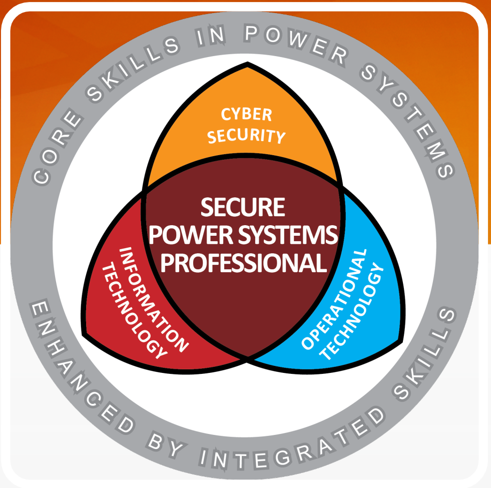
PNNL-24140

Pacific Northwest
NATIONAL LABORATORY

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


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

SPSP Phase III Recruiting, Selecting, and Developing Secure Power Systems Professionals: Behavioral Interview Guidelines by Job Roles

March 2015

LR O'Neil
TJ Conway
DH Tobey

FL Greitzer
AC Dalton
PK Pusey

U.S. DEPARTMENT OF
ENERGY

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

DISCLAIMER

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

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

Printed in the United States of America

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

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

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

PNNL-24140

SPSP Phase III Recruiting, Selecting, and Developing Secure Power Systems Professionals: Behavioral Interview Guidelines by Job Roles

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

March 2015

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

Pacific Northwest National Laboratory
Richland, Washington 99352

Summary

The rapidly approach retirement of significant numbers of power system experts and a continuing trend of increasing complexity in modern power systems prompted the U.S. Department of Energy (DOE) to establish the three-phase Secure Power Systems Professional (SPSP) project. The project developed resources for job definition and competency analysis along with tools to guide assessment and curriculum design and to help identify and develop required knowledge, skills, and abilities in technical and operational cybersecurity for power systems.

A major accomplishment during Phase III of the project was the development of psychometrically validated job profiles for four identified SPSP job roles: the secure power systems engineer, incident responder, intrusion analyst, and security operator. The job profiles were produced by integrating the results of Phases I and II to capture the relevant job requirements that would be necessary to accurately predict job performance. They can be immediately applied by human resources professionals, recruiters, and hiring managers to assist in the recruitment, selection, and training of SPSPs, as well as to identify needed skills to train existing employees to meet the new requirements of SPSPs.

The complete list of knowledge, skills, and abilities required in each of the studied job roles was assembled into the Behavioral Interview Guidelines. The guidelines were developed to apply the results of Phases I and II in a format that can be used in part or in whole to align workforce capabilities with the strategic goals and tactical focus of a power grid organization. These guidelines may 1) be applied to develop performance reviews or to produce individual professional development programs for existing staff; 2) assist in specifying learning objectives for a training or education program; and 3) be easily incorporated into most human capital software to facilitate development of job descriptions that comply with guidelines established by the Society of Human Resource Management. The guidelines can be immediately applied by human resources professionals, recruiters, and hiring managers to assist in recruiting and interviewing candidates for new SPSP position openings.

The Behavioral Interview Guidelines were excerpted from the original final SPSP project report (*Secure Power Systems Professional Phase III Final Report: Recruiting, Selecting and Developing Secure Power Systems Professionals*), and are presented in this report for standalone reference and application by users in the field.

Acronyms and Abbreviations

AMI	advanced metering infrastructure
CIP	critical infrastructure protection
DHS	U.S. Department of Homeland Security
DOE	U.S. Department of Energy
IDS	intrusion detection system
IPS	intrusion prevention system
IR	incident response
NERC	North American Electric Reliability Corporation
SIEM	Security Information and Event Management
SPSP	Secure Power Systems Professional

Contents

1.0 Introduction

For the convenience of the user, the contents of this report were excerpted from Appendix E of *Secure Power Systems Professional Phase III Final Report: Recruiting, Selecting and Developing Secure Power Systems Professionals* (O'Neill et al. 2014), which reviews the findings of the three-year Secure Power Systems Professional (SPSP) project for the Office of Electricity Delivery and Energy Reliability (OE) at the U.S. Department of Energy (DOE).

1.1 Background

The SPSP project was developed to address the growing national deficit of electric power industry workers that have sufficient cybersecurity expertise and skills to effectively respond to the growing threat posed by cybersecurity vulnerabilities in critical infrastructure. With significant numbers of power system experts retiring and a continuing trend of increasing complexity in modern power systems, there is a great need throughout the power industry for cybersecurity awareness and competence in tasks that previously had no cyber components. DOE responded to this call for action to secure and protect critical infrastructure by establishing the three-phase SPSP project. The project applied a holistic approach to workforce development that continuously adapts to the latest tactics, techniques, and tools, bringing together world-class security, risk, and critical infrastructure domain experts so that current industry best practices can be rapidly documented, replicated, and enhanced to determine SPSP competencies.

The Phase I effort identified the critical, fundamental, and differentiating job responsibilities and competencies of four essential job roles: secure power systems operator, secure power systems intrusion analyst, secure power systems incident responder, and secure power systems engineer. In Phase II, the competencies identified in Phase I were analyzed against current workforce development frameworks, certifications, and education programs, yielding a greater understanding of how certifications, frameworks, and training/education program topics align with the job responsibilities. Phase III established the framework for developing important tool sets and capabilities, including job profiles for selecting candidates most suited for specific SPSP roles (O'Neil et al. 2015). Candidate selection remains a challenge for electric power entities because most of these entities lack an adequate candidate selection tool that can map behavioral interview questions to the identified SPSP roles. All three phases of the SPSP project have provided much-needed strategic findings to aid entities in addressing workforce issues; in addition, each phase has provided immediate tactical tools, data, and approaches to help solve the problems of today. In particular, Phase III helps address the industry's SPSP workforce development needs by providing the foundation for the industry to begin strategic work on selecting the most qualified individual for a specific SPSP role, as well as providing a tactical resource to help identify and train the SPSP employees that the industry needs now.

1.2 Report Contents

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

2.0 Behavioral Interview Guidelines

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

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

Phase I of this project produced the required job task analysis. The result was a predictive model of job performance that identified the major responsibilities reported in Appendix D of the SPSP Phase III Final Report (O’Neil et al. 2014) and in the related standalone report (O’Neil et al. 2015b). The complete list of knowledge, skills and abilities required in each of the studied job roles was assembled into the Behavioral Interview Guidelines reported below.

Promoting Defensibility of Fair Hiring Practices

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

- Recruitment and Career Development guides (see Appendix C in O’Neil et al. 2014)
- Job profiles (Appendix D in O’Neil et al. 2014, or O’Neil et al. 2015b)
- Behavioral interview guidelines (this report)
- Individual and team performance guidelines (see Appendix F in O’Neil et al. 2014, or O’Neil et al. 2015a).

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

How to Use This Guide

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

3.0 Secure Power Systems Engineer

4.0 Secure Power Systems Intrusion Analyst

5.0 Secure Power Systems Incident Responder

6.0 Secure Power Systems Security Operator.

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

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

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

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

3.0 Behavioral Interview Guideline Items: Secure Power Systems Engineer

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

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

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

4.0 Behavioral Interview Guideline Items: Secure Power Systems Intrusion Analyst

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

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

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

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

5.0 Behavioral Interview Guideline Items: Secure Power Systems Incident Responder

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

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

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

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

6.0 Behavioral Interview Guideline Items: Secure Power Security Operator

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

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

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

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

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

X	**Ability** ***The application of skills to new domains; ability is measured by the extent of skill transfer, from narrow to broad.***
	vulnerabilities related to power systems security components.
	Monitor vendor notifications for updates to software and signatures and compare against deployed versions.
	Monitor vulnerability reports.
	Prioritize alerting after analysis into predefined buckets.

7.0 References

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

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

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

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

O’Neil LR, TJ Conway, DH Tobey, FL Greitzer, AC Dalton, PK Pusey. 2014. *Secure Power Systems Professional Phase III Final Report: Recruiting, Selecting and Developing Secure Power Systems Professionals*. PNNL-23583, Pacific Northwest National Laboratory, Richland, Washington.

O’Neil LR, TJ Conway, DH Tobey, FL Greitzer, AC Dalton, PK Pusey. 2015a. *Secure Power Systems Professional Phase III Recruiting, Selecting, and Developing Secure Power Systems Professionals: Individual and Team Performance Guidelines*. PNNL-24139, Pacific Northwest National Laboratory, Richland, Washington.

O’Neil LR, TJ Conway, DH Tobey, FL Greitzer, AC Dalton, PK Pusey. 2015b. *Secure Power Systems Professional Phase III Recruiting, Selecting, and Developing Secure Power Systems Professionals: Job Profiles*. PNNL-24138, Pacific Northwest National Laboratory, Richland, Washington.

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

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

Pacific Northwest
NATIONAL LABORATORY

U.S. DEPARTMENT OF
ENERGY

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

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

www.pnnl.gov