Cybersecurity and the Solar Workforce: Considerations for States

A Cybersecurity Advisory Team for State Solar (CATSS) Tool

NASEO
National Association of State Energy Officials

National Association of Regulatory Utility Commissioners

Cybersecurity and the Solar Workforce: Considerations for States

A Cybersecurity Advisory Team for State Solar (CATSS) Tool

Disclaimer:
The CATSS Toolkit is designed to provide states with basic education on cybersecurity issues for solar and enable their efforts to support cybersecurity enhancements efforts for solar. Cybersecurity challenges for solar should not be viewed as unique. All electricity generation technologies are, to varying degrees of potential severity and vulnerability, susceptible to cyberattacks and disruption. As interconnected electricity generation technologies, solar systems—and DERs generally—have a unique advantage to ensure that cybersecurity is incorporated by-design and prior to deployment, rather than applied ex post facto. The recommendations provided within the CATSS Toolkit/this tool were developed to meet the expressed needs of State Energy Offices and Public Utility Commissions during the project, and their respective purviews, priorities, and directives to support cyber-secure solar deployment in their states. While many industry and federal partners were included in the CATSS Advisory Group, it must be noted that neither the states' nor other stakeholders' perspectives collected are exhaustive. The Toolkit represents a snapshot of a quickly evolving and complex area, and should not be treated as a definitive guide, but rather a basis for continued discussion and adaptation of public-private partnerships for solar cybersecurity.

This material is based upon work supported by the U.S. Department of Energy (DOE) under award number DE-EE0009004. This report was prepared as an account of work sponsored by an agency of the United States government. Neither the United States government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or any agency thereof.

Introduction

The solar industry is growing rapidly. Forecasts suggest solar generation in the United States will grow by record-breaking numbers – to 30% by 2030.[1] This rapid growth has created significant employment opportunities. Over the past decade, solar employment has more than doubled from 105,145 jobs in 2011 to 255,037 jobs in 2021. The most significant growth has taken place in the installation and project development areas, where employment more than tripled since 2011 to reach 168,960 jobs in 2021.[2] Estimates suggest more than 1,500,000 workers will be needed by 2035.[3]

Cybersecurity skills and related knowledge have emerged as priority needs in the solar industry to support continued growth and quell concerns from stakeholders concerned with electric grid reliability and resilience. Traditionally, power systems were operated with dedicated communication channels to large generators and utility-owned assets. As the solar sector continues to grow as a distributed resource, particularly when combined with storage, the power system attack surface is expanding because solar systems often communicate to utilities, aggregators, and other grid operators over the public internet. Technology advancements are also allowing solar systems to provide a range of grid-support functions, that—if controlled or programmed improperly—present a risk of power system disturbances.[4]

Yet, research suggests there are more unfilled cybersecurity jobs than there are well-trained skilled people to fill them, regardless of industry sector. Demand is growing rapidly. In the solar sector, the cybersecurity skills shortfall has raised concerns among solar industry participants, utilities, and policymakers alike.

For State Energy Offices and Public Utility Commissions (PUCs), the topic of cybersecurity workforce is highly relevant. These state agencies ensure that consumer- and investor-owned utilities operate in a reliable, secure and safe manner. They also ensure that state-wide and utility specific plans are in place to effectively respond to energy related cybersecurity incidents should they occur. It is imperative that these agencies have knowledgeable staff to engage with energy stakeholders to identify emergent cybersecurity risks that may affect service reliability and recommend viable mitigation strategies. Given the rapid growth of solar, it is worthwhile for states to understand the intersection of cybersecurity risk management in the solar and utilities sectors, and encourage the growth of skilled cybersecurity workforces in both. Moreover, State Energy Offices and PUCs can amplify solar workforce training initiatives and build partnerships that help develop cyber-specific skills.

Cybersecurity Competencies for the Solar Workforce

A well-trained workforce is an essential ingredient to the growth of the solar energy sector. For example, solar installation professionals must be trained to properly design, install, and maintain solar energy systems. Power systems engineers must be trained to successfully integrate these new distributed resources into the grid and drive innovation. Similarly, well- trained cybersecurity professionals are required to mitigate cyber risk in the solar system design, installation, integration, and operational stages. However, cybersecurity professionals are typically trained to focus on data confidentiality, integrity, and availability (CIA) in information technology (IT) systems and, as such, they are not accustomed to thinking in terms of safety and reliability of operational systems, often referred to as OT. While IT is studied more than OT, there is a small but growing OT workforce and resources. Both IT and OT professionals are trained on CIA, but IT tends to focus predominantly on data confidentiality, while OT tends to focus on data integrity and availability. This focus contributes to grid safety and reliability. The difference is challenging to overcome – in part because it is engrained in the disparate educational pathways that professionals often travel. Instrument technicians, who calibrate flow meters, or engineers who manage programmable logic controllers (PLC) directly from their laptop have little idea about verifying the integrity of software they have downloaded or only running signed code.[5]

This challenge is exacerbated at the hiring stage. Cybersecurity jobs encompass a broad range of work, not all of which are deeply technical. As cybersecurity becomes an increasingly critical part of virtually every industry, the number of non-technical roles that require some amount of cybersecurity expertise is growing as well. Acknowledging and delineating the variations in cybersecurity jobs and associated competencies allow hiring managers to target the skills they need in the workplace. It also signals the need to develop a variety of cybersecurity educational and training solutions tailored to specific requirements in the solar industry.

The National Initiative on Cybersecurity Education (NICE) has worked to standardize the language and taxonomy used to describe work in cybersecurity. It developed the NICE Workforce Framework for Cybersecurity, which provides a common definition of cybersecurity, a comprehensive list of cybersecurity tasks, and the knowledge and skills required to perform those tasks. This taxonomy focuses on the work to be done and the attributes of people who are qualified to perform that work. According to NICE, employers can use the Framework to improve their ability to identify, recruit, develop, and retain cybersecurity talent. It provides job seekers a way to demonstrate in-demand competencies. It also helps educators create programs that are aligned to the cybersecurity jobs market, which, in turn, helps students develop in-demand skills. Use of the Framework also assists policy makers incentivize cybersecurity workforce development policies and standards of practice.

The Framework's foundational building blocks are Tasks, Knowledge, and Skills, which comprehensively describe cybersecurity work. Earlier versions of the Framework also used Categories as a means of grouping common cybersecurity functions and Specialty Areas to describe distinct areas of cybersecurity work. Although these groupings have since been removed from the Framework for simplicity purposes, NICE suggests that employers can continue to use them to identify key cybersecurity functions and work performed in the IT and OT domains.[6] The original categories are shown in Table 1.

Table 1: Cybersecurity Workforce Categories

Category	Description
Analyze	Performs highly specialized review and evaluation of incoming cybersecurity data to determine its usefulness for information and intelligence.
Collect and Operate	Provides specialized collection of cybersecurity data that may be used to develop information and intelligence.
Investigate	Investigates cybersecurity events or crimes related to digital systems, networks, and evidence.
Operate and Maintain	Provides the support, administration, and maintenance necessary to ensure effective and efficient cyber system performance and security.
Oversee and Govern	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
Protect and Defend	Identifies, analyzes, and mitigates threats to internal cyber systems and/or networks.
Securely Provision	Conceptualizes, designs, procures, and/or builds secure cyber systems, with responsibility for aspects of system and/or network development.

Table 2[7] breaks down each category into 33 specialty areas contained within the Framework to exemplify areas ripe for cybersecurity expertise within solar project design/ systems engineering or installation. It also indicates those areas where State Energy Offices and PUCs, collectively referred to as States in this document, may find cybersecurity expertise useful when working with utilities and solar industry stakeholders. Green checks indicate that hiring expertise in that specialty area will help embed cybersecurity in core business and operational activities. Typically, grid operators and solar industry developers/aggregators and installers require expertise in most of these specialty areas. State Energy Offices and Public Utility Regulators, however, do not have operational roles and as such, may only require familiarity with the skills required to perform them may enhance their program assessment and analysis efforts. The orange checks indicate familiarity with the specialty area is suggested.

Table 2: Sample NICE Cybersecurity Workforce Framework Specialty Areas

Framework Category	Framework Specialty Area	Description	Skill Sets		
			Solar Developers/ Systems Engineering	Solar Installers[8]	States[9]
Analyze	Threat Analysis	Identifies and assesses the capabilities and activities of cybersecurity criminals or foreign intelligence entities; produces findings to help initialize or support law enforcement and counterintelligence investigations or activities.	✓	✓	✓
	Exploitation Analysis	Analyzes collected information to identify vulnerabilities and potential for exploitation.	✓	✓	✓
	All-Source Analysis	Analyzes threat information from multiple sources, disciplines, and agencies across the intelligence community. Synthesizes and places intelligence information in context; draws insights about the possible implications.	✓	✓	✓
	Cyber Operational Planning	Performs in-depth joint targeting and cybersecurity planning process. Gathers information and develops detailed operational plans. Conducts strategic and operational-level planning across the full range of operations for integrated information and cyberspace operations.	✓	✓	
	Cyber Operations	Performs activities to gather evidence on criminal or foreign intelligence entities to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities.	✓	✓	
	Digital Forensics	Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.	✓	✓	✓
Operate and Maintain	Data Administration	Develops and administers databases and/ or data management systems that allow for the storage, query, protection, and utilization of data.	✓	✓	✓[10]
	Customer Service and Technical Support	Addresses problems; installs, configures, troubleshoots, and provides maintenance and training. Typically provides initial incident information to the Incident Response Specialty.	✓	✓	
	Network Services	Installs, configures, tests, operates, maintains, and manages networks, including hardware and software that permit the sharing and transmission of all spectrum transmissions to support the security of information and operational systems.	✓	✓	

Key: Skill Sets Likely Needed (✓), Skill Sets Likely Helpful (✓)

Framework Category	Framework Specialty Area	Description	Skill Sets		
			Solar Developers/ Systems Engineering	Solar Installers[8]	States[9]
Operate and Maintain	Systems Administration	Installs, configures, troubleshoots, and maintains hardware and software to ensure their confidentiality, integrity, and availability. Manages accounts, firewalls, and patches. Responsible for access control, passwords, and account creation and administration.	✓	✓	✓
	Systems Analysis	Studies an organization's current computer systems and procedures, and designs information systems solutions to help the organization operate more securely, efficiently, and effectively. Brings IT and OT together by understanding the needs and limitations of both.	✓	✓	✓
	Training, Education, and Awareness	Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, delivers and/or evaluates training courses, methods, and techniques as appropriate.			✓
	Cybersecurity Management	Oversees the cybersecurity program of an information system or network, including managing information security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, requirements, policy enforcement, emergency planning, security awareness, and other resources.	✓	✓	✓
	Strategic Planning and Policy	Develops policies and plans and/or advocates for changes in policy that support organizational cyberspace initiatives or required changes/enhancements.	✓	✓	✓
	Executive Cyber Leadership	Supervises, manages, and/or leads work and workers performing cyber and cyber-related and/or cyber operations work.	✓	✓	✓
	Program/ Project Management and Acquisition	Applies knowledge of data, information, processes, organizational interactions, skills, and analytical expertise, as well as systems, networks, and information exchange capabilities to manage acquisition programs. Executes duties governing hardware, software, and information system acquisition programs and other program management policies. Provides direct support for acquisitions that use IT/OT, applying related laws and policies, and provides related guidance throughout the total acquisition life cycle.	✓	✓	✓
Protect and Defend	Cyber Defense Analysis	Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network to protect information, information systems, and networks from threats.	✓	✓	✓

Key: Skill Sets Likely Needed (✓), Skill Sets Likely Helpful (✓)

Framework Category	Framework Specialty Area	Description	Skill Sets		
			Solar Developers/ Systems Engineering	Solar Installers[8]	States[9]
Protect and Defend	Cyber Defense Infrastructure Support	Tests, implements, deploys, maintains, reviews, and administers the infrastructure hardware and software that are required to effectively manage the computer network defense service provider network and resources. Monitors network to actively remediate unauthorized activities.	✓	✓	
	Incident Response	Responds to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.	✓	✓	✓[10]
	Vulnerability Assessment and Management	Conducts assessments of threats and vulnerabilities; determines deviations from acceptable configurations, enterprise, or local policy; assesses the level of risk; and develops and/or recommends appropriate mitigation countermeasures in operational and nonoperational situations.	✓	✓	
Securely Provision	Risk Management	Oversees, evaluates, and supports the documentation, validation, assessment, and authorization processes necessary to assure that existing and new cyber systems meet the organization's cybersecurity and risk requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.	✓	✓	✓
	Software Development	Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.	✓		
	Systems Architecture	Develops system concepts and works on the capabilities phases of the systems development life cycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.	✓		
	Technology R&D	Conducts technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility.	✓	✓	
	Systems Requirements Planning	Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions. Provides guidance about applicability of cyber systems to meet business needs.	✓	✓	

Key: Skill Sets Likely Needed (✓), Skill Sets Likely Helpful (✓)

Framework Category	Framework Specialty Area	Description	Skill Sets		
			Solar Developers/ Systems Engineering	Solar Installers[8]	States[9]
Securely Provision	Test and Evaluation	Develops and conducts tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost-effective planning, evaluating, verifying, and validating of technical, functional, and performance characteristics (including interoperability) of systems or elements of systems incorporating IT.	✓	✓	
	Systems Development	Works on the development phases of the systems development life cycle.	✓	✓	

Key: Skill Sets Likely Needed (✓), Skill Sets Likely Helpful (✓)

Cybersecurity Talent Pipelines and Pathways

Research shows that most cybersecurity job openings nationwide match the NICE Framework's "Operate & Maintain" category, followed closely by "Securely Provision."[11] These numbers suggest that businesses are primarily searching for hands-on cybersecurity professionals to ensure effective and efficient system performance and security. Job openings in the "Oversee & Govern" category, however, are also high. As Table 2 implies, States may be in direct competition with industry for these cybersecurity skills. Unless more talent pipelines are developed or skills development expedited, the shortfall of skilled professionals will impede progress to improving cybersecurity across the solar industry. Rethinking where and how cybersecurity skills are learned and acquired is necessary.

Historically, many employers use a college or university degree, particularly in STEM, to pre-qualify potential cybersecurity job candidates. Experts contend that such hiring practices ignore the pool of potential candidates with diverse educational and experiential backgrounds which may be well suited for the challenges in cybersecurity[12]. Employers also heavily weight certifications ¾ most often the Certified Information Security Systems Professional (CISSP) ¾ in their cybersecurity hiring practices. Ironically, research shows that there are approximately 141,000 current job openings requesting CISSP certifications, but only 95,000 certification holders worldwide.[13]

Another consideration for employers is timely access to skilled talent. Alternative workforce training programs, including apprenticeships and similar on-the-job training, which are designed to provide real-world, hands-on experience, are still somewhat rare in the cybersecurity space. Nonetheless, the inclusion of such programs, coupled with the addition of work-based learning into degree programs, will accelerate the growth in qualified cybersecurity talent to meet current and future needs.

Importantly, programs dedicated to increasing diversity and inclusion in the cybersecurity workforce will open new talent avenue for employers in the solar industry. Based on recent reporting, however, the solar industry must focus on improving efforts to prioritize diversity, equity, and inclusion in their hiring practices to tap into these new pools of cybersecurity talent.[14]

Cybersecurity Workforce Development Programs

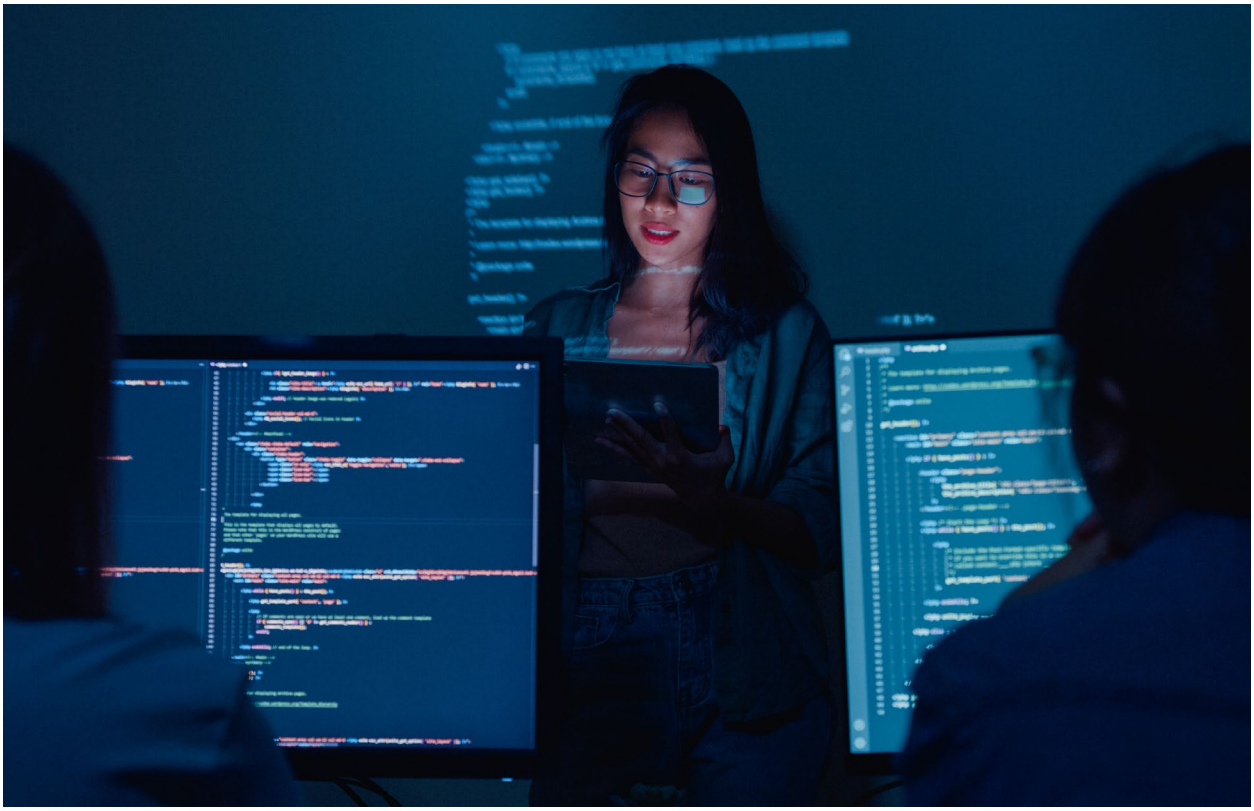
In addition to conventional degree programs, numerous cybersecurity training opportunities exist today. Although none are specific to the solar industry, skills developed during such training, especially focused on operational technology systems, are transferable among many industry sectors. The following is a sampling of available cybersecurity training resources. (Note that inclusion in this list does not imply endorsement.)

National Initiative for Cybersecurity Careers and Studies/ National Centers of Academic Excellence in Cybersecurity (NCAE–C) Program - DHS/ National Security Agency (NSA) program that promotes higher education and expertise in cybersecurity. Currently, there are more than 340 colleges and universities across 48 states, the District of Columbia, and the Commonwealth of Puerto Rico designated as National Centers of Academic Excellence in Cybersecurity.

Training for Cybersecurity Careers Training – collated by DHS, this catalog organizes more than 2,000 courses provided by organizations across the cybersecurity industry to meet the needs of cybersecurity professionals who want to update their skills and advance their career, students who are looking to enter the cybersecurity field, and people interested in career changes. The courses map to the NICE Framework functions and specialty areas.

Cybersecurity Workforce Development and Training for Underserved Communities - DHS-funded partnerships with community-based, non-profit organizations that help military veterans and young adults from underserved communities develop cyber skills through entry-level training and apprenticeships.

SANS Training Institute – offers practitioner-focused training and certification that bridges IT, engineering and cyber security to achieve security for industrial control systems from design through retirement.



Solar Workforce Development Programs

The U. S. Department of Energy offers a number of programs aimed at solar workforce development and connecting job seekers with employers in the solar and other energy related sectors. Although not specifically aimed at cybersecurity skills development in this sector, some programs contain aspects of cybersecurity training.

- **Solar Ready Vets** – connects veterans and transitioning military service members with career training, professional development, fellowships, and employment opportunities in the solar industry.
- **Solar District Cup** – annual collegiate competition challenging multidisciplinary student teams to design and model optimized distributed energy systems for a campus or urban district.
- **Education Materials for Professional Organizations Working on Efficiency and Renewable Energy Developments (EMPOWERED) Program** – provides training and educational resources for first responders, safety officials, and building managers and owners working with distributed energy resources.
- **Expanding the Solar Workforce and Digital Adaptation Training for DER on the Grid** - develops solar training for a variety of participants while also preparing the utility industry for a digital future and modern grid with high penetration levels of solar and other distributed energy resources.
- **CyberStrike Training Program** - enhances the ability of energy sector owners and operators to prepare for a cyber incident impacting operational technology. Training features live exercises using real equipment and scenarios routinely experienced by utility owners and operators. DOE is currently developing a version of this training curriculum that focuses on renewable energy systems.
- **Clean Energy Innovator Fellowship** – this program funds recent graduates and energy professionals to work with critical energy organizations like public utility commissions and grid operators to advance clean energy solutions.

Additional Resources

- IREC: Clean Energy Workforce Development Strategies (irecusa.org/our-work/workforce-development-strategies/?)
- A & R Solar: Get Started in a Career in Solar_ (www.a-rsolar.com/solar-jobs-training/)
- Solar Energy Industries Association (SEIA): Apprenticeships in the Solar Industry (www.seia.org/initiatives/apprenticeships)
- DOE: Solar Technologies Energy Office Fellowship and Research Opportunities (www.energy.gov/eere/solar/fellowships-and-research-opportunities)

Conclusion

Because of the competition for individuals trained or educated in cybersecurity is so great, it can be challenging for state agencies to offer competitive salaries for individuals with cybersecurity experience. As such, states are often faced with developing individuals within their existing workforce. Proper skill development and training takes resources, time, and commitment. The constant risk is that once trained by the state, individuals are often incentivized to move on to other better paying jobs in the private sector.

State Energy Offices and PUCs have unique positions to their states to highlight risks to energy infrastructure and work towards mitigating those risk in our increasingly cyber dependent world. The information provided in this document is intended to assist states manage cyber risk. As noted, the shortfall of cybersecurity talent, generally, and in the solar sector specifically contributes to the growing threat that new interconnected technologies create. This document provides a good starting point for states to understand the scope of skills necessary to manage relevant cybersecurity risks across the value chain as well as options for training and developing the requisite talent pool.

References

1 Solar Energy Industries Association. "Solar Data Cheat Sheet." Last modified December 13, 2022. https://www.seia.org/research-resources/solar-data-cheat-sheet

2 Lewis, Michelle. "US solar jobs increased 9% in 2021 – here's how it breaks down by sector and state." *Electrek*, July 26, 2022. https://electrek.co/2022/07/26/us-solar-jobs-increased-9-in-2021-heres-how-it-breaks-down-by-sector-and-state/#:~:text=Over%20the%20past%20decade%2C%20US,reach%20168%2C960%20jobs%20in%202021

3 https://irecusa.org/programs/solar-jobs-census/

4 Johnson, Jay. "Roadmap for Photovoltaic Cyber Security." Sandia National Laboratories, Printed December 2017. https://sunspec.org/wp-content/uploads/2020/01/Roadmap-for-Photovoltaic-Cyber-Security-SAND2017-13262-4-10-2018.pdf

5 https://industrialcyberforce.org/wp-content/uploads/2020/08/A-Security-Workforce-to-Bridge-the-IT-OT-Gap.pdf

6 Petersen, Rodney, Danielle Santos, Mattew C. Smith, Karen A. Wetzel, and Greg Witte. "Workforce Framework for Cybersecurity (NICE Framework)." *NIST Special Publication* 800-181, Rev. 1, November 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

7 Adapted from *A Guide for Public Utility Commissions: Recruiting and Retaining a Cybersecurity Workforce*, NARUC, 2021.

8 https://www.a-rsolar.com/solar-jobs-training

9 States will not necessarily perform activities described, but expertise within this specialty area will likely help maximize their efforts.

10 Most relevant for States who have designated emergency management responsibilities per State Energy Security Plan or State Emergency Operations Plans.

11 Cyber Seek. "Job Openings By NICE Workforce Framework Category." Accessed March 6, 2023. https://www.cyberseek.org/heatmap.html

12 Bate, Laura. "Cybersecurity Workforce Development: A Primer." *New America*, November 1, 2018. www.newamerica.org/cybersecurity-initiative/reports/cybersecurity-workforce-development/

13 Cyber Seek. "Certification Holders/Openings Requesting Certification." Accessed March 6, 2023. www.cyberseek.org/heatmap.html

14 Interstate Renewable Energy Council. "National Solar Jobs Census." July 25, 2022. irecusa.org/resources/national-solar-jobs-census-2021/

NASEO
National Association of State Energy Officials