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

How to Recruit Secure Power Systems Professionals

A Guide for Human Resources and Hiring Managers

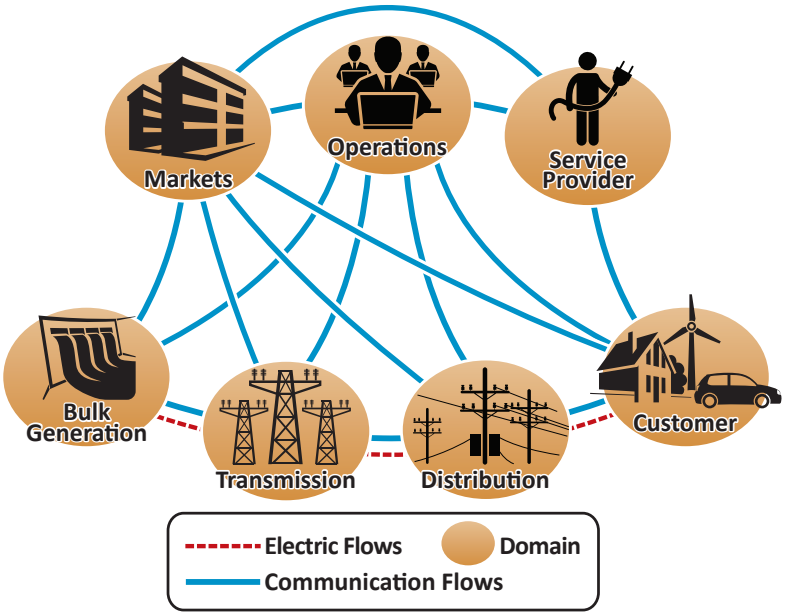
Faced with an aging power infrastructure and growing energy demand, the United States has embarked on an ambitious endeavor to expand and modernize the electric power grid, leading to a digital, highly adaptable, and demand-driven smart grid. With the current lack of cybersecurity practitioners, there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

What Does an SPSP Do?

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

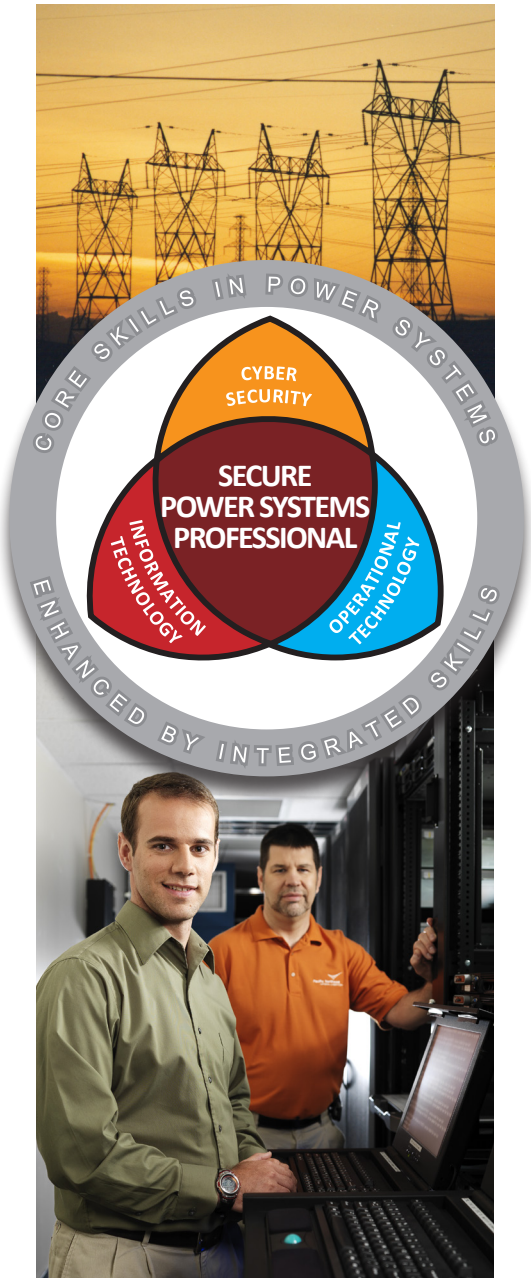
Power System Intrusion Analysis: Monitor networks, conduct traffic analysis, and detect intrusions due to malware, employee misconduct, sensitive data breaches, and other forms of external attacks.

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



Based on NIST Smart Grid Framework 1.0, September 2009

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



Profile of an Ideal Candidate

Basic Qualifications:

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

Preferred Skills:

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

Desirable Professional Attributes:

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

Recruitment Resources

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

Contact

Lori Ross O'Neil
Pacific Northwest National Laboratory
509-375-6702, lro@pnnl.gov

https://www.controlsystemsroadmap.net/efforts/Pages/SPSP.aspx

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