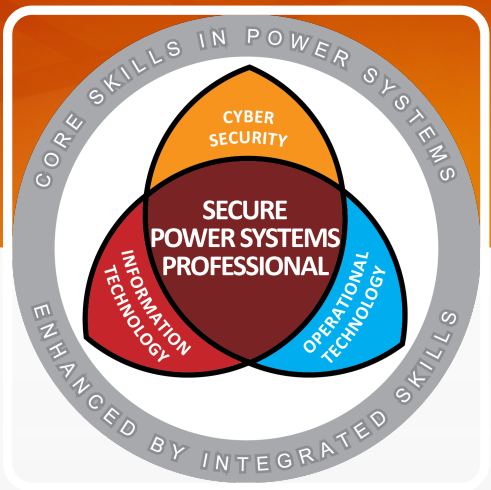
PNNL-24138



Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle Since 1965

SPSP Phase III Recruiting, Selecting, and Developing Secure Power Systems Professionals: Job Profiles

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-24138

SPSP Phase III Recruiting, Selecting, and Developing Secure Power Systems Professionals: Job Profiles

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 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 qualify and equip existing employees to work as SPSPs.

The job profiles presented in this report 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 intended for standalone reference and application by interested users in the field.

Acronyms and Abbreviations

C2M2	Cybersecurity Competency Maturity Model
CEH	certified ethical hacking
CISA	Certified Information Systems Auditor
CISM	Certified Information Security Manager
CISSP	Certified Information Systems Security Professional
CRISC	Certified in Risk and Information Systems Control
DOE	U.S. Department of Energy
ES-C2M2	Electricity Subsector Cybersecurity Capability Maturity Model
GCIA	GIAC Certified Intrusion Analyst
GCIH	GIAC Certified Incident Handler Certification
GIAC	Global Information Assurance Certification
GPEN	GIAC Penetration Testing Certification
GWAPT	GIAC Web Application Penetration Tester
IRT	Incident Response Teams
n.d.	no date
NICE	National Initiative for Cybersecurity Education
OE	Department of Energy Office of Electricity Delivery and Energy Reliability
SHRM	Strategic Human Resource Management
SOC	System Operator Certification
SPSP	Secure Power Systems Professional

Contents

1.0 Introduction

For the convenience of the user, the contents of this report were excerpted from Appendix D 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 (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 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 approaching retirement 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.

Phase I of this project 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

Promoting Defensibility of Fair Hiring Practices

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

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

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

established the framework for developing important tool sets and capabilities (see O'Neil et al. 2014, 2015a, b) for selecting candidates who are best suited for specific SPSP roles.

The previous two phases of the SPSP project have provided much-needed strategic findings to help power grid entities address workforce issues. In addition, each phase has provided immediate tactical tools, data, and approaches to help solve the most pressing problems facing the power industry today. Without exception, Phase III provided the foundation for the industry to begin strategic work on selecting the most qualified individual for a specific SPSP role, which remains a challenge for electric power entities because most entities currently lack an adequate candidate selection tool that can map behavioral interview questions to the identified SPSP roles. The completion of Phase III provided a timely and valuable tactical resource and capability to help identify and train the SPSP employees that the industry needs now.

1.2 Report Contents

This report presents the psychometrically validated job profiles that meet the U.S. Equal Employment Opportunity Commission and American National Standards Institute requirements. They 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.

2.0 Job Profiles

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

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

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

- a valid job task analysis that produces a list of essential responsibilities (or functions) and a comprehensive list of knowledge, skill, and abilities required for successful job performance

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

- a list of related workforce requirements (e.g., the National Initiative for Cybersecurity Education functional role requirements, and the Electricity Sector Cybersecurity Capability Maturity Model [ES-C2M2] objectives), certifications, and education.

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

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

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

How to Use This Guide

This report contains the following sections:

3.0 Secure Power Systems Engineer

4.0 Secure Power Systems Incident Responder

5.0 Secure Power Systems Intrusion Analyst

6.0 Secure Power Systems Security Operator

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

3.0 Secure Power Systems Engineer

3.1 Major Responsibilities

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

4. Log power systems security incidents.

3.2 NICE − National Cybersecurity Workforce Framework Tasks

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

3.2.1 Assess and Manage Power Systems Risk

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

3.2.2 Identify and Mitigate Power Systems Vulnerabilities

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

3.2.3 Implement Power Systems Security Monitoring

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

3.2.4 Log Power Systems Security Incidents

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

3.3 ES-C2M2 Objectives to Determine Maturity Level

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

3.3.1 Assess and Manage Power Systems Risk

- Establish Cybersecurity Risk Management Strategy (4.3.1 Risk Management)[2]
- Manage Cybersecurity Risk (4.3.1 Risk Management)
- Manage Dependency Risk (4.3.8 Supply Chain and External Dependencies Management)
- Manage Risk Activities (4.3.1 Risk Management)

3.3.2 Identify and Mitigate Power Systems Vulnerabilities

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

3.3.3 Implement Power Systems Monitoring

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

[2] The numbered section cited parenthetically here and ensuing sections refer to the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2 2014).

3.3.4 Log Power Systems Security Incidents

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

3.4 Applicable Certifications

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

SPSP-Specific Certifications (and issuing organizations)

- Certified Ethical Hacker (EC-Council)
- Certified Incident Hacker (Global Information Assurance Certification [GIAC])
- Certified Security Manager (Information Systems Audit and Control Association [ISACA])
- Certified Intrusion Analyst (GIAC)
- Certified Information Systems Security Professional (International Information System Security Certification Consortium, Inc. (ISC^2)®)
- Control Systems Engineer license (International Society of Automation [ISA])
- System Operator Certification (North American Electric Reliability Corporation [NERC])
- Global Industrial Cyber Security Professional (GIAC)

3.4.1 Assess and Manage Power Systems Risk

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

3.4.2 Identify and Mitigate Vulnerabilities

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

3.4.3 Implement Power Systems Security Monitoring

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

3.4.4 Log Power Systems Security Incidents

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

4.0 Secure Power Systems Incident Responder

4.1 Major Responsibilities

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

4.2 NICE − National Cybersecurity Workforce Framework Tasks

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

4.2.1 Develop and Manage Power Systems Personnel

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

4.2.2 Log Power Systems Security Incidents

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

NICE Task ID	Description
861	Track and document Computer Network Defense incidents from initial detection through final resolution.

4.2.3 Manage Power Systems Process and Procedures

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

4.2.4 Respond to Power Systems Intrusions

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

4.3 ES-C2M2 Objectives to Determine Maturity Level

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

4.3.1 Develop and Manage Power Systems Personnel

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

4.3.2 Log Power Systems Security Incidents

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

4.3.3 Manage Power Systems Process and Procedures

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

4.3.4 Respond to Power Systems Intrusions

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

4.4 Applicable Certifications

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

4.4.1 Develop and Manage Power Systems Personnel

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

4.4.2 Log Power Systems Security Incidents

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

A.1.1.1 Manage Power Systems Process and Procedures

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

4.4.3 Respond to Power Systems Intrusions

None

5.0 Secure Power Systems Intrusion Analyst

5.1 Major Responsibilities

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

5.2 NICE − National Cybersecurity Workforce Framework Tasks

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

5.2.1 Analyze Power Systems Security Incidents

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

5.2.2 Develop and Manage Power Systems Personnel

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

5.2.3 Identify and Mitigate Power Systems Vulnerabilities

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

5.2.4 Log Power Systems Security Incidents

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

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

5.2.5 Respond to Power Systems Intrusions

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

5.3 ES-C2M2 Objectives to Determine Maturity Level

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

5.3.1 Analyze Power Systems Security Incidents

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

5.3.2 Develop and Manage Power Systems Personnel

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

5.3.3 Identify and Mitigate Power Systems Vulnerabilities

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

5.3.4 Log Power Systems Security Incidents

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

5.3.5 Respond to Power Systems Intrusions

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

5.4 Applicable Certifications

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

5.4.1 Analyze Security Incidents

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

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

5.4.2 Develop and Manage Personnel

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

5.4.3 Identify and Mitigate Vulnerabilities

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

5.4.4 Log Power Systems Security Incidents

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

5.4.5 Respond to Power Systems Intrusions

None

6.0 Secure Power Systems Security Operator

6.1 Major Responsibilities

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

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

6.2 NICE − National Cybersecurity Workforce Framework Tasks

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

6.2.1 Analyze Power Systems Security Incidents

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

NICE Task ID	Description
823	Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.
846	Serve as technical experts and liaisons to law enforcement personnel and explain incident details, provide testimony, etc.
861	Track and document Computer Network Defense incidents from initial detection through final resolution.

6.2.2 Develop and Manage Power Systems Personnel

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

6.2.3 Identify and Mitigate Power Systems Vulnerabilities

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

6.2.4 Implement Power Systems Security Monitoring

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

6.2.5 Log Power Systems Security Incidents

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

6.2.6 Manage Power Systems Projects and Budgets

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

6.2.7 Respond to Power Systems Intrusions

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

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

6.3 ES-C2M2 Objectives to Determine Maturity Level

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

6.3.1 Analyze Power Systems Security Incidents

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

6.3.2 Develop and Manage Power Systems Personnel

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

6.3.3 Identify and Mitigate Power Systems Vulnerabilities

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

6.3.4 Implement Power Systems Security Monitoring

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

6.3.5 Log Power Systems Security Incidents

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

6.3.6 Manage Power Systems Projects and Budgets

- Sponsor Cybersecurity Program (4.3.10 Cybersecurity Program Management)

6.3.7 Manage Power Systems Security Operations

- Assign Cybersecurity Responsibilities (4.3.9 Workforce Management)
- Escalate Cybersecurity Events (4.3.7 Event and Incident Response, Continuity of Operations)

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

6.4 Applicable Certifications

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

6.4.1 Analyze Security Incidents

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

6.4.2 Develop and Manage Personnel

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

6.4.3 Identify and Mitigate Vulnerabilities

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

6.4.4 Implement Power Systems Security Monitoring

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

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

6.4.5 Log Power Systems Security Incidents

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

6.4.6 Manage Power Systems Projects and Budgets

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

6.4.7 Manage Power Systems Security Operations

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

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.

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

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

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

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: Individual and Team Performance Guidelines*. PNNL-24139, 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