Management tool.
9183	Understand the company's incident response process and procedures.
9191	Understand incident response, notification, and log handling requirements of business.
9200	Identify repeat incidents involving the same person or persons, systems, or adversaries.
9201	Prioritize systems within your network to determine which ones are of the High, Moderate, or Low impact value.
9244	Report vulnerabilities to staff and stakeholders.
9254	Configure vulnerability scanners to operate safely and effectively in the targeted environment.
9259	Assess whether network scan results are real or false positives.
9262	Review vulnerability scan results.
9263	Test all vulnerability scanners for modes or configurations that would be disruptive to the communication paths and networks being tested and host communication processing looking for possible conflicts that may result in negative operational impacts.
9265	Analyze vulnerability reports.
9268	Coordinate assessment of any target systems with System Owners ahead of time.
9270	Develop a scanning plan and make sure all network operations staff and key stakeholders are consulted and notified about the timing of test initiation.
9276	Review assessment results in accordance with defined risk categorization model.
9295	Communicate timing and schedule of scans.
9298	Coordinate efforts with the vendor to develop an understanding of the component and security implications.
9304	Understand how phishing attacks can adversely impact web-based management applications.
9314	Alert end-users of potential risks and vulnerabilities that they may be able to mitigate.
9318	Understand environment (culture, staff) to create a better relationship for transmitting delicate and sometimes poorly understood information.
9319	Monitor industry groups and forums to stay up to date on the latest security vulnerabilities related to smart grid components.
9331	Identify threat actors.
9342	Identify sources of targets to scan.
9361	Review log files for signs of intrusions and security events.
9363	Develop and/or procure a data logging and storage architecture that scales and is fast enough to be useful for analysis.

Task	Task Description
9399	Coordinate with other departments to make sure that routine business operations are not affected during testing.
9406	Identify all systems that may be affected by testing.
9430	Verify all devices are being submitted to Security Information and Event Management for full network visibility.
9538	Communicate changes to user security tools and information regarding identified events and incidents.
9544	Monitor for new systems installed on the network.
9556	Communicate with the vendor to make sure you are registered to receive updates.
9572	Implement solution to identify new devices connecting to the network(s).
9575	Understand the data classification strategies that are in place.
9595	Maintain a prioritized list of critical resources.
9597	Maintain or be able to access a list of assigned system owners.
9604	Maintain incident data repository and analyze data and metrics regarding types of incidents, frequency, and systems impacted.
9606	Review past incidents to determine whether host security solutions and logs are providing data that can identify an event.
9610	Report the attack Tactics, Techniques, and Procedures (used in the last 6 months against the organization).
9611	Review tool configurations and target configurations to reduce false positives based on historic information.
9619	Develop a periodic verification process to make sure that the assets are logging in alignment with the intended operational architecture.
9628	Scan all affected systems to make sure the patch or mitigations are present and the risk associated with the vulnerability has been reduced as expected.
9629	Test all identified mitigations or patches to make sure they remove or mitigate the vulnerability as expected with no negative impacts.
9632	Identify security incidents that require training or awareness for users and security staff.
9633	Develop mitigations based on incidents analyzed and recommend improvements in security capabilities or tools as appropriate.
9640	Analyze the intrusion by looking for the initial activity and all follow-on actions of the attacker.
9641	Collect images of affected system for further analysis before returning the system to an acceptable operational state.
9674	Document all actions taken to contain systems.
9690	Assess what configuration settings result in capturing the required information for monitoring.
9701	Monitor all systems that were suspected or confirmed as being compromised during an intrusion/incident.
9703	Review running processes to determine whether incident response successfully removed malware.
9708	Develop and publicize ways to distinguish between routine system errors and malicious activities.
9709	Protect classified or proprietary information related to the event, but release general incident information to stakeholders.
9710	Review incident response actions to make sure actions were taken properly.
9711	Monitor systems that were affected and the entire sub-network for activity associated with the attack.

Task	Task Description
9717	Monitor security news and intelligence sources to include vendor web pages for vulnerability disclosures, incident announcements, and knowledge briefs.
9718	Communicate with vendors about a vulnerability or incident in order to understand risk and devise a mitigation strategy.
9720	Decide what mitigations should be implemented on remote connections.
9722	Understand company policies and procedures for downloading and installing third-party software.
9725	Access company policies to verify that the software being downloaded is allowed.
9729	Scan systems in an attempt to detect the use of unacceptable software.
9750	Define reports on the current patch and update status of all security tools and identify any variances against vendor releases.
9751	Establish a systems and tools patching program and schedule.
9755	Document current patch levels and updates before use in critical situations.
9781	Sign up for vendor notifications and alerts
9785	Maintain a current list of stakeholders' contact information and link this information to notification requirements.
9791	Monitor for unauthorized access to tools and data.
9802	Define security events and incidents with evaluation criteria.
9807	Develop Security Event and Information Management rule sets to detect documented event classes for each monitored system.
9808	Communicate warning signs of security events to internal stakeholders.
9809	Collect observed attacker Tactics, Techniques, and Procedures from available sources to include Information Sharing and Awareness Councils, peer utilities, government sources.
9819	Analyze the security incident and identify defining attributes.
9831	Escalate findings to appropriate personnel to review event and accuracy of false-positive findings.
9849	Report the time of discovery for all reportable events and incidents and the time of notification.
9850	Verify that all reported events and incidents were handled in compliance with the reporting requirements.
9859	Understand desired outcome as well as purpose of assessment so that the solution can be configured appropriately.
9860	Test the vulnerability assessment solution in a development environment to see whether desired results are achieved.
9861	Implement monitoring system that meets design criteria.
9878	Minimize spread of the incident by making sure contaminated systems cannot communicate to systems outside of the network boundary.

Appendix U – Preliminary Differentiating Tasks

Task	Task Description
9129	Review known intrusion Tactics, Techniques, and Procedures and observables to assist in profiling log events and capture event information that may relate to known signatures.
9192	Understand the basic components of an incident response process (Prepare, Identify, Contain, Eradicate, Recover, Lessons Learned).
9267	Develop a prioritized list of critical resources.
9338	Understand NERC CIP and audit requirements.
9348	Understand how to run wireshark and tcpdump.
9414	Review all internal incidents for the purposes of staying current in threats and how to stay up to date on current threats and determine the best way to analyze them.
9491	Monitor vulnerability reports.
9527	Update database of device configurations upon changes to configurations.
9577	Understand data classification levels and how to identify such levels with assets.
9605	Review incidents over time to determine lessons learned or how to better align security tools.
9625	Assess the risk ratings of the vulnerability based on the technical information, how the technology is deployed and the importance of the systems.
9627	Implement vulnerability mitigations in accordance with the plan to include patches or additional security controls.
9634	Define how systems were initially compromised, how the attack progressed and what observables were available for detection and response.
9649	Monitor security tool providers for updates and patches for tools that are in use.
9712	Report closing of the incident and all incident response processes that were followed.
9719	Monitor all logs associated with third party accessing your systems; this may require a manual review against historic use profiles.
9749	Maintain a list of approved security tools and their approved patch levels.
9783	Maintain knowledge of reporting requirements associated with systems.
9857	Develop a standardized process to make sure appropriate steps are taken during and after an event occurs.
9877	Minimize spread of the incident by making sure contaminated systems are monitored.

Appendix V – Glossary of Terms

A

Ability

Ability is the application of skills to new domains. Thus ability is measured by the degree of skill transfer, from narrow to broad.

Accreditation

Recognition of an organization that has met a standard of performance

Achievement Assessment

Achievement assessments are used to assess knowledge acquisition.

Achievement Test

Achievement tests measure the proficiency of recall of past knowledge. These tests are descriptive, and a score is determined based on a candidate's depth of understanding of a domain (whether that domain is broad or narrow). These tests can prove valuable in a college classroom, for example, where a professor is attempting to gauge mastery of a certain specific subject matter or where a trainer wants to validate that her students are grasping the content of a lecture-heavy course. These instruments measure the "observed" score on a test: a candidate might be expected to significantly improve their score by studying harder before a retest.

ADAPTS

Advanced Defender Aptitude and Performance Testing and Simulation Program
Through its Advanced Defender Aptitude and Performance Testing and Simulation Program, the NBISE is working to bring the collective resources of a wide range of academic institutions, from leading universities to community colleges and institutes, to bear on the U.S.'s growing cybersecurity workforce crisis. Innovative and groundbreaking, the ADAPTS program is focused on developing, evaluating, and validating state-of-the-art assessment instruments, curriculum components proven to accelerate students' skills acquisition, and hands-on simulation practice ranges to help students and professionals hone their skills for a range of cybersecurity professions.

The ADAPTS virtual laboratory will also support the continuing development of cybersecurity science by providing researchers a real-time and real-world data collection opportunity to work with both students and practitioners as they demonstrate and hone their skills against a growing library of current threats, vulnerabilities, and system failures available through the ADAPTS "practice range."

ADAPTS Libraries

The ADAPTS libraries are maintained by NBISE as part of its mission to serve the public interest through development of Job Performance Models and associated assessment and development techniques to facilitate the development and measurement of cybersecurity skills.

Advanced Threat Response Panel

The Advanced Threat Response Panel is focused on advanced cybersecurity threats such as advanced persistent threats and other highly sophisticated threat vectors.

Aptitude Test

Aptitude tests are assessment instruments designed to measure the future potential of a candidate to perform in a specific role. These tests are considered predictive – forecasting how the tested individual can be expected to perform in the future. These tests use adaptive testing techniques and statistical analyses to measure a candidate's "true" score on a test: studying is generally not expected to significantly alter a candidate's score during a retest.

B

Behavioral Consistency

Given the same set of conditions defining the environment of performance, behavioral response will be repeated within a very limited range of variability across numerous trials.

C

Causal Model of Job Performance

A set of factors and relationships among factors which explain and predict individual or group performance differences in a job.

Certificate (examination)

Training that has an examination at the end to determine whether the learning outcomes have been achieved.

Certification

A third-party assessment of validated knowledge and skills, reassessed at defined intervals, has due processes to take away the certification, and is "firewalled" away from training.

Construct

"any variable (i.e., entity capable of assuming two or more values) of a mental or conceptual nature." From Schwab, DP (1980). Construct validity in organizational behavior. *Research in Organizational Behavior, 2*, p. 5.

Construct Validity

"representing the correspondence between a construct (conceptual definition of a variable) and the operational procedure to measure or manipulate that construct. From this definition it is acceptable to

think of construct validity as representing the correlation coefficient between the construct and the measure."
From Schwab (1980), p. 6.

Content Validity

"prototypical characteristics of the target persons, settings, treatments, and outcomes that study operations are thought to reflect."
From Shadish WR, TD Cook, and DT Campbell. 2002. *Experimental and quasi-experimental designs for generalized causal inference*. Boston, MA: Houghton Mifflin.

Critical-Differentiation Analysis

A statistical analysis of task statement ratings to determine the degree of criticality for job performance and the degree to which the task differentiates in the method or outcome by which the task is performed by persons of varying levels of expertise.

Critical-Differentiation Matrix

A technique for identifying influential task performance, the Critical-Differentiation Matrix identifies the fundamental and differentiating tasks that should best predict job performance.

Critical Incident

Any event or situation that threatens individual or organizational harm. An incident being a specific event identified with a description of who, what, when, where, how and why a person, organization, or system is impacted by the event.

Critical-Incident Analysis

Intensive, in-depth interviews with subject matter experts to solicit critical incidents and documenting what the experts were thinking, feeling, and doing during the incident. A critical incident is a characteristic and challenging event that embodies the most important aspects of the job.

Criticality

The product of arithmetic means of frequency and importance across all levels of expertise.

Cyber Learning Diversity

Despite their broad distribution and use, electronic learning management systems for cybersecurity have yet to undergo rigorous testing to determine how they impact learning patterns, skill profiles, practice routines, and use by students of diverse gender, ethnicity, or socioeconomic status. The large and rapidly growing demand for cybersecurity talent requires that underrepresented groups be encouraged and supported in joining the workforce.

D

Differentiation

The slope of criticality scores, signifying the frequency that a person with a given skill level must be involved, and the importance of that task for determining the performer's skill level.

Differentiating Tasks

Those tasks that exhibit both high criticality and high differentiation scores.

F

Face Validity

Constructs in a model appear to reflect the phenomena they intend to measure.

Functional Area Definition

Functional Area Definition is a scoping statement used for Job Performance Panels.

Fundamental Tasks

Those tasks that are rated as highly critical but show little differentiation across different levels of expertise. Performance on these tasks is essential and should be considered minimal entrance requirements for the field.

G

Goal

A statement that expresses an action that must be successfully completed to accomplish the job mission, or to facilitate the accomplishment of another goal.

Goal Objective

The measurable outcome that establishes the criteria by which the degree of success or effectiveness may be assessed.

Ground Truth

Current vulnerabilities or techniques being exploited or used by adversaries in attacking a system.

Ground Truth Expertise Development

A model for accelerating expertise development.

I

Item Difficulty Index

The percentage of students who answered the item correctly.

Item Discrimination Index

Distinguishes for each item between the performance of students who did well on the exam and students who did poorly.

J

Job Audit (or Analysis) Questionnaire

The Job Analysis Questionnaire is a set of surveys forming the primary data collection method for developing a theoretical model of job performance.

Job Performance Lab

A laboratory facility for administering aptitude, achievement, and performance tests and validating Job Performance Models or the associated assessment instruments.

Job Performance Model

A Job Performance Model is a list of competencies, often organized into five or more groupings or clusters, attributable to satisfactory or exceptional employee performance for a specific job role. Competency models are used throughout various professions to define success in a given job role, allowing for the development of tailored training and development programs, assessment and examination instruments, and other job aids. Competency models are developed by working with a group of experts to identify the tasks that they complete as part of their jobs. This list is then distributed to a broader audience of experts who rate the tasks for their importance and the frequency with which they are conducted. This data is augmented by "critical-incident analysis"—intensive, in-depth interviews with subject matter experts to solicit critical incidents and documenting what the experts were thinking, feeling, and doing during the incident. A critical incident is a characteristic and challenging event that embodies the most important aspects of the job.

Job Performance Model Driven Workforce Development

Panels contribute to identifying the job tasks, goals, and levels of satisfactory performance in a given job, as well as the methods and tools professionals should be familiar with. These are built into a survey, which is more broadly disseminated within the community and seeks to gauge both the relative importance of given tasks and the frequency with which they are conducted. In parallel with survey data analysis, NBISE staff and researchers work with experts to augment the growing competency model report with critical-incident analyses—intensive, in-depth interviews geared toward documenting characteristic and challenging events that embody the most important aspects of the job. Further work is done with these "critical incidents" and "situational judgment scenarios" to determine how the actions taken by a novice, apprentice, journeyman, and expert-level practitioner are differentiated.

Once the competency model process is complete, this model is used to develop assessment instrument items (e.g., questions) and packaged components (e.g., tests), curriculum components (e.g., e-learning or

in-class course segments), and simulation exercises (e.g., hands-on, Virtual Machines based practice ranges). Once developed, these items are distributed into the classroom through NBISE's ADAPTS Research Network. Items are piloted, evaluated, and improved. Data is then provided back to NBISE to accelerate the validation process.

Job Performance Panel

A panel of experts and practitioners in a specific field of the cybersecurity workforce, established to consult on and contribute to the development of a Job Performance Model.

NBISE panels play a crucial role in defining the current and future cybersecurity workforce needs of industry and government. Once a role or job has been identified by the National Board as critical to a cybersecurity team, a panel of experts and practitioners in that field is established to consult on:

- What does a successful professional in this role need to know and do?
- What methods and tools must she be familiar with?
- What defines successful performance?
- How should the job be segmented into specialties & tasks?
- What differentiates an expert from a novice?
- Identifying and developing scenarios for critical-incident analysis and assessment instruments
- Providing review and consulting on resulting course/test/simulation/performance support components (curriculum tools).

Input from the panel is used to create a comprehensive competency and measurement model for the role and to identify "ground truths" and real-world scenarios experienced by practitioners on the front lines. Once these tasks are complete, the panel provides additional guidance on the development of skill and performance-based assessments for individuals in the field and provides ongoing direction and insight to NBISE's ADAPTS cybersecurity workforce development network: university and institutional researchers, collegiate educators, K-12 teachers, and corporate trainers.

Job Performance Panel Advisory Group

National Board advisors are people who hire, contract, and apply cybersecurity talent to manage risk to a system or organization. They advise the National Board in the commissioning process of a Job Performance Panel, through the nomination process and charter development, and serve as a resource for panel work product feedback. Advisors engage with NBISE staff for a total time commitment of four hours over a two-week period during the panel's startup phase and will be called upon to conduct short reviews of work product over the course of the panel's work plan.

National Board advisors are responsible for applying cybersecurity teams in the defined scope of the specific Job Performance Panel they advise on. An advisor should be knowledgeable of key talent in the community performing in the identified job roles and have a strong understanding of the goals associated with job performance for those roles.

Job Performance Panel Chair

The subject matter expert co-leader of a Job Performance Panel.

Job Performance Panel Member

A participant in a Job Performance Model Panel.

Job Performance Panel Vice Chair

The subject matter expert co-leader of a Job Performance Panel.

Job Responsibilities

Defined as action statements which result in outcome states that may be monitored or assessed to determine whether an objective has been accomplished. Accordingly, responsibility statements use passive verbs, such as "ensure," "follow," or "obtain" that are not included in Bloom's taxonomy.

K

Knowledge

Knowledge is the understanding of a concept, strategy, or procedure. Thus, knowledge is measured by depth of understanding, from shallow to deep.

Knowledge, Skills, Abilities

Knowledge, skills, and abilities necessary to successfully perform the responsibilities of a job role.

Knowledge, Skills, Abilities and Other

Knowledge, skills, abilities, and other work-related characteristics including attitudes and motivation.

L

Levels of Competencies

Competencies defined at novice, apprentice, journeyman, and expert levels for multiple roles (organizational language).

Licensure

A legal credentialing process administered by the federal or state government based on some type of examination process or recognition of a national certification.

Literature Review

The process of identifying and reviewing literature pertaining to the focus of a Job Performance Panel. The review is primarily two things: 1) job descriptions and/or evaluations for personnel in the private and public sector performing relevant job roles; 2) articles or descriptions of methodologies or recommended

procedures, vulnerabilities, errors and omissions, and incidents involving cybersecurity practices affecting the Job Performance Panel's focus area.

M

Master Vignettes

A collection of vignettes which experts frequently label using terse phrases such as a "Network Attack" or a "Data Leakage."

Metrics of Cybersecurity Skill Assessment and Development

The high-level metrics include:
1. Job Performance Model development (Are we measuring the right things?)
2. Assessment instrument development and validation (Are we measuring the right way?)
3. Aptitude vs. achievement testing (Are our measures meaningful?)

N

National Board

The National Board provides national leadership to industry, government, and academia on cybersecurity workforce development. Comprising executive-level leaders and expert practitioners, academics, and policy makers, the National Board advises on NBISE strategy and priorities, oversees the work of NBISE panels, and specifically consults on:

- What roles within an information security team are most needed?
- What are the major trends affecting the cybersecurity workforce?
- What guidelines of performance should be established and maintained for cybersecurity knowledge, skills, and abilities?
- What guidelines for learning should be established and maintained for cybersecurity education and training?
- What guidelines in simulation of cybersecurity environments should be established and maintained to provide appropriate practice ranges for converting knowledge into skill?
- What guidelines for assessment should be followed by student and professional development, selection and certification organizations?
- What guidelines of research should be established and maintained to further advance the science of information assurance and cybersecurity?

In its leadership capacity, the National Board provides crucial guidance to the academic sector in targeting programs of research and curriculum development to the areas of greatest need.

National Board of Information Security Examiners (NBISE) Community

These groups work collaboratively to support NBISE programs. NBISE's work involves identifying the critical job roles that make up the cybersecurity workforce of today and tomorrow, defining competency models for those roles, and developing a standards-based library of validated assessment, curriculum, and simulation-based learning components.

NBISE Programs

NBISE is instituting programs designed to bring all players to the table to create a virtuous circle of information exchange, collaborative research, and the creation of state-of-the-art assessment, curriculum, and simulation instruments capable of predicting on-the-job performance. NBISE's work involves identifying the critical job roles that make up the cybersecurity workforce of today and tomorrow, defining competency models for those roles, and developing a standards-based library of validated assessment, curriculum, and simulation-based learning components.

O

Operational Security Testing

The Operational Security Testing Panel is focused on penetration testing, red teaming, and attacker emulation testing.

P

Performance-Based Assessment

Performance-based assessments are used to assess efficacy in both skillful application of knowledge (i.e., practical test) and the ability to adapt to real-time, dynamic alteration of the threat landscape that occurs during the active defense of an information system (i.e., interactive challenge event).

Performance Profile

Provided to an individual assessment/test taker to aid in self-assessment. The use of a visual indication of performance bands reflecting the precision of measurement (narrow bands indicate greater precision).

Personal Development Plan

By identifying the timing of cognitive change through formative assessments, the psychometrics of learning may enable personalized selection of interventions best suited to expand the depth of knowledge, increase the consistency of skilled performance, and improve the ability to transfer skills into new domains.

Potential Performance Analysis

The meaning of skill and its effect on future performance.

Predictive Validity

The ability of a test or measure to predict the results of an analysis of the same data made with another test instrument or measurement tool.

PRISM

A method for eliciting goals and objectives (Tobey 2007)

R

Registration

Listing in a registry based on the "Qualifications" of an individual (e.g., education, experience).

Reliability Index

Degree to which a measurement instrument produces the same results under repeat administrations.

S

Scenario

One of several possible event sequences for how a vignette may play out.

Simulation Research

Intended to advance understanding of how situated, immersive, and low- and high-fidelity simulations may impact learning curves in volatile, uncertain, complex and ambiguous environments. Low-fidelity simulations depict hypothetical job environments within a training session, such as in virtual reality games. High-fidelity simulations involve performing work under conditions very similar to the workplace, such as during interactive challenge events involving active defense of an information system.

Situational Judgment Test

A type of psychological test which presents the test taker with realistic, hypothetical scenarios and asks the individual to identify an appropriate response.

Skill

Skill is the reliable application of knowledge to achieve desired outcomes. Thus, skill is measured by the degree of reliability, from inconsistent to consistent.

Skill Assessment Instrument

A validated assessment methodology capable of determining the depth of understanding and *when* knowledge has become "conditionalized" through situated enactment into fluent and adaptive performance. By identifying the timing of cognitive change, the psychometrics of learning may enable

personalized selection of interventions best suited to expand the depth of knowledge, increase the consistency of skilled performance, and improve the ability to transfer skills into new domains. NBISE will use recent advances in cognitive science that provide methods for identifying when knowledge is converted into skill. Using these techniques we can assess the shape and timing of learning curves as strategy (knowledge) and skill (consistency at applying knowledge) are developed.

Smart Grid Cybersecurity Panel

The Smart Grid Cyber Security Panel is formed in conjunction with the U.S. Department of Energy and Pacific Northwest National Laboratory. The Panel is focused on securing all elements of the smart grid from a utility perspective, from meter data to operational systems. The functional job area named Smart Grid Cybersecurity Specialist is a person charged with cybersecurity operations and management in a smart grid environment. Their jobs include the security functions for day-to-day operations, but not engineering the architecture. The protection of the smart grid network and core SCADA control systems requires a very challenging blend of control engineering and security, which can best be executed by security engineers who have a very special mix of abilities, acquired skills, and learned knowledge.

T

Tasks

In a review of task analysis methods, the word "task" is defined as "what a person is required to do, in terms of actions and/or cognitive processes, to achieve a system goal." (Schraagen 2006, p. 185) This definition implies several important constructs which need to be elicited from subject matter experts to fully understand the factors impacting performance on the job.

TestLet

A module of an assessment system containing items that pertain to a specific learning objective for demonstrating knowledge, skill or ability in one of factors identified in a Job Performance Model.

ThinkLet

The smallest unit of intellectual capital required to create one repeatable, predictable pattern of thinking or behavior by an individual or group working toward a goal.

V

Vignettes

A vignette is the label (terse description) given to various scenarios, which contain various critical incidents.

VUCA

An acronym used to describe the volatility, uncertainty, complexity, and ambiguity contained in specific problem, event, or environment.

Appendix W – Acronym Descriptions

Advanced Threat Response Panel
The Advanced Threat Response Panel is focused on advanced cybersecurity threats such as advanced persistent threats and other highly sophisticated threat vectors.

Critical-Differentiation Matrix
A technique for identifying influential task performance, the Critical-Differentiation Matrix identifies the fundamental and differentiating tasks that should best predict job performance.

Critical-Incident Analysis
Intensive, in-depth interviews with subject matter experts to solicit critical incidents and documenting what the experts were thinking, feeling, and doing during the incident. A critical incident is a characteristic and challenging event that embodies the most important aspects of the job.

Functional Area Definition
A Functional Area Definition is a scoping statement used for Job Performance Panels

General Work Activities
Categorization of activities used during elicitation in the O*NET method for job task analysis.

Group Decision Support Systems
Computer software that facilitates collaborative decision analysis.

Ground Truth Expertise Development
A model for accelerating expertise development based on aligning assessment and learning systems with a job performance model.

Industrial Control Systems Joint Working Group
A group of organizations interested in industrial control systems technology.

Knowledge Exchange
A cloud computing tool for exchange of ideas among a group of individuals sharing interest in a topic.

National Board of Information Security Examiners
A Maryland not-for-profit corporation formed to leverage the latest advances in assessment and learning science toward the solution of one of the United States' most critical workforce shortages: cybersecurity professionals. Through its Advanced Defender Aptitude and Performance Testing and Simulation (ADAPTS) program, NBISE coordinates the work of teams of practitioners, researchers, and educators who develop and validate or enhance existing performance-based learning and assessment vehicles to materially accelerate the acquisition of hands-on skill and tacit knowledge by students and practitioners in collegiate and continuing education programs. NBISE's work and research seeks to develop assessment instruments to reliably predict future performance and aptitude for cybersecurity jobs, allowing for a better understanding of the efficacy of performance-based learning platforms.

National Cyber Security Division
A division of the U.S. Department of Homeland Security that seeks to protect the critical cyber infrastructure by coordinating the cyber leadership, processes, and protocols that will determine when and what action(s) need to be taken as cyber incidents arise.

National Initiative for Cybersecurity Education
(Source: http://csrc.nist.gov/nice/aboutUs.htm)
National Initiative for Cybersecurity Education (NICE) evolved from the Comprehensive National Cybersecurity Initiative, and extends its scope beyond the federal workplace to include civilians and students in kindergarten through post-graduate school. The goal of NICE is to establish an operational, sustainable and continually improving cybersecurity education program for the nation to use sound cyber practices that will enhance the nation's security.

The National Institute of Standards and Technology (NIST) is leading the NICE initiative, comprising more than 20 federal departments and agencies, to assure coordination, cooperation, focus, public engagement, technology transfer and sustainability. Many NICE activities are already underway and NIST will highlight these activities, engage various stakeholder groups and create forums for sharing information and leveraging best practices. NIST will also be looking for "gaps" in the initiative—areas of the overarching mission that are not addressed by ongoing activities.

National Institute of Standards and Technology
(Source: http://www.nist.gov/public_affairs/nandyou.cfm)
Founded in 1901 and now part of the U.S. Department of Commerce, NIST is one of the nation's oldest physical science laboratories. Congress established the agency to remove a major handicap to U.S. industrial competitiveness at the time—a second-rate measurement infrastructure that lagged behind the capabilities of England, Germany, and other economic rivals. Today, NIST measurements support the smallest of technologies—nanoscale devices so tiny that tens of thousands can fit on the end of a single human hair—to the largest and most complex of human-made creations, from earthquake-resistant skyscrapers to wide-body jetliners to global communication networks.

Operational Security Testing Panel
A Job Performance Model Panel under NBISE focused on penetration testing and red teaming.

Pacific Northwest National Laboratory
(Source: http://www.pnnl.gov/about/)
Pacific Northwest National Laboratory is one among ten U.S. Department of Energy national laboratories managed by U.S. Department of Energy's Office of Science.

Potential Performance Analysis
Calculation of an individual's aptitude and achievement in developing knowledge, skill, and ability in performing a set of tasks contained within a TestLet.

Processing, Personality, Interests, and Knowledge
A model of motivation developed by John W. Atkinson.

Smart Grid Cybersecurity Panel
A Job Performance Model Panel under NBISE focused on smart grid cybersecurity.

Subject Matter Expert
A domain expert. Someone who has demonstrated significant expertise in a particular area or topic.

Volatility, Uncertainty, Complexity and Ambiguity
The volatility, uncertainty, complexity, and ambiguity contained in specific problem, event, or environment.

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.pnl.gov