NARUC
National Association of Regulatory Utility Commissioners

A Guide for Public Utility Commissions: Recruiting and Retaining a Cybersecurity Workforce

Ashton Raffety
Lynn P. Costantini
February 2021

Contents

Disclaimer

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000818.

Acknowledgments

The authors wish to thank the following individuals for contributing their time and expertise to the development of this paper:

- **Kate Marks**, **Brandi Martin**, and **Jason Pazirandeh**, U.S. Department of Energy
- **Keven Kleweno**, **Christina Ann Hunter**, **Claire Knudsen-Latta**, and **John Paul R. Manaois**, Regulatory Commission of Alaska
- **Stephen Capozzi**, Connecticut Department of Energy and Environmental Protection—Public Utilities Regulatory Authority
- **Jim Harmening** and **Wei Chen Lin**, Illinois Commerce Commission
- **Alexander Morese**, **Cody Matthews**, **Patrick Hudson**, **Brian Sheldon**, and **Joy Wang**, Michigan Public Service Commission
- **Chairman Gladys Brown Dutrieuille**, **David A. Alexander**, **Michael Holko**, **Rhonda Daviston**, **Colin Scott**, **Nathan Paul**, and **Patricia Wiedt**, Pennsylvania Public Utility Commission
- **Chuck Bondurant**, Texas Public Utility Commission
- **Jeff Baumgartner**, Berkshire Hathaway Energy
- **Ben Bolton**, Tennessee Department of Environment & Conservation, Office of Energy Programs
- **Tony Coulson**, **Vincent Nestler**, and **Anette Vladescu**, California State University—San Bernardino, Cybersecurity Center
- **Steve Mallard**, Tennessee College of Applied Technology
- **Dominic Saebeler**, The Information Trust Institute, University of Illinois
- **Craig Barrett**, Federal Energy Regulatory Commission
- **Danielle Byrnett** and **Will McCurry**, National Association of Regulatory Utility Commissioners

Foreword

Chairman Gladys Brown Dutrieuille
Chairman, Pennsylvania Public Utility Commission
Chair, NARUC Committee on Critical Infrastructure
Second Vice President, Mid-Atlantic Conference of Regulatory Utilities Commissioners

Over the last few decades, rapid advancements in technology have transformed the energy sector, especially electricity. From the smart grid, to solar, wind, and battery storage, to new operational models, these advancements improve reliability and resilience, which benefit consumers. And the pace of change is not slowing down. Although such innovation has proved invaluable, it has also generated more points of access to critical operating systems and opened new doors for potential cyberattacks perpetrated by those looking to inflict long-term damage.

We all play a role in keeping critical infrastructure cyber secure. As regulators, it is incumbent on us to engage our utilities and other key stakeholders on cybersecurity matters for this purpose. We must understand the evolving threats and vulnerabilities as well as the risk mitigation options that are available. We must weigh the costs and benefits of utilities' cybersecurity investments. And, should the day come, we must be ready to work with our utilities to recover from a successful cyberattack. To perform these functions, access to cybersecurity expertise is vital.

In Pennsylvania, the public utility commission created a division to focus entirely on cybersecurity issues and hired in-house cybersecurity experts to lead and grow it. Hiring isn't always an option, so some states have hired third-party experts to assist them. As this white paper describes, other avenues exist to acquire cybersecurity expertise, such as resource sharing. Regardless of the hiring path chosen, the key to commission success is prioritizing cybersecurity as if our nation's critical infrastructure depended on it. In fact, it does.

Introduction

Public utility commissions (PUCs) recognize that the critical infrastructure sectors they regulate face ever-evolving cybersecurity threats from malicious actors. To provide effective oversight and support their regulated utilities in addressing these threats, PUCs are striving to increase their cybersecurity expertise. Yet, a shortage of trained cybersecurity professionals in the workforce, coupled with internal budget constraints and strict civil service hiring requirements, may impact a PUC's ability to hire and retain qualified staff. These challenges, however, are not insurmountable.

This paper serves as a reference guide for PUCs trying to develop or expand their cybersecurity proficiency. It describes the role of cybersecurity personnel within a PUC and a range of cybersecurity skill sets that may fit a PUC's needs, as well as avenues for recruiting, retaining, and growing cybersecurity expertise. Appendices provide lists of cybersecurity training resources, recruitment pipelines, and a compendium of sample cybersecurity job descriptions for PUC consideration.

Cybersecurity Roles within PUCs

A PUC's mission is to ensure safe, reliable, and adequate utility service at a fair and equitable cost to ratepayers. For this reason, PUCs have historically maintained a staff of engineers, finance experts, environmental planners, lawyers, and other experts to advise commissioners on service rates based on reasonable and expected utility expenses. Because of today's evolving threat environment, commissioners need experts to advise on utilities' cybersecurity-related programs and cost recovery issues, emerging technical standards and requirements, and risks associated with applicable new technologies. These professionals identify, gather, and analyze pertinent information regarding utilities' cybersecurity risk management and preparedness programs. They identify gaps and articulate the impact to customer service reliability, and help identify ranges of viable improvements and associated costs for decision makers. They may also facilitate information sharing to help utilities prevent or recover from a cybersecurity incident.

Commissioners may call upon these experts to participate in or lead cybersecurity audits or risk assessments of utilities by utilizing their subject matter expertise to engage utilities in discussions about their risk management strategies, processes, and practices, and identify potential gaps. Upon completion of an assessment, cybersecurity professionals are uniquely positioned to advise commissioners on how utilities are approaching risk and thereby commissioners may choose to advise or direct utilities to stimulate additional investment. Expert knowledge is essential for this scope of work. Cybersecurity professionals within PUCs may also facilitate cybersecurity incident response and recovery exercises or observe those exercises hosted by utilities or emergency support function (ESF) 12 partners. These exercises provide participants with a solid understanding of what happens during a cybersecurity incident and how PUCs can facilitate the process for expediency. It also helps PUCs clarify their roles in the response and recovery process. Lessons learned become part of the prudency discussion at the PUC.

It is important to note that cybersecurity experts may perform different functions in different PUCs. In some PUCs, they exclusively have external utility facing roles; in others, they may only secure PUC-specific IT infrastructures, and in others, they may perform both functions. It is worth noting that in some PUCs, cybersecurity may not be a full-time role; rather, it may be part of a more extensive umbrella of critical infrastructure and risk management work.

As PUCs begin their journey to develop or expand their cybersecurity expertise, executive-level leadership within the PUC should act as a "champion" for any new cybersecurity programming. Discussions about utilities' cybersecurity operations are sensitive, and PUC efforts to establish a cybersecurity function may be met with resistance and fail to achieve their purpose without an executive-level leader driving the conversation forward. The champion should also ensure that new efforts align with the PUC's cybersecurity strategy. If your

PUC does not have a cybersecurity strategy, one can be developed utilizing NARUC's *Cybersecurity Strategy Development Guide*.[1]

In Their Own Words

"As a Cybersecurity Analyst for the Michigan Public Service Commission, I am responsible for the development and maintenance of the commission's Cybersecurity Program. This includes drafting and implementing the commission's cybersecurity rules, engaging industry leaders through annual meetings and reporting, collaborating with cybersecurity subject matter experts from government and industry, researching cybersecurity threats and vulnerabilities, and liaising with critical cybersecurity personnel at Michigan's energy providers. In addition, I advise the commission on state and federal policy or laws regarding cybersecurity and on the appropriate regulatory approaches to improve the planning, response, recovery, and mitigation of potential cybersecurity incidents at energy providers serving Michigan."

—***Brian Sheldon**, Cybersecurity Analyst, Michigan Public Service Commission*

"As a Policy Advisor for the Office of Cybersecurity and Risk Management (C&RM) at the Illinois Commerce Commission (ICC) I work on both internal and external projects. Internally, I advise the Director of C&RM on laws and policy regarding cybersecurity, privacy, information security, and critical infrastructure protection; this is accomplished by researching issues, conducting analysis, and developing explanations and opinions on a wide range of topics. I also liaise and collaborate with other divisions within the ICC to improve, train, test, and exercise our Continuity of Operations Plan, host continuing education events, produce cybersecurity educational materials, and provide technical assistance or data analytics on other projects. Externally, I examine, assess, encourage, and support ongoing efforts of public utilities to ensure the reliability, resiliency, and security of critical infrastructure. These activities include ensuring compliance with statutory provisions concerning cybersecurity, sharing of information in furtherance of critical infrastructure protection, encouraging adoption of widely accepted industry standards and frameworks, participating in conference and workshops, and designing and participating in exercises to foster cross-sector communication, coordination and collaboration among critical infrastructure entities."

—***Wei Chen Lin**, Policy Advisor, Cybersecurity & Risk Management, Illinois Commerce Commission*

Types of Cybersecurity Skills

Like other professions, cybersecurity includes areas of specialization. There is no "default" cybersecurity expert or single skill set that applies to cybersecurity broadly. When hiring, PUCs must carefully consider their state's cybersecurity strategy, their own cybersecurity strategy, the roles and responsibilities that a cybersecurity professional will undertake, and the essential skills necessary to perform them.

In 2017, the National Institute of Standards and Technology (NIST) released a special publication outlining a consistent and federally recognized lexicon to describe cybersecurity work. It is known as the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework)[2]. PUCs can use this framework to determine the type of cybersecurity expertise they may need. Note that the NICE Framework was not explicitly designed to assist regulatory agencies. Nevertheless, the framework provides useful context into the types of expertise necessary to regulate a utility's cybersecurity operations. Table 1 describes each of the seven categories outlined within the NICE Framework.

1 Cybersecurity Strategy Development Guide, https://pubs.naruc.org/pub/8C1D5CDD-A2C8-DA11-6DF8-FCC89B5A3204

2 NICE Cybersecurity Workforce Framework, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf?trackDocs=NIST.SP.800-181.pdf

Table 1: NICE Framework Categories

Category	Description
Analyze	Performs highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
Collect and Operate	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
Investigate	Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.
Operate and Maintain	Provides the support, administration, and maintenance necessary to ensure effective and efficient IT 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 IT systems and/or networks.
Securely Provision	Conceptualizes, designs, procures, and/or builds secure IT systems, with responsibility for aspects of system and/or network development.

Each NICE Framework category includes several specialty areas. Table 2 describes these specialty areas and indicates whether such expertise may be useful within a PUC. Although PUC personnel may not directly perform all of the functions outlined in Table 2, expertise in these areas may prove useful when working with utilities that are performing those specialty area tasks. It is vital for personnel within PUCs to understand the cybersecurity functions performed by utilities, and it is especially beneficial if staff within the PUC and utility share common skill sets. PUC hiring managers can utilize Table 2 to compare candidates' skills versus the skills they need to meet cybersecurity goals.

The "Skill Sets a PUC Likely Needs" and the "Skill Sets a PUC May Need" columns shown in Table 2 represent the following:

- **Skill Sets a PUC Likely Needs** (✔): Generally, expertise within this specialty area will likely help PUCs maximize their efforts when working with utilities to address the efficacy of their cybersecurity risk management programs. For example, this may include:
  - conducting cybersecurity audits or assessments,
  - managing cybersecurity reporting mechanisms,
  - developing cybersecurity standards,
  - analyzing cybersecurity-related rate cases, and
  - responding to a cybersecurity incident in coordination with utilities.

Expertise in these areas may also support internal needs, including:

  - cybersecurity training for relevant staff,
  - assisting in systems procurement for the PUC, and
  - working with third parties during the response and recovery stages of a cyber incident.

- **Skill Sets a PUC May Need** (✔): Expertise in this specialty area may help depending on a PUC's cybersecurity strategy and goals. Utilities typically undertake work in these specialty areas. Still, PUCs may find that a familiarity with these areas and the skills required to perform them may enhance their program assessment and analysis efforts.

Table 2: NICE Framework Specialty Areas

Framework Category	Framework Specialty Area	Description	Skill Sets a PUC Likely Needs[3]	Skill Sets a PUC May Need[4]
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.	✔	
	Targets	Applies current knowledge of one or more regions, countries, nonstate entities, and/or technologies.		✔
	Language Analysis	Applies language, cultural, and technical expertise to support information collection, analysis, and other cybersecurity activities.		✔
Collect and Operate	Collection Operations	Executes collection using appropriate strategies and within the priorities established through the collection management process.		✔
	Cyber Operational Planning	Performs in-depth joint targeting and cybersecurity planning process. Gathers information and develops detailed operational plans and orders supporting requirements. 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.		

3 PUCs will not necessarily perform activities described, but expertise within this specialty area will likely help PUCs maximize their efforts when working with utilities to address the efficacy of their cybersecurity risk management programs.

4 PUCs will not necessarily perform activities described, but expertise in the specialty area may help PUCs maximize their efforts when working with utilities to address the efficacy of their cybersecurity risk management programs.

Framework Category	Framework Specialty Area	Description	Skill Sets a PUC Likely Needs[3]	Skill Sets a PUC May Need[4]
Investigate	Cyber Investigation	Applies tactics, techniques, and procedures for a full range of investigative tools and processes to include, but not limited to, interview and interrogation techniques, surveillance, counter surveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.		
	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.	✔[5]	
	Knowledge Management	Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.	✔	
	Customer Service and Technical Support	Addresses problems; installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support). Typically provides initial incident information to the Incident Response Specialty.		✔
	Network Services	Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.		✔
	Systems Administration	Installs, configures, troubleshoots, and maintains server configurations (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 business and IT together by understanding the needs and limitations of both.		✔

5 In cases where the PUC is storing sensitive information provided by a utility.

Framework Category	Framework Specialty Area	Description	Skill Sets a PUC Likely Needs[3]	Skill Sets a PUC May Need[4]
Oversee and Govern	Legal Advice and Advocacy	Provides legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain. Advocates legal and policy changes, and makes a case on behalf of clients via a wide range of written and oral work products, including legal briefs and proceedings.	✔	
	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.	✔	
Oversee and Govern	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, applying IT-related laws and policies, and provides IT-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.		✔
	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.		✔

Framework Category	Framework Specialty Area	Description	Skill Sets a PUC Likely Needs[3]	Skill Sets a PUC May Need[4]
Protect and Defend	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.	✔[6]	
	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 IT 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 to customers about applicability of information systems to meet business needs.	✔	
	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.		✔

6 Most relevant for PUCs who have designated emergency management responsibilities per State Energy Assurance Plan or State Emergency Operations Plan.

Types of Cybersecurity Employees

Cybersecurity professionals within PUCs will perform tasks that match the NICE Framework's specialty areas or work with utility professionals who perform these tasks to accomplish PUC goals. There are distinct levels of cybersecurity professionals who collectively work toward these goals, including director-level, mid-level, and entry-level employees. Although they perform similar contextual duties, each team member is generally responsible for work products matching their education and experience level.

Director-level employees provide direction and guidance for the division's strategic operations and planning. They manage a team of mid- and entry-level employees who work with utilities and their cybersecurity programs and possibly control the PUC's internal networks. Directors are ultimately responsible for achieving goals. **Mid-level** employees are seasoned professionals who are experts in their specialty areas of focus. They advise the director and PUC staff on cybersecurity issues, provide information to utilities regarding PUC rules as they relate to cybersecurity, research and analyze cybersecurity threat indicators and behaviors, and among other things, lead specific efforts within their area of expertise. **Entry-level** employees are typically recent graduates with an education in a cybersecurity-related field or people who are transitioning into the cybersecurity field. These emerging professionals will build their cybersecurity knowledge and abilities by contributing to mid-level employees' projects and providing programmatic support to the entire division. Last, cybersecurity **interns/fellows** serve in limited roles primarily designed to foster their own education in cybersecurity practices. Their work within a commission typically includes leading a short-term research project or imitative. Although this paper does not focus on how to recruit interns/fellows, utilizing existing intern/fellow programs for cybersecurity roles can build interest in the PUC as an employer and contribute to longer term staffing goals.

Alternatives to hiring in-house cybersecurity talent include hiring **consultants**, utilizing **existing cybersecurity talent** within another state agency, and **training PUC staff** on cybersecurity basics. These alternatives are discussed in a later section in detail.

A PUC's cybersecurity division's organizational structure is not inherently different from any other PUC division, but outsourcing specialized cybersecurity expertise may be necessary to achieve goals. NARUC identified four organizational models for PUCs to consider as they organizationally structure their cybersecurity division, but recognizes that many effective variations of these models exist. These models are outlined in Table 3.

Table 3: Organizational Models for PUC Cybersecurity Divisions

Model	Leadership	Analytical Support	Programmatic Support
All In-house Cybersecurity Division	Hire **director-level** talent.	Hire **mid-level** talent.	Hire **entry-level** talent or **train current staff.**
	Description: This traditional model will develop and sustain institutional knowledge within the PUC and allow for long-term relationship building between the PUC and utilities' cybersecurity staff.		
In-house Cybersecurity Division and Outsourced Support	Hire **director-level** talent.	Hire **consultants.**	Hire **consultants.**
	Description: Hiring consultants on an as-needed basis allows for expert support and flexibility depending on the amount of support desired for specific projects. Hiring consultants through long-term contracts may be favorable if it is difficult to hire qualified in-house candidates because of strict civil service hiring requirements or open bidding processes.		
In-house Cybersecurity Division and Shared Resources	Hire **director-level** talent.	Utilize **existing cybersecurity talent** in other state agencies.	Hire **entry-level** talent or **train current staff.**
	Description: Utilizing existing cybersecurity expertise in other state agencies is an efficient way to utilize state funds and save resources within the PUC (dependent on the agreement). Building long-term relationships with utilities and institutional knowledge within the PUC still exist with this option.		
Consolidate Cybersecurity Activities within an Existing Division	Utilize **existing leadership** within the PUC's organizational structure.	Hire **mid-level** talent or **consultants** or utilize **existing cybersecurity talent** in other state agencies.	Hire **entry-level** talent or **train current staff.**
	Description: Particularly relevant for small PUCs with fewer resources, housing cybersecurity activities within an existing division obviates the need to hire additional leadership. This model can be equally as effective as creating a division specifically for cybersecurity activities as long as the PUC still hires or obtains technical cybersecurity expertise to perform tasks.		

Recruitment and Retention of a Cybersecurity Workforce

A 2019 study by the International Information System Security Certification Consortium, or (ICS)², suggests that the U.S. cybersecurity workforce needs to grow by 62 percent to meet demand.[7] Between June 2019 and May 2020, an estimated 922,720 individuals worked in cybersecurity-related positions within the United States across all sectors, public and private. During this same period, 507,924 cybersecurity job openings remained unfilled because of the very low supply/demand ratio of qualified cybersecurity personnel.[8] For now, this means that cybersecurity professionals are in high demand, with competition for talent driving high salaries and generous compensation packages. Table 4 below shows that the public and utility sectors face the same drastically low supply/demand ratios for qualified cybersecurity professionals.

Table 4: Cybersecurity Jobs—Supply and Demand by Sector

June 2019 through May 2020

Sector	Total Cybersecurity Job Openings[9]	Total Employed Cybersecurity Workforce[10]	Cybersecurity Workforce Supply/Demand Ratio[11]
All Sectors (Public and Private)	507,924	922,720	1.8 (Very Low)
All Private Sectors	476,256	870,447	1.8 (Very Low)
Public Sector	31,669	52,273	1.7 (Very Low)
Utility Sector	2,139	4,504	2.1 (Very Low)

Across core cybersecurity roles, average salaries for entry-level employees across all sectors, public and private, range between $89,000 and $95,000.[12] Thus, budget constraints may hamper PUCs' ability to compete with private industry in their attempts to recruit skilled cybersecurity professionals. Once hired, retaining cybersecurity talent may prove challenging, owing to the abundance of opportunities for higher-paying positions with unfettered advancement potential in the private sector.

On a positive note, PUCs are not necessarily competing for the same type of cybersecurity skill sets. Research shows that most cybersecurity job openings across all sectors (public and private) nationwide match the NICE Framework's "Operate & Maintain" category, with only 7 percent of job openings matching the "Oversee & Govern" category.[13] These numbers suggest that the industry as a whole is primarily searching for hands-on cybersecurity professionals to ensure effective and efficient system performance and security. When analyzing the public and utility sectors separately, a similar breakdown is evident and outlined in Figure 1. As a subset of the Public Sector pie chart, PUCs likely need cybersecurity professionals with familiarity and expertise in various NICE Framework categories, but they are typically searching for professionals with experience or interest in the "Oversee and Govern" category, as outlined in Table 2 above.

---

7 Strategies for Building and Growing Strong Cybersecurity Teams, 2019, https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=1827084508A24DD75C60655E243EAC59ECDD4482.

8 Cybersecurity Supply/Demand Heat Map (data collected on October 7, 2020), https://www.cyberseek.org/heatmap.html.

9 Shows the number of online job listings for cybersecurity-related positions from June 2019 through May 2020.

10 Shows the estimated number of workers employed in cybersecurity-related jobs from June 2019 through May 2020. This includes workers in primary cybersecurity jobs—such as cybersecurity analysts—as well as workers in roles requiring cybersecurity-related skills and certifications to capture the full potential cybersecurity workforce.

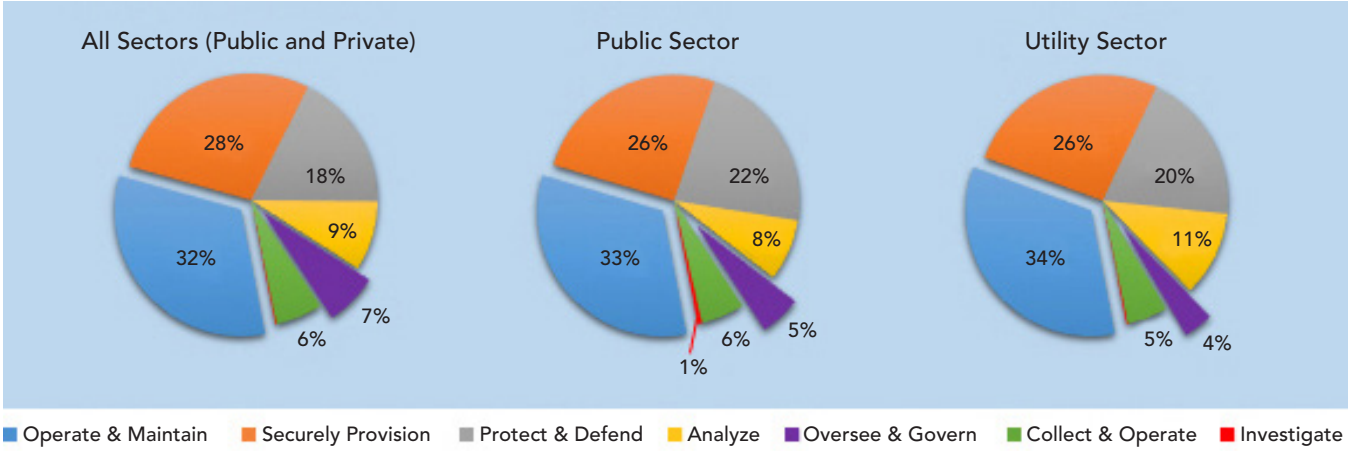
11 Shows the ratio of existing cybersecurity workers to cybersecurity job openings. The national average for all jobs is 3.7; the national average for cybersecurity jobs is only 1.8.

12 Average advertised salary listed in online job openings from June 2019 through May 2020 (data collected on October 7, 2020), https://www.cyberseek.org/pathway.html

13 Job Openings by NICE Cybersecurity Framework Category (data collected on October 7, 2020), https://www.cyberseek.org/heatmap.html

Figure 1: Job Openings by NICE Cybersecurity Framework Category

June 2019 through May 2020



(Data collected on October 7, 2020), https://www.cyberseek.org/heatmap.html

Recruiting Cybersecurity Talent

How PUCs target their recruitment efforts will depend on the level of cybersecurity talent they are attempting to hire. A cybersecurity professional's ideal characteristics will differ based on their level of experience in the cybersecurity industry. A candidate's experience level will also indicate appropriate recruitment pipelines, what attracts them to government service, and challenges PUCs may face as they recruit qualified talent. As expected, entry-level talent will likely be searching for their first job, mid-level talent should have at least a few years of relevant experience, and director-level talent should be experts in their field. The matrix outlined in Table 5 identifies recruitment considerations for each level of cybersecurity professional, and Table 6 identifies possible pipelines for recruitment.

Sample job postings for each level (including an internship-level position for long-term recruitment efforts) are in Appendix A. It is vital to include a thorough description of the desired roles and responsibilities for each position. If publicly available, consider including references to your PUC's cybersecurity strategy or cybersecurity risk assessment methodology to provide candidates with an understanding of the commission's expectations for the position.

Table 5: Recruiting Cybersecurity Talent

Level	Ideal Characteristics	What Attracts Candidates?	Recruitment Challenges
Director-Level	• 10+ years of experience in cybersecurity operations/maintenance • Looking for a career change or new challenge • Experience working closely with or for the government • Has an interest in developing or expanding oversight and governance programs • Has a basic understanding of utility operations and regulations • Ability to obtain and maintain a security clearance • Experienced auditor or a regular auditee	• A positive work/life balance. Many private-sector cybersecurity experts feel overworked • An opportunity for a new environment and challenge • Career progression opportunity • Sense of civic duty	• Difficult to compete with salaries offered by the private sector • State government protocols are relatively rigid compared to the private sector (i.e., leaders typically need approval before instituting new policies) • Some states may have civil service eligibility requirements, while others will not • Low supply of cybersecurity workers compared to demand
Mid-Level	• 5+ years of experience in cybersecurity operations/maintenance • Holds a cybersecurity-related degree and certifications—or—no cybersecurity degree but transitioned into the industry and holds cybersecurity certifications with years of experience in the field • Strong operational skills, including knowledge of hardware, software, networks, and data centers • Familiarity with utility regulatory principles and government protocols • Has specific knowledge related to operational technology (OT) networks • Experienced auditor or a regular auditee	• Continuous training and certification opportunities • Security of a government job • Opportunities for advancement • A positive work/life balance. Many private-sector cybersecurity experts feel overworked • Sense of civic duty	• Difficult to compete with salaries offered by the private sector • Hiring within civil service eligibility requirements • Low supply of cybersecurity workers compared to demand
Entry-Level	• Recent graduate with a cybersecurity-related degree or equivalent, or in other areas of study, including accounting, public administration, and law • Holds cybersecurity certifications • Mid-level professional who has transitioned into the cybersecurity field • Has an understanding of cybersecurity operations and maintenance techniques, but has a primary interest in cybersecurity oversight and governance • Displays high levels of aptitude, curiosity, and perseverance	• Continuous training and certification opportunities • Security of a government job • Opportunities for advancement • Opportunity to learn how a broad range of organizations approach cybersecurity issues • Sense of civic duty	• Difficult to compete with salaries offered by the private sector • Difficult to compete with amenities and nonmonetary benefits offered by tech firms • Low supply of cybersecurity workers compared to demand • Hiring within civil service eligibility requirements

Table 6: Recruitment Pipelines[14]

Level	By Talent Level	For All Talent Levels
Director-Level	• Cybersecurity divisions of other state agencies, municipalities, or other states • Military job fairs • Cybersecurity directors within the private sector • Energy consulting firms • Utility professionals	• PUC and State Job Boards • Word of mouth • NARUC Job Board • Women in Cybersecurity (WiCyS) Job Board • Minorities in Cybersecurity (MiC) Job Board • Society of Women Engineers (SWE) Job Board • Society for Advancement of Chicanos/Hispanics & Native Americans in Science (SACNAS) Job Board • LinkedIn • Indeed • Monster • Glassdoor
Mid-Level	• Cybersecurity divisions of other state agencies, municipalities, or other states • Military job fairs • Professionals in mid-/entry-level positions across public and private sectors • Energy consulting firms • Utility professionals • National Cybersecurity Training & Education (NCyTE) Center • Young Professionals in Energy (YPE) Job Board	
Entry-Level	• Recent graduates from Centers for Academic Excellence (CAE-C) • CAE-C Community Job Fairs • "CyberCorps®: Scholarship for Service" recipients • U.S. Department of Energy's CyberForce Competition • NCyTE Center • YPE Job Board • PUC Internship or Fellowship Programs (can target CAE-C programs)[15]	

Retaining Cybersecurity Talent

The cybersecurity realm continuously adapts and evolves as technology improves and becomes more sophisticated. Beyond compensation and common employer benefits, research shows that cybersecurity professionals generally stay with employers who offer continuous training/certification opportunities, take their opinions/suggestions seriously, provide a positive work/life balance, and offer opportunities for promotion/career advancement.

- **Offer Continuous Training/Certification Opportunities:** Especially valid for cybersecurity professionals toward the beginning of their careers, opportunities to obtain additional training, certifications, or recertification paid for by their employer is a crucial retention tool. The tactics used by malicious cyber actors continue to adapt and evolve, and so should cybersecurity professionals' skills. Other opportunities include attending cybersecurity-related conferences to maintain an awareness of current trends and network with peers in the industry. Regular training will lead to more competent staff and help them reach their career potential.

14 An annotated list of cybersecurity workforce recruitment pipelines is located in Appendix B. This table is not an exhaustive list of relevant job boards or pipelines to find cybersecurity talent.

15 An example job description for a Cybersecurity Intern (or Fellow) is located in Appendix A. Hiring interns is a long-term recruitment strategy to build interest.

- **Take their Opinions/Suggestions Seriously:** All employees want their ideas taken seriously, and cybersecurity professionals are no exception. According to a 2017 survey, 36 percent of cybersecurity professionals believe that high Chief Information Security Officer (CISO) turnover in the private sector is caused by a lack of organizational culture that emphasizes cybersecurity, and 34 percent believe CISOs leave because they are not an active participant with executive management or the board of directors.[16] Translated to a PUC perspective, a positive culture of trust between PUC leadership and cybersecurity professionals within the PUC is vital. As cybersecurity becomes more widely recognized as a critical issue, organizations will need to embrace that reality and foster trust to retain qualified cybersecurity talent.
- **Provide a Positive Work/Life Balance:** Many cybersecurity professionals within the private sector often experience burnout by spending an extraordinary amount of time working late evenings and weekends to keep up with a demanding workload.[17] Although cybersecurity professionals within PUCs rarely work nights and weekends at the same scale as private sector employees, they may be called upon off-hours in the event that a cybersecurity incident occurs within a utility or their own network. To avoid burnout, finding innovative ways to ensure current employees have a positive work/live balance is one way to retain qualified cybersecurity talent. For example,
    - Identify multiple individuals to alternate "on-call" weekends in case of an emergency so employees can fully enjoy their time off.
    - Encourage employees to utilize their paid time off (PTO). State government PTO policies are typically generous.
    - Allow employees to work flexible hours.
    - Allow employees to work from home on specific days of the week. The average American commute is 26.9 minutes, which would give an employee 53.8 minutes of personal time back per day.[18]
- **Communicate Opportunities for Promotion/Career Advancement:** Cybersecurity professionals, like other professionals, are drawn to positions with opportunities for promotion or career advancement. PUCs should ensure that promotion and advancement opportunities are regularly communicated to current staff who are interested and eligible.
- **Appeal to their Sense of Civic Duty:** Typically used as a recruitment tool, regularly acknowledging and appealing to employees' sense of civic duty is one way to ensure they remain interested in the organization's mission. Take time to recognize the importance of all employees' work and how it benefits the state's citizens. Reminding people that what they do makes a difference is a compelling reason to continue working on behalf of the people.

Beyond these proactive approaches, emphasize the value of exit interviews from employees who previously left the PUC and consider innovative ways to address negative comments from those interviews. Consider monitoring employee reviews on Glassdoor[19] or Indeed[20] to evaluate possible solutions and institute

16 The Life and Times of Cybersecurity Professionals, https://www.esg-global.com/hubfs/issa/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Nov-2017.pdf?hsCtaTracking=a63e431c-d2ce-459d-8787-cc122a193baf%7Ce74f0327-0bbc-444a-b7a8-e2cd08d1999e

17 "According to a survey of 360 information security professionals at Infosecurity Europe 2017 by Farsight Security, 57 percent work weekends and, on average, nearly a third (29 percent) work ten hours a day. Also, more than half (51 percent) of respondents said that they had missed an important event due to a security-related incident at work more than once," https://www.infosecurity-magazine.com/news/security-professionals-weekend/

18 Mean travel to work (minutes), workers age 16 years+, https://www.census.gov/search-results.html?q=Average+Commute+Time+Census&page=1&stateGeo=none&searchtype=web&cssp=SERP

19 Glassdoor Company Reviews, https://www.glassdoor.com/Reviews/index.htm

20 Indeed Company Reviews, https://www.indeed.com/companies?from=gnav-acme--acme-webapp

improvements when appropriate. Negative reviews on these sites may prevent qualified candidates from applying, so implementing a strategy to address them is crucial for brand management purposes.

Alternatives to Hiring In-House Cybersecurity Talent

Some PUCs might find the hurdles to hiring skilled cybersecurity talent too formidable and pursue cybersecurity subject matter expertise through other avenues. Alternatives to hiring include retraining current PUC staff to perform cybersecurity duties, contracting with expert consultants, and leveraging cybersecurity expertise resident within other state agencies. Each of these options is discussed next.

Train Current PUC Staff

The nationwide shortage of cybersecurity professionals has led to an interesting phenomenon—people "accidentally" transitioning into cybersecurity careers within their organizations,[21] especially those who are tech-savvy already or possess strong analytical skills. When considering hiring alternatives, PUCs may find that current staff members have cybersecurity aptitude. Pursuant to civil service hiring requirements, PUCs can identify interested personnel and provide training to build foundational cybersecurity skills. A wide range of free and paid training options exist; Appendix B includes an annotated list of available opportunities.

Note that the degree to which this option is worthwhile depends on the PUC's strategy and cybersecurity goals. For example, a novice skill set may be satisfactory to verify whether utilities have met predefined cybersecurity requirements or determine if performance metrics have been satisfied. If the role requires more direct engagement with utilities—to discuss and assess the sufficiency of their cybersecurity risk management efforts, for example—hiring a more seasoned professional would be more appropriate.

Pros:

- Employee already familiar with the PUC and regulatory principles
- No additional in-house hiring needed

Cons:

- Cybersecurity training is required, which takes time, effort, and in many cases, financial investment
- No real-world experience with cyber systems in a utility
- May overload current employee
- Hiring consultants may still be necessary

An employee's workload and level of interest in cybersecurity work should be considered before assigning new responsibilities and investing in training. In some cases, employees may begin training and decide that cybersecurity is no longer of interest. While the position would remain unfilled, this should not be considered a failure. Even if the trained individual decides that cybersecurity is no longer of interest, the PUC will benefit by gaining an employee in a noncyber division who is now more conscious of cybersecurity risks at the PUC and their regulated utilities. In other cases, an employee may take advantage of cybersecurity training opportunities and end up leaving for a higher paying job in the private sector. To mitigate this risk, consider options to increase compensation in step with increased cybersecurity knowledge or certifications.

Also, consider instating a formal or informal mentorship program for new team members within the cybersecurity division. Current PUC employees are likely familiar with the PUC as an organization, but would benefit from a mentor to help bring them up to speed on the cybersecurity division's efforts and protocols.

21 Rise of the "accidental" cybersecurity professional, https://www.techrepublic.com/article/rise-of-the-accidental-cybersecurity-professional/

Hire Consultants

PUCs hire cybersecurity consultants to perform a variety of tasks. Tasks can range from developing a single product to serving a long-term supporting role with regular responsibilities defined within a contract. A PUC might hire consultants to conduct specific studies on behalf of the commission or provide subject matter expertise to commissioners during a cybersecurity-related rate case. Hiring in-house cybersecurity professionals and hiring outside consulting services are not mutually exclusive options.

In-house cybersecurity personnel may benefit from additional support through consulting services on an as-needed basis. Consultants can perform or assist in-house PUC staff as they perform cybersecurity audits or assessments of utility operations, manage cybersecurity reporting mechanisms, and advise the PUC on cybersecurity standards and rate setting decisions. If consultants work directly with utilities in any of these respects, consider in advance how forthcoming or frank your regulated utilities might be with a third party, especially about potentially sensitive cybersecurity information.

Pros:

- Flexible commitment based on contract
- External support and advice typically exceeds the PUC's internal capacity
- Consultants may have insight into effective cybersecurity practices in other states

Cons:

- Consultants may not be appropriately familiar with PUC processes, such as contested rate cases
- Limited tasks and functions
- Difficult for consultants to build trust with utilities
- Personnel turnover within consultant firms
- Can be costly

Share Resources with Other State Agencies

Resource constraints may prohibit a PUC from hiring full-time cybersecurity talent or hiring consultants. In-house cybersecurity personnel may benefit from additional support through consulting services on an as-needed basis. In those cases, there may be cybersecurity professionals within other state agencies who can assist on an as needed basis through a memorandum of understanding or otherwise established mechanism. For example, Connecticut's Public Utilities Regulatory Authority (CT PURA) does not have a cybersecurity expert on staff but utilizes cybersecurity experts within the Connecticut Intelligence Center Unit (CTIC; state fusion center) to assist during annual cybersecurity reviews of regulated utilities. There is no official memorandum of understanding between CT PURA and CTIC to support this work. The partnership initially began informally as a result of both agencies' participation in a state-wide Cyber Security Committee.[22] Since then, a formalized "Public Utility Company Cybersecurity Oversight Program" was established as part of CT PURA's cybersecurity action plan. Under this program, representatives from CT PURA, CTIC,[23] and other state agencies hold voluntary reviews with utility companies on an annual basis to discuss their "(1) cyber defense programs, (2) cyber threat experiences over the prior year, and (3) anticipated corrective measures."[24]

Pros:

- Already familiar with government protocols
- Other state agencies may be able to advise utilities on unique risks
- Cost-effective or free depending on agreement
- Can lead to other useful cybersecurity collaboration

Cons:

- PUC cannot control workload or schedule
- May need education on basic regulatory principles

22 Connecticut Cyber Security Committee, https://portal.ct.gov/DEMHS/Homeland-Security/Cybercrimes-and-Cybersecurity

23 CTIC is organizationally housed within Connecticut's Division of Emergency Management and Homeland Security.

24 Cyber Threats and Cybersecurity Report, Connecticut General Assembly (2019-R-0047), https://www.cga.ct.gov/2019/rpt/pdf/2019-R-0047.pdf

Other PUCs can apply the CT PURA model to enhance their cybersecurity expertise without hiring in-house professionals or costly consultants. Many state agencies already employ cybersecurity professionals, but they may need basic training on regulatory basics to ensure that they do not cross any regulatory lines if posing questions to utilities about their cybersecurity operations. The following state agencies may already employ cybersecurity professionals who could provide value to a PUC:

- State Fusion Centers[25]
- National Guard Cybersecurity Units[26]
- State and Territory Energy Offices[27]
- State Information Offices[28]
- State Emergency Management Agencies[29]
- State Homeland Security Departments[29]
- Governor's Offices

Summary

Cybersecurity professionals are rare, yet more than ever, PUCs recognize the need to have access to this expertise. Many seek to hire full-time cybersecurity professionals, but competition is fierce. When making hiring decisions, PUCs must balance their expectations against factors such as: available recruitment pipelines, long-term professional development needs, and other retention issues. Alternatives to hiring in-house expertise may be more practical for some PUCs because of limited staff time or resources, and special consideration should be given to sharing resources with other state agencies to acquire the right cybersecurity expertise. Moreover, as PUCs explore building or expanding their cybersecurity programs, the support of PUC leadership is a critical component to acquiring and retaining dedicated professionals to successfully meet their cybersecurity goals.

25 Fusion Center Locations and Contact Information, https://www.dhs.gov/fusion-center-locations-and-contact-information

26 National Guard Cyber Units operate in at least 38 states, https://www.lawfareblog.com/hybrid-benefits-national-guard

27 NASEO State and Territory Energy Offices, https://www.naseo.org/members-states

28 State Chief Information Officers, https://www.nascio.org/member-profiles/

29 State Homeland Security and Emergency Services, https://www.dhs.gov/state-homeland-security-and-emergency-services

Appendix A: Compendium of PUC Cybersecurity Job Descriptions

In coordination with PUCs, NARUC compiled the following compendium of cybersecurity job descriptions used in PUCs today. These are provided as examples, which can be tailored to fit individual PUC needs.

Example Language to Excite Candidates

The general public is likely unfamiliar with the role of PUCs. Therefore, qualified applicants may be hesitant to invest time into an application if they know nothing about the organization's role, mission, and how the position aligns with their career interests. The following language can be included with job postings (or listings) to excite candidates about the opportunity.

Example Descriptors:

- The *[Public Utility Commission]* has an exciting new opportunity for a full-time *[position title]* in *[city, state]*. As outlined by state statute, the commission's primary responsibility is to regulate the state's electric, natural gas, telecommunication, water, and sewer utilities. The commission's mission is to ensure reliable access to affordable energy that citizens rely on for every facet of their lives. As a commission employee, you'll have an opportunity to contribute to this mission, fulfill a sense of civic duty, and make a lasting impact on the energy industry.
- The *[Public Utility Commission]* is consistently ranked in the top five state agencies to work for, according to the [source]. Within subrankings, the commission is regularly ranked #1 for encouraging a positive work/life balance.[A1] The commission cares about its employees and their career aspirations. Through an array of state-sponsored benefits, employees can take advantage of mentorship programs, paid training opportunities to hone their skills, and maintain priority for other state positions over the general public.
- A position with the *[Public Utility Commission]* offers cybersecurity talent a way to fulfill their sense of duty to public service and contribute to a government mission. The criticality of utility services to the life, health, and well-being of the public is becoming more apparent. Employment at the commission lets cybersecurity professionals contribute to the resiliency of critical infrastructure. In fact, because of the breadth and depth of regulatory authority conferred on the commission, cybersecurity professionals at the commission can make an outsized impact compared to the private sector. The limited number of employees at the commission gives new hires at any career level an opportunity to interact and learn from people at high levels of public and private sector organizations. There can also be a sense of satisfaction working on behalf of the people of the community.

A1 The Federal Energy Regulatory Commission (FERC) regularly uses their standing as the #1 ranked midsized agency in the Best Places to Work rankings to recruit qualified candidates. Source, https://www.ferc.gov/about/careers/why-choose-ferc.

Director, Office of Cybersecurity Compliance and Oversight

Level: Director-Level
Job Title: Director, Office of Cybersecurity Compliance and Oversight

THE POSITION

The commission is seeking a highly motivated, experienced, and hardworking individual to fill the role of Director, Office of Cybersecurity Compliance and Oversight (OCCO). Directing the Office of Cybersecurity Compliance and Oversight at the [state]'s public utility commission is a challenging, yet rewarding, position that allows you to build a better and more secure tomorrow. In this role, you'll lead a team of cybersecurity professionals and regulatory oversight programs to help protect utilities from cyberattacks to ensure adequate, safe, and reliable public utility services to consumers. This position reports directly to the commission's Executive Director and is expected to regularly advise Commissioners on policy and investment strategies to mitigate cybersecurity vulnerabilities within regulated utilities.

DESCRIPTION OF WORK

The qualified candidate will perform the following functions:

- Work closely with the Executive Director and Commissioners on policy issues involving cybersecurity oversight functions of regulated utilities.
- Provide expert advice to commission executive and bureau staff on cybersecurity matters.
- Lead the commission's Cyber Team, a multibureau working group composed of technical, policy, legal, and communications staff responsible for designing, implementing, and maintaining a compliance and oversight program of cybersecurity regulatory functions for electric, natural gas, water, wastewater, telecommunications, and transportation utilities.
- Engage in communication and coordination with relevant external stakeholders.
- Develop team goals, define performance metrics, and provide oversight and reporting to management.
- Work is performed independently and is evaluated and reviewed by the Executive Director and Commissioners through periodic conferences and written reports.

REQUIRED EXPERIENCE, TRAINING & ELIGIBILITY

- A bachelor's degree in any IT field, and 5+ years of experience performing technical work in cybersecurity program management or IT security.
- Possession of a certification as a Certified Information Systems Security Professional (CISSP) by the International Information Systems Security Certification Consortium or Certified Information Security Manager (CISM) by the Information Systems Audit and Control Association.

Cybersecurity Analyst Program Specialist VI–VII

Level: Mid-Level
Job Title: Cybersecurity Analyst Program Specialist VI–VII

GENERAL DESCRIPTION

As a Cybersecurity Analyst Program Specialist, you will play a key role in overseeing the development of new regulatory policies and procedures that will have a lasting impact on the security of services that citizens rely on for every facet of their lives. Among other tasks, you will perform highly advanced work on issues that concern security activities of electric, telephone, and water and sewer utility operations, with a focus on cybersecurity in the Critical Infrastructure Security and Risk Management division. Work involves reporting on issues that concern cybersecurity, physical security, and homeland security activities of utilities. Work under minimal supervision with considerable to extensive latitude for the use of initiative and independent judgment.

ESSENTIAL FUNCTIONS

- Make recommendations and advise the Division Director and public utility commission (PUC) staff on issues involving cybersecurity for electric, telephone, and water and sewer utility operations.
- Assist with updating energy assurance and emergency management rules and plans to incorporate cybersecurity.
- Analyze cybersecurity utility initiatives for best practices and risk-based access controls.
- Provide information to utilities and the public regarding commission rules, policies, and requirements as they relate to cybersecurity, physical security, and homeland security activities.
- Make recommendations concerning proposed rules and amendments to rules as they relate to cybersecurity, physical security, and homeland security activities.
- Assist in developing recommendations for a cybersecurity program that includes a process for monitoring threats, increasing awareness, and developing contacts with utilities to share information.
- Stay up-to-date on cybersecurity, physical security, and other homeland security issues as they affect the electric, telecommunications, and water and sewer utility industries.
- Research cybersecurity and privacy legislation, regulations, advisories, alerts, and vulnerabilities.
- Research and analyze cybersecurity threat indicators and their behaviors.
- Participate with electric utilities and the state operations center on drills and exercises designed to test cybersecurity and emergency preparedness.
- Participate in PUC-related homeland security activities.
- Participate in emergency management activities of the commission's Emergency Management Response Team.
- Participate in investigations and the preparation of reports.
- Participate in activities conducted by the regional reliability organization and federal and state agencies.

MINIMUM QUALIFICATIONS

- Graduation from an accredited four (4) year college or university with a bachelor or postgraduate degree in public policy, homeland security, business administration, information technology (IT), engineering, economics, energy resource economics, or related field.
- Program Specialist VI—minimum of one (1) year of full-time work experience in a position involving

utilities, cybersecurity analysis, information security analysis, homeland security, or regulatory analysis.

- Program Specialist VII—minimum of three (3) years of full-time work experience in a position involving utilities, cybersecurity analysis, information security analysis, homeland security, or regulatory analysis.

PREFERRED QUALIFICATIONS

- Professional certifications, such as: SEC+, CEH, CCNA CISSP, GCIP, GRID, or GICSP.

KNOWLEDGE, SKILLS AND ABILITIES

- Knowledge of cybersecurity and information security controls, practices, procedures, and regulations; and of incident response program practices and procedures.
- Strong IT skills including knowledge on hardware, software, networks, and data centers.
- Critical thinking skills, problem-solving aptitude.
- Public speaking and presentation skills.
- Ability to analyze complex security issues in diverse and decentralized environments.
- Ability to manage multiple concurrent objectives, projects, groups, or activities, making effective judgments as to prioritizing and time allocation.
- Ability to effectively communicate complex concepts orally and in writing.
- Ability to assimilate and use diverse, complex information to advance the commission's goals.
- Ability to work harmoniously with commission personnel, industry stakeholders, customers, personnel of the legislature, other government agencies, and the public.

Utility Cybersecurity Specialist

Level: Mid-Level
Job Title: Utility Cybersecurity Specialist

GENERAL SUMMARY OF FUNCTION/PURPOSE OF POSITION

The Utility Cybersecurity Specialist is responsible for the commission's Cybersecurity Program, including drafting and executing the commission's cybersecurity rules, engaging industry leaders through annual meetings and reporting, collaborating with cybersecurity subject matter experts from government and industry, researching cybersecurity threats and vulnerabilities, and liaising with critical cybersecurity personnel at utilities. The specialist is responsible for advising the commission on state and federal policy or laws regarding cybersecurity and advising the agency on appropriate regulatory approaches to improve the planning, response, recovery, and mitigation of potential cybersecurity incidents at energy providers serving the state.

The position also works with state partners to build a Statewide Energy Sector Infrastructure Committee, acts as a backup emergency management coordinator at the State Emergency Operations Center (SEOC), and will represent the commission on national associations addressing cybersecurity and critical infrastructure protection.

GENERAL SUMMARY OF DUTY 1 (60% of Time)

Serve as the commission's cybersecurity subject matter expert. Develops and implements the commission's cybersecurity program in a manner consistent with federal and state guidelines and frameworks. Facilitates the commission's cybersecurity rulemaking process to ensure accountability, preparedness, and response capabilities of utilities. Serves as cybersecurity liaison to the energy industry and affiliated stakeholders. Researches and evaluates complex cybersecurity threats and vulnerabilities facing the energy industry, and maintains knowledge of state and federal issues that overlap between the commission and critical partner's interest/responsibilities.

Individual Tasks Related to Duty 1

- Serve as technical advisor to Commissioners and staff in the event of a cybersecurity emergency/incident affecting critical energy infrastructure assets that may contribute to a disruption of energy supplies within the state.
- Interpret existing and proposed policies, procedures, rules, and guidelines as they relate to cybersecurity and critical infrastructure protection.
- Develop and implement the commission's cybersecurity program in coordination with commission goals and objectives. Ensure coordination of agency cybersecurity policy and plans with existing state and federal guidelines.
- Facilitate the commission's cybersecurity rule-making process to ensure accountability, preparedness, and response capabilities of utilities.
- Assess general response, recovery, prevention, protection, and mitigation capabilities of electric and natural gas providers through annual meetings and review of Cybersecurity Management Plans. Make recommendations for improvement, as appropriate.
- Collect and maintain schedules, records, and determinations of annual meetings; Aggregate data into annual cybersecurity report for Commissioners.
- Research and analyze the various applicable cybersecurity standards and guidelines (i.e., NERC CIP, NIST) that are created by standards development organizations and utilized by utilities through their cybersecurity management plans.

- Serve as cybersecurity liaison to electric and natural gas utilities, state partners, and other critical energy infrastructure owners and operators as they address their cybersecurity challenges.
- Represent the commission at cybersecurity trainings and conferences. Design and develop applicable professional presentations.
- Evaluate customer inquiries and complaints regarding cybersecurity within the electric and natural gas sectors and determine potential violations of commission rules or state privacy and data protection standards.
- Recommend updates to cybersecurity section of the state's Energy Assurance Plan.

GENERAL SUMMARY OF DUTY 2 (20% of Time)

Collaborate with critical partners to design and implement the Energy Sector Infrastructure Committee; research and provide guidance on data required for the Critical Energy Infrastructure Information Database, design, and implement spatial data tracking system at the commission.

Individual Tasks Related to Duty 2

- Research and collect information related to the ownership and management of critical energy systems and the negative consequences of each system failure.
- Develop process to digitally map the state's energy infrastructure in a manner consistent with the goals and objectives of the commission.
- Work with the state partners and industry owners and operators to develop energy system profiles for each of the primary natural gas, electric, and petroleum systems within the state.
- Collaborate with Local Energy Assurance (LEAP) planning team to facilitate critical energy infrastructure data sharing and protection.
- Represent the commission at energy sector meetings.

GENERAL SUMMARY OF DUTY 3 (10% of Time)

Represent commission as a backup emergency management coordinator (1 of 3). Serve on the commission's Energy Emergency Response Team.

Individual Tasks Related to Duty 3

- Maintain certification in applicable Incident Command System (ICS) courses offered by FEMA.
- Serve as on-call State Emergency Operations Center (SEOC) representative approximately one weekend per month.
- Participate in energy emergency exercises and training.

GENERAL SUMMARY OF DUTY 4 (10% of Time)

Other duties as assigned by the manager or agency director.

Individual Tasks Related to Duty 4

- Preparing special statistical or economic analyses at the request of others in the commission.
- Participate and present at state and national conferences.
- Evaluate proposed laws, plans, and resolutions (from National Association of Regulatory Utility Commissioners, U.S. Department of Homeland Security, U.S. Department of Energy, etc.) and prepare interpretations and comments when appropriate.

MINIMUM EDUCATION AND EXPERIENCE QUALIFICATIONS

Education

- Bachelor's degree, with a preferred major in engineering or computer science. Certificate or knowledge of cybersecurity and knowledge of utility infrastructure is a plus.

Experience

- 2–5 years of professional experience, including one year of experience equivalent to the intermediate level in state service.

Knowledge, Skills, and Abilities

- Excellent communications skill, both written and oral. Ability to plan and undertake research, use technical research methods, and prepare a formal report. Strong analytical skills along with ability to formulate procedures and analyze and appraise issues to make effective recommendations. Good public relations skills. Proficient computer skills, including Microsoft Word, Excel, PowerPoint, and the ability to learn other software as needed.

Public Utilities Regulatory Analyst III

Level: Mid-Level
Job Title: Public Utilities Regulatory Analyst III

GENERAL SUMMARY

This position is located in a new cybersecurity branch within the public utility commission. Applicants must have a strong passion for cybersecurity and possess the drive needed to establish a new program, build interagency relations, and network with limited oversight. Candidates must be innovative, and able to invest the time needed to design, build, and grow the branch. The selected candidate will have access to continuous training and other career advancement opportunities.

ESSENTIAL FUNCTIONS

- Research, analyze, develop, and propose methods and tools to evaluate the effectiveness of utility cybersecurity programs. Identify best practices pertaining to utility cybersecurity and propose standards, regulations, or policies that should be considered for adoption by the commission.
- Support the Program Manager in establishing and maintaining partnerships with federal, state, and industry organizations that focus on utility cybersecurity including, but not limited to, U.S. Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), Cyber Information Sharing and Collaboration Program (CISCP), Electricity Subsector Coordinating Council (ESCC), the State's Office of Emergency Services, the State Department of Technology, and the State Cybersecurity Task Force.
- Develop and maintain expertise in utility cybersecurity best practices. Maintain an inventory of latest standards and best practices in utility cybersecurity, such as the Cybersecurity Primer issued by National Association of Regulatory Utility Commissioners (NARUC), North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standard, and others. Analyze data provided by utilities, such as reports pertaining to cybersecurity programs and information provided in testimony and briefings as part of commission proceedings.
- Assist with the establishment of the Utility Cybersecurity Branch and development of the utility cybersecurity program. Support Program Manager in analyzing and developing internal policies, procedures, methods, and tools for the functioning of the utility cybersecurity program.
- Attend meetings; represent the commission before various public agencies and the legislature; provide presentations to management, industry groups, and government representatives. Conduct workshops and help coordinate efforts with a wide variety of industry stakeholders.

ADDITIONAL DUTIES

- The analyst performs key analytical work of the cybersecurity branch, with a specific focus on development of the methods and tools to evaluate the effectiveness of utility cybersecurity programs. This is a new program being created to address cybersecurity risks to utility infrastructure. Under the direction from the Program Manager, the analyst will perform the analytical work required to support development of a utility cybersecurity policy at the commission, such as identifying best practices and evaluating regulations adopted by other states. The analyst will develop and maintain expertise in utility cybersecurity policy and best practices, help establish the utility cybersecurity program, and perform ongoing analytical work as the program matures.

KNOWLEDGE AND ABILITIES

- **Knowledge of:**
  - Trends and issues pertaining to public utilities and transportation regulations;
  - Principles of program evaluation and planning;
  - Principles and concepts of economics,
  - Statistics and finance in a research setting;
  - Public utilities regulatory policy analysis and formulation;
  - Federal and state agencies involved in utilities regulation;
  - Federal and state legislation and policies pertaining to public utilities; and
  - Utility general rate cases.
- **Ability to:**
  - Reason logically and creatively;
  - Utilize a variety of analytical and research techniques to resolve complex utility and transportation regulatory problems;
  - Develop and evaluate alternatives;
  - Analyze data and present ideas and information effectively;
  - Both orally and in writing; testify as a subject-matter expert;
  - Consult with and advise Commissioners, top management, and other interested parties on a wide range of issues relating to public utilities regulations;
  - Coordinate the complex technical work of others;
  - Serve as a team leader to analyze the more technical and difficult situations;
  - Establish and maintain project priorities; and
  - Analyze situations accurately and take effective action.

Cybersecurity Analyst I

Level: Entry-Level
Job Title: Cybersecurity Analyst I

GENERAL DESCRIPTION

Joining the public utility commission (PUC) means being part of the team focused on securing the state's critical infrastructure, and more broadly, national security. Within the PUC, the Cybersecurity Division leads cybersecurity programs and initiatives in collaboration with partners in the federal government, other state agencies, and regulated utility service providers. As a Cybersecurity Analyst, you'll have the opportunity to grow your career through continuous training opportunities, learn how a broad range of organizations approach cybersecurity issues, and fulfill a sense of civic duty.

ESSENTIAL FUNCTIONS

- Analyze cybersecurity programs by assisting with researching new solutions for emerging cybersecurity threats.
- Research cybersecurity tools and techniques.
- Participate in the creation of cybersecurity materials, including training documents, risk assessment tools, cybersecurity guidance planning templates, etc.
- Provide input in the development of policies and procedures to enhance the internal cybersecurity of the PUC.
- Provide input in the development of policies and procedures to enhance the cybersecurity of utilities regulated by the PUC.
- Implement policies or procedures and track internal/external cybersecurity compliance.
- Assist in the sharing of cybersecurity threat information with government and industry partners.
- Coordinate cybersecurity-focused tabletop exercises with key utility partners.
- Assist or lead special studies and projects.
- Prepare written correspondence and other documentation.

PREFERRED EXPERIENCE

- 0–2 years' experience in a cybersecurity role.
- Experience with risk management frameworks or cybersecurity maturity models.

EDUCATION

One or more of the following:

- Associates degrees in accounting, cybersecurity, information technology (IT) security, management information systems, application development, or computer networking along with cybersecurity certifications or work experience in a cybersecurity field.
- Military training in cybersecurity or IT security.
- BA or BS in a technical discipline. Cybersecurity coursework preferred.

CERTIFICATION/LICENSES

The following certifications can be substituted for or complement educational requirements:

- CompTIA Security+ (Must Have)
- Certified Information Systems Security Professional
- Certified Information Systems Auditor
- Certified Information Security Manager
- Certified Ethical Hacker

KNOWLEDGE, SKILLS, AND ABILITIES

- Awareness of information security, IT audit, and IT risk management principles. Basic understanding of management audit procedures. Excellent written and oral communication skills. Ability to draft formal reports for senior leadership review. Advanced computer skills, including Microsoft Word, Excel, PowerPoint, and the ability to learn other software as needed. Ability to work cohesively within a small team of cybersecurity subject matter experts. Ability to interact with others in a professional manner and develop relationships with utility partners.

Departmental Analyst

Level: Entry-Level
Job Title: Departmental Analyst

GENERAL SUMMARY OF FUNCTION/PURPOSE OF POSITION

At the entry level, the analyst will perform cybersecurity and IT analysis for commission oversight of regulated utility and nonutility cyber security management systems and cost recovery of such investments by regulated utilities through the rate case process. These duties will include research and analysis of cybersecurity management plans and the various interoperability standards for such technologies. This position will monitor the utility's performance through a combination of NERC-CIP security compliance review, review of annual reports and audit reports, review of compliance to various other standards, and analysis of risk assessment practices. In addition to continuous training and certification opportunities, the selected candidate will be paired with an experienced mentor to learn how a broad range of organizations approach cybersecurity.

GENERAL SUMMARY OF DUTY 1 (50% of Time)

Research and review of specific company cybersecurity management systems by regulated electric and natural gas utilities in rate case proceedings. Including research and analysis to determine the impact and cost benefit of cybersecurity programs on the existing electric system.

Individual Tasks Related to Duty 1

- Researches and conducts review including detailed analysis of the performance of the electric and natural gas provider's Cybersecurity Management Plan to obtain information, summarize, and make recommendations to the manager as appropriate.
- Review/evaluate cost and performance estimates for cybersecurity plans that focus on the reliability, resiliency, and safety of critical infrastructure. Compare costs and performance criteria to traditional electric system operations and performance.
- Develop system performance estimates to determine the impact of NERC-CIP standards and specifications on the current electric and gas systems.
- Develop an understanding of the various applicable cybersecurity standards that are created by standards development organizations and utilized by regulated utilities through their management system plans.
- Research and conduct on studies of cybersecurity attacks on utility systems.

GENERAL SUMMARY OF DUTY 2 (30% of Time)

Provide research and analysis support for rate cases in the Operations and Wholesale Markets Division. Prepare testimony and recommendations as part of rate recovery cases for cybersecurity investments by regulated utilities.

Individual Tasks Related to Duty 2

- Develop spreadsheets and/or databases for monitoring utility cybersecurity investments.
- Serve as a case coordinator for electric and gas providers in commission cases involving cybersecurity.
- Provide reports and recommendations to manager on any of the above activities as assigned.
- Examine technical, cost, and other data including commission annual reports, NERC-CIP guidelines, audit reports and risk assessment, and recommendations to the Manager as appropriate.
- Work as a liaison with unregulated utilities and other critical infrastructure providers as they address their cybersecurity challenges and solutions.

GENERAL SUMMARY OF DUTY 3 (10% of Time)

Assist with the preparation of exhibits and expert testimony covering security matters related to contested case proceedings on rate recovery cases before the commission.

Individual Tasks Related to Duty 3

- Assist Manager and senior staff with preparation of written expert testimony regarding cybersecurity and physical security threats to the electric or gas systems before the public service commission (PSC) and testify in PSC proceedings regarding rate recovery proceedings.
- Review testimony regarding the above energy issues prepared by other expert witnesses submitted to the PSC and advise Staff Managers and Attorneys regarding such issues and provide plan issues for purposes of discovery, cross-examination, and preparation of case documents.

GENERAL SUMMARY OF DUTY 4 (10% of Time)

Other duties as assigned.

Individual Tasks Related to Duty 4

- Prepare and make presentations explaining cybersecurity targets on utility information technology systems, supervisory control, and data acquisition systems and the smart grid.
- Handle customer inquiries regarding cybersecurity electric and gas issues.
- Work with regulated utilities and staff to improve situational awareness.
- Conducts field investigations related to cybersecurity of regulated utilities to impact on grid reliability and resiliency.

FUNCTION OF THE WORK AREA AND HOW THIS POSITION FITS

- The Energy Data & Security Section is responsible for energy data research and statistical analysis and assuring the reliability and security of the state's energy needs. This includes: tracking the adequacy of the state's energy supply; preparing energy and utility forecasts; monitoring heating oil and propane prices; quantifying policy and regulatory issues under consideration; and agency performance measures. Security matters include: maintaining energy emergency plans; overall coordination on critical energy and communications infrastructure protection and homeland security. In addition the section provides management and operational support of the commission's website and web-based applications. It also assists with technology application and coordination and serves as the agency's point of contact with the Department of Information Technology.
- This is a newly established position, so the PSC can monitor and make decisions on rate recovery of cybersecurity investments by regulated utilities.

EDUCATION

- Bachelor's degree, with a preferred major in engineering or computer science. Certificate or knowledge of cyber security and knowledge of utility infrastructure is a plus.

EXPERIENCE

- No specific amount or type is required.

KNOWLEDGE, SKILLS, AND ABILITIES

- Excellent communications skill, both written and oral. Ability to plan and undertake research, use technical research methods, and prepare a formal report. Strong analytical skills along with ability to formulate procedures and analyze and appraise issues to make effective recommendations. Good public relations skills. Good computer skills, including Microsoft Word, Excel, PowerPoint, and the ability to learn other software as needed.

Cybersecurity Intern/Fellow

Level: Intern/Fellow
Job Title: Cybersecurity Intern/Fellow

GENERAL DESCRIPTION

As an intern with the public utility commission (PUC), you'll have a seat at the table and the chance to offer strategic insights that will shape cybersecurity policies and regulations within the state. Under the guidance of senior analysts and engineers, the intern will be given the opportunity to lead a small research project or initiative relating to emerging cybersecurity issues within the energy industry. In addition to their specific job duties, the intern will be invited to learn about diverse policy issues and participate broadly in the cybersecurity division's meetings, workshops, and preparedness exercises.

Essential Functions of the Internship Include:

- Research and become familiar with the PUC's rulemaking process.
- Assist in updating and maintaining the PUC's cybersecurity assessment records in coordination with utilities.
- Track emerging cybersecurity regulations, plans, or products from the Federal Energy Regulatory Commission (FERC), the U.S. Department of Energy, the U.S. Department of Homeland Security, the National Association of Regulatory Utility Commissioners (NARUC), and relevant state agencies.
- Compile a list of cybersecurity initiatives and programs within regulated utilities.
- Update the commission's cybersecurity incident emergency point of contacts list.
- Assist in the development of processes to share cybersecurity threat information with key stakeholders.
- Attend meetings, workshops, and exercises with energy sector partners.
- Lead a small project or initiative related to emergency cybersecurity issues within the energy industry.

MINIMUM QUALIFICATIONS

- Current enrollment in an undergraduate or graduate degree program at an accredited university studying cybersecurity, computer science, policy, law, or a related field of study.

À La Carte—Cybersecurity Job Descriptors

For PUCs interested in developing unique job descriptions tailored to their needs, this section includes a mix of example cybersecurity job duties, knowledge, and abilities, which can be considered for inclusion. Cybersecurity personnel within a PUC may not directly perform these tasks, but experience in these areas may be useful when working with utilities that do. NARUC does not recommend utilizing all examples outlined, but instead, pick and choose specific duties, knowledge, and abilities that will contribute to your PUC's cybersecurity strategy and goals.

EXAMPLES: CYBERSECURITY JOB DUTIES

- Maintain technical expertise, leadership, and guidance for the analyses of cybersecurity issues affecting public utilities.
- Observe and evaluate regulated utilities' physical and cybersecurity programs by conducting annual surveys to assess their cybersecurity posture.
- Explore public/private partnerships to assess utilities' implementation of security standards, guidelines, and best practices.
- Collaborate with external agencies such as information sharing and analysis centers, fusion centers, and other organizations to establish and maintain utility best practices in cybersecurity.
- Liaise with utility sector-specific organizations responsible for widespread incident response and recovery.
- Attend briefings (classified and unclassified) that provide industry and the commission with current threat information.
- Conduct public and private outreach.
- Provide industry oversight, direction, or development and advocacy so regulated utilities may effectively conduct cybersecurity work.
- Provide technically sound advice and recommendations to commission leadership and staff concerning cybersecurity.
- In consultation with senior staff and general counsel, advocate for policy changes that may be necessary to protect regulated utilities from cybersecurity threats.
- Manage any third-party vendors contracted by the commission to perform cybersecurity activities (vendor management).
- For regulated industries, review cybersecurity plans, strategy, and policy to ensure they align with cybersecurity initiatives and regulatory compliance where appropriate.
- Work to advance cooperation across organizations and between cyber operations partners.
- Support the integration of partner cyber and physical security teams by providing guidance, resources, and collaboration to develop best practices and integrated cyber actions.

EXAMPLES: CYBERSECURITY KNOWLEDGE

- Knowledge of information security technologies the areas of risk assessment, compliance, and vulnerability management.
- Working knowledge of cybersecurity protocols log correlation tools.
- Packet analysis tools.
- Basic routing concepts and protocols.

- How DNS works in the enterprise/internet.
- TCP/IP protocol suite, security architecture, and security techniques/products.
- Working knowledge of cloud perimeter and firewall security controls.
- Common security management frameworks such as NIST, SANS Twenty Critical Security Controls, and other cybersecurity standards.
- Network architectures and theory and principles of secure network design, integration, configuration, and management.
- Knowledge of technical security best practices, in dealing with endpoint, server, and network security (firewalls, IDS/IPS, VPN, etc.).
- Principles and methods of enterprise-level data management and data storage solutions.
- Knowledge of information security best practices, in dealing with sensitive data (PII, PHI, etc.).
- Knowledge of various programming languages and security programming best practices.
- Knowledgeable on adopting strategies for the use of cloud services (AWS, GCP, Azure) and hybrid cloud security.
- Complex computer network system environments.
- Strong understanding of network administration protocols.
- IT risk/threat assessment process and practices and countermeasures.
- Principles, framework, and methods used in the analysis and development of information security systems and procedures.
- Cybersecurity software and systems.
- Utility operating practices and procedures.
- Federal government regulations specific to cybersecurity.
- Contracts and legal requirements.
- Regulatory compliance programs.
- Effective presentation and training methods.

EXAMPLES: CYBERSECURITY ABILITIES

- Ability to provide guidance and recommendations from a group composed of subject matter experts in solving technical architectural issues.
- Ability to assist security operation center with integrations of security tools and diagnosing technical issues with hands-on experience.
- Ability to continuously monitor cybersecurity alerts and bulletins (NERC, MS-ISAC, etc.) for updates, emerging threats, and vulnerabilities, and quickly disseminate relevant information.
- Stay up-to-date on information technology trends and security standards.
- Experience with the following security tools/processes: Intrusion Prevention System (IPS), Intrusion Detection Systems (IDS), Security and Information Event Management (SIEM), NAC, antivirus/malware detection, endpoint detection and response, vulnerability scanning, dynamic application scanning, incident response, and digital forensics.

- Maintain a high degree of expertise to research, analyze, evaluate, recommend security, and network applications.
- Interpret and summarize a variety of data and information.
- Understand the benefit and risks of various IT and OT security solutions.
- Develop information security services related to policy and strategy.
- Perform cybersecurity risk assessments and problem resolutions.
- Recommend and implement preventative techniques.

EXAMPLES: GENERAL ABILITIES

- Demonstrate good time management skills.
- Safeguard and maintain confidential information.
- Make effective presentations to groups.
- Communicate effectively, both orally and in writing with various levels.
- Interact effectively with the public and peers.
- Ability to work as part of a team to help drive change and improve the state's security posture and maturity.

Appendix B: Annotated List of Cybersecurity Workforce Recruitment Pipelines

Pipeline	Description	Links
NARUC Job Board	Members of NARUC are encouraged to post their employment opportunities on NARUC's website to expand their reach. This service is free of charge for NARUC members.	https://www.naruc.org/about-naruc/employment-opportunities/member-employment-opportunities/
Centers for Academic Excellence Community	The Centers for Academic Excellence in Cybersecurity (CAE-C) program has over 300 higher education institutions designated by the National Security Agency and the U.S. Department of Homeland Security as having a rigorous cybersecurity curriculum. The CAE community regularly hosts career fairs and other networking opportunities.	Homepage: https://www.caecommunity.org/ List of CAE designated institutions: https://www.caecommunity.org/content/cae-institution-map
CyberCorps®: Scholarship For Service Recipients	Scholarship For Service (SFS) is a unique program designed to recruit and train the next generation of IT professionals, industrial control system security professionals, and security managers to meet the needs of the cybersecurity mission for federal, state, local, and tribal governments. The program provides scholarships for up to 3 years for cybersecurity undergraduate and graduate (MS or PhD) education. Scholarships recipients must agree to work after graduation for the U.S. Government or a state government, in a position related to cybersecurity, for a period equal to the length of the scholarship. Many scholarship recipients continue to work for the government afterward because they enjoy the job security and the opportunity for regular career ladder progression.	Homepage: https://www.sfs.opm.gov/ Recruiting SFS students: https://www.sfs.opm.gov/AODefault.aspx
DOE's CyberForce Competition	The CyberForce Competition is a cyber workforce development competition for university students that focuses on the defensive/hardening nature of energy cyber infrastructure. The competition takes place on an annual basis at participating national labs across the country. Becoming competition sponsors or volunteering to help conduct the competition would be a good opportunity for PUCs to network with cybersecurity talent. Students who compete receive an individual competition proficiency report mapped to the NICE Framework.	https://cyberforcecompetition.com/.
National Cybersecurity Training & Education (NCyTE) Center	The NCyTE Center focuses on building a comprehensive network of higher education institutions, businesses, and government agencies dedicated to developing and maintaining a robust cybersecurity workforce.	https://www.ncyte.net/
Women in Cybersecurity (WiCyS)	WiCyS is an organization with national reach dedicated to bringing together women in cybersecurity from academia, research, and industry to share knowledge, experience, networking, and mentoring. WiCyS hosts an annual networking conference, an annual career fair, and maintains a job board. There is a monetary cost to employers seeking to partner with WiCyS as an employer.	https://www.wicys.org/.

Pipeline	Description	Links
Minorities in Cybersecurity (MiC)	MiC is a nonprofit corporation dedicated to the leadership and career development of its members. They strive to create a community of cybersecurity professionals that will support, develop, and help prepare their members to excel in the cybersecurity field and achieve personal success. MiC hosts monthly calls, offers mentoring and coaching services, and maintains a job board. There is a monetary cost to employers seeking to partner with MiC as an employer.	https://www.mincybsec.org/
Society of Women Engineers (SWE)	SWE is an electronic recruitment resource for leading companies in the engineering and technology field. There is a monetary cost to employers seeking to partner with SWE as an employer.	https://careers.swe.org/
Young Professionals in Energy (YPE)	YPE is a nonprofit organization with more than 40,000 members worldwide. By providing a forum for networking and career development through social, educational, and civic service opportunities, YPE aims to facilitate the advancement of young professionals in the global energy industry. YPE runs a year-round calendar of events in 40 chapters around the world. There is a monetary cost to employers seeking to partner with YPE as an employer.	https://ypenergy.org/jobs/
Society for Advancement of Chicanos/ Hispanics & Native Americans in Science (SACNAS)	SACNAS is an inclusive organization dedicated to fostering the success of Chicanos/Hispanics and Native Americans, from college students to professionals, in attaining advanced degrees, careers, and positions of leadership in STEM. It is free to post a position for 30 days, other options exist for a monetary cost.	https://opportunitiesboard.sacnas.org/

Appendix C: Annotated List of Cybersecurity Training Opportunities

Free Training Opportunities

Opportunity	Description	Links
NARUC's Cybersecurity Training for State Regulatory Commissions	Open to commissioners and commission staff, NARUC's Center for Partnerships and Innovation (CPI) hosts "Cybersecurity Training for State Regulatory Commissions" to develop cybersecurity subject matter expertise and understanding. The training focuses on building technical expertise, specifically in IT/OT technologies and threat mitigation, federal regulatory requirements, and PUC strategies for ensuring utility cybersecurity preparedness. Each training event includes an instructional session on the use of two components of the Cybersecurity Manual: (1) Cybersecurity Preparedness: Questions for Utilities and (2) Cybersecurity Preparedness Evaluation Tool. Training events are free and are typically held regionally twice per year.	Contact NARUC to inquire about the next training opportunity.
U.S. Department of Homeland Security (DHS) Training	DHS's Cybersecurity and Infrastructure Security Agency (CISA) offers web-based and instructor-led cybersecurity courses from introductory to advanced levels. Courses focus on the cybersecurity of industrial control systems.	Calendar: https://www.us-cert.gov/ics/Calendar Training Opportunities: https://www.us-cert.gov/ics/Training-Available-Through-ICS-CERT#need Virtual Learning Portal: https://ics-training.inl.gov/learn
U.S. DHS Training	Through the National Initiative for Cybersecurity Careers and Studies (NICCS), the Federal Virtual Training Environment (FedVTE) provides free online cybersecurity training to federal, state, local, tribal, and territorial government employees, federal contractors, U.S. military veterans, and the public. FedVTE contains more than 800 hours of training on topics such as ethical hacking and surveillance, risk management, and malware analysis. FedVTE offers courses for all proficiency levels, certification prep courses for Certified Information Security Manager (CISM), and Certified Information Systems Security Professional (CISSP), and the ability to work at your own pace.	https://niccs.us-cert.gov/training/federal-virtual-training-environment-fedvte
U.S. Department of Energy's (DOE) CyberFire	DOE's CyberFire is a free week-long cybersecurity training designed for entry-level to experienced cybersecurity analysts from all levels of government, critical infrastructure operators, students, and multinational partners. Instructors from DOE's National Labs will lead instruction, hands-on learning, puzzles, and briefings. Attendees choose between six different instructional lanes. • **Entry Point**: An overview of everything. Start here if you're just getting into incident investigation! • **Host Forensics:** Examine memory and disk forensic artifacts to find forensic artifacts. • **Incident Coordination:** How to manage incident response teams and communicate clearly and effectively to vested parties. • **Malware Analysis:** Examine malicious software to discover capabilities, methods, and more. • **Network Archaeology:** A combination of "Binary Network Protocols 101," "Cryptanalysis 101," and "Back Engineering 101," with a focus on mathematics and information theory. • **Operational Technology:** Learn the peculiarities of computers that interact with the physical environment.	https://cyberfire.energy.gov/

Paid Training Opportunities

Opportunity	Description	Links
SANS Institute	SANS provides intensive, hands-on cybersecurity training for beginners to advanced learners. Courses were developed through a consensus process involving hundreds of administrators, security managers, and information security professionals, and address both security fundamentals and awareness, and the in-depth technical aspects of the most crucial areas of IT security. SANS mapped their training courses to match the NICE Framework's workforce categories and specialty areas.	Interactive NICE Framework Mapping: https://www.sans.org/niceframework/
NICCS Education and Training Catalog	The NICCS Education and Training Catalog is a central location with over 5,000 cybersecurity-related courses. Anyone can use the interactive map and filters to search for courses in their local area so they can add to their skill set, increase their level of expertise, earn a certification, or even transition into a new career. All courses align with specialty areas of the National Cybersecurity Workforce Framework.	Catalog: https://niccs.us-cert.gov/training/search
Cybrary	Cybrary offers courses to develop the skills needed for cybersecurity and IT careers. Their course catalog includes over 1,000 hands-on experiences to build cybersecurity skills. They offer certification preparation, mentorship and guidance, virtual labs, skill development, and skill assessments. Areas of expertise include cybersecurity, IT, Cloud, Data Science, and DevSecOps.	https://www.cybrary.it/
(ISC)² Professional Development Institute	(ISC)² is an international, nonprofit membership association for information security leaders, and they offer cybersecurity training courses at a cost for nonmembers. Course offerings focus on, but are not limited to, industrial control systems, the internet of things (IoT) ecosystem, cloud services, DevSecOps, and incident management.	Professional Development Institute: https://www.isc2.org/Development Mapping (ISC)² Courses to the NICE Cybersecurity Framework: https://www.isc2.org/NICE-Cybersecurity-Framework-Map

NARUC
National Association of Regulatory Utility Commissioners

1101 Vermont Ave, NW • Suite 200 • Washington, DC 20005
www.naruc.org • (202) 898-2200