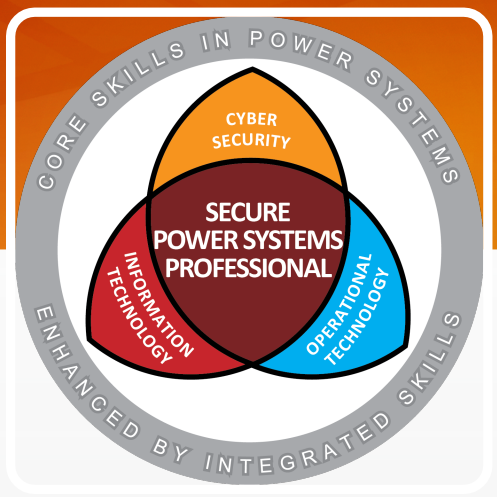
PNNL-24139



Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle Since 1965

SPSP Phase III Recruiting, Selecting, and Developing Secure Power Systems Professionals: Individual and Team Performance Guidelines

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

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-24139

SPSP Phase III Recruiting, Selecting, and Developing Secure Power Systems Professionals: Individual and Team Performance Guidelines

LR O'Neil, PNNL
TJ Conway, SANS
DH Tobey, VivoWorks
FL Greitzer, PsyberAnalytix
AC Dalton, PNNL
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 pending 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 aspects of power systems cybersecurity

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 SPSP 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 competently fulfill the new responsibilities of SPSPs.

Individual/Team Performance Guidelines were developed for each of the four job roles. They enable an "at-a-glance" view of the multidisciplinary and collaborative nature of SPSP job roles, for which skill sets were studied and then mapped to stories of critical incidents or vignettes. This afforded an enumeration of tasks required of each job role to effectively perform responsibilities and to meet best-practice goals for that operation. Assignment of these tasks among the job roles, either as an individual responsibility or a collaborative responsibility, was validated during a job performance model analysis. The analysis identified 13 master vignettes from the collection of critical incident stories, many of which shared a common set of job responsibilities and tasks that were grouped into four vignette categories according to the task requirement for effective response to each event.

The Individual/Team Performance 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*). They are presented in this report for standalone reference and application by users in the field.

Acronyms and Abbreviations

AMI	advanced metering infrastructure
ANSI	American National Standards Institute
CIP	critical infrastructure protection
DHS	U.S. Department of Homeland Security
DOE	U.S. Department of Energy
EEOC	(United States) Equal Employment Opportunity Commission
IDS	intrusion detection system
IR	incident response
NERC	North American Electric Reliability Corporation
NTP	Network Time Protocol
SIEM	Security Information and Event Management
SME	subject matter expert
SPSP	Secure Power Systems Professional

Contents

1.0 Introduction

For the convenience of the user, the contents of this report were excerpted from Appendix F of *Secure Power Systems Professional Phase III Final Report: Recruiting, Selecting and Developing Secure Power Systems Professionals* (O'Neil 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 at the U.S. Department of Energy (DOE) O.

1.1 Background

The SPSP project was developed to address the growing national deficit of electric power industry workers who 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 (see O'Neil 2015a, b) for selecting the best candidates for specific 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 SPSP workforce-related problems of today. Phase III is no different in this aspect. Candidate selection remains a challenge for many electric power entities as a result of the lack of adequate candidate selection tools that can map behavioral interview questions to the identified SPSP roles. The Phase III research has provided the foundation for the industry to begin strategic work on selecting the most qualified individual for a specific SPSP role, and offering a timely and invaluable tactical resource to help identify and train the SPSP employees to meet the industry's most pressing workforce development needs.

1.2 Report Contents

This report presents the Individual/Team Performance Guidelines for use in part or in whole to align workforce capabilities with the strategic goals and tactical focus of an organization. The guidelines provide a resource for recruiting and interviewing candidates for new position openings and may be applied to the professional development of existing staff.

2.0 Individual/Team Performance Guidelines

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

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

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

Promoting Defensibility of Fair Hiring Practices

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

- Recruitment and career development guides (see Appendix G in O'Neil et al. 2014)
- Job profiles (see Appendix D in O'Neil et al. 2014, or O'Neil et al. 2015b)
- Behavioral interview guidelines (see Appendix E in O'Neil et al. 2014, or O'Neil et al. 2015a).
- Individual and team performance guidelines (this report).

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

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

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

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

How to Use This Guide

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

3.0 AMI Attacks

4.0 Data Leakage and Related Attacks

(5.0 Encryption and Phishing Incidents

6.0 Incident Response Process and Log Management.

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

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

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

3.0 Vignette: AMI Attacks

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

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

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

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

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

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

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

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

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

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

GOAL: Investigate security events and analyze whether they are incidents.

RESPONSIBILITY: Make sure sufficient artifacts are available.

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

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

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

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

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

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

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

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

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

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

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

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

RESPONSIBILITY: Make sure communication plans are updated.

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

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

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

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

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

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

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

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

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

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

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

4.0 Vignette: Data Leakage and Related Attacks

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

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

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

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

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

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

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

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

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

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

GOAL: Investigate security events and analyze whether they are incidents.

RESPONSIBILITY: Make sure sufficient artifacts are available.

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

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

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

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

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

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

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

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

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

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

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

5.0 Vignette: Encryption and Phishing Incidents

GOAL: Investigate security events and analyze whether they are incidents.

RESPONSIBILITY: Make sure sufficient artifacts are available.

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

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

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

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

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

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

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

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

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

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

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

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

6.0 Vignette: Incident Response Process and Log Management

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

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

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

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

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

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

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

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

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

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

GOAL: Install security monitoring solutions.

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

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

RESPONSIBILITY: Make sure all solutions being installed have been authorized.

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

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

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

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

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

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

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

Cyber Secure Power Engineer	Security Operator	Incident Response	Intrusion Analyst
Develop possible attack techniques against specific technologies and implementations in your power systems deployments.	Understand incident response, notification, and log handling requirements of business.	Understand incident response, notification, and log handling requirements of business.	Understand incident response, notification, and log handling requirements of business.
	Configure rules for SIEM tools to capture and flag events known to be intrusion indicators.		Configure rules for SIEM tools to capture and flag events known to be intrusion indicators.
	Configure your security log management tool to sort and filter data to best suit the event being analyzed.		Configure your security log management tool to sort and filter data to best suit the event being analyzed.
	Coordinate with administrators from other departments (i.e., networking, operating systems, servers) to identify strengths and weaknesses in the organization's logging implementations.		Coordinate with administrators from other departments (i.e., networking, operating systems, servers) to identify strengths and weaknesses in the organization's logging implementations.

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

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

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

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

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

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

GOAL: Investigate security events and analyze whether they are incidents.

RESPONSIBILITY: Make sure sufficient artifacts are available.

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

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

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

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

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

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

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

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

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

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

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

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

O'Neil LR, 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: Behavioral Interview Guidelines by Job Roles*. PNNL-24140, 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

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

U.S. DEPARTMENT OF
ENERGY

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

www.pnnl.gov