NATIONAL GOVERNORS ASSOCIATION

ENERGY CYBER WORKFORCE POLICY BRIEF

The National Governors Association Center for Best Practices (NGA Center), with support from the U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response (DOE CESER) convened a group of public and private stakeholders in June 2023 to explore the roles Governors can play in ensuring an adequate cybersecurity workforce in the energy sector. These stakeholders included the electricity sector, the oil and natural gas sectors, state cybersecurity agencies, state workforce and education leaders, plus representatives from four federal agencies.

These stakeholders spoke to their state and industry perspectives on cyber workforce challenges and articulated ways Governors and states can expand the cyber workforce pipeline. Several broad avenues for states to pursue emerged from the conversation. This policy brief is an effort to capture this dynamic conversation and act as a springboard for a continuation of the partnership between these stakeholders, DOE CESER, and the NGA Center. At the roundtable, participants identified policy and programmatic solutions that Governors and state leaders can implement, which are further described herein.

Governors are well-positioned to bolster the pipeline of qualified cybersecurity personnel, in both the public and private sector, by spurring interagency collaboration, building relationships with energy companies, strengthening the cyber talent pipeline into the public sector, and establishing programs that prioritize the cyber workforce pipeline.

BACKGROUND

Globally there is an estimated shortage of 3.4 million qualified cybersecurity professionals. This gap is expected to widen as the need for cybersecurity skills is projected to grow rapidly over the next decade.[1]

A recent National Institute of Standards and Technology (NIST) summary of cybersecurity workforce demand reported that 83% of corporate boards recommend increasing information technology security staff numbers. While this shortage is felt throughout the economy, these staffing shortages are particularly acute in the energy sector. Furthermore, the energy sector sits at the confluence of multiple macro trends, such as growing energy demand, escalating cyber threats from malicious individuals and nation-states, and the integration of new technologies on energy infrastructure.

Over the past several years, the United States has devoted significant resources toward modernizing dated energy infrastructure by integrating a broad array of new communications, monitoring, and virtual operational technologies. These investments can make electric, oil and natural gas systems more resilient, reliable, and efficient. However, integrating internet connected or internet adjacent technologies can provide access for nefarious parties who might seek to disrupt the delivery of energy throughout the United States.

Coincident with these trends, the United States broadly and the energy sector specifically have also seen an increase in attempted cyber-attacks on critical infrastructure.[2] These growing threats have led to increased awareness of system vulnerabilities and a renewed effort to secure energy systems. Training, hiring, and maintaining a well-trained cybersecurity workforce are key to protecting these energy systems. Worryingly, a recent International Energy Agency (IEA) report found that the energy industry faces serious difficulties in finding and retaining skilled cybersecurity professionals. The same IEA report found that, on average, the salaries of energy sector cybersecurity personnel were substantially lower than other sectors such as finance and insurance. This competition from other sectors may serve to exacerbate the shortage of cyber talent through inter-industry competition. Governors can play a critical role in creating pathways for cybersecurity professionals, through workforce development programs, reskilling efforts, public outreach, and raising awareness of cybersecurity job opportunities in the energy sector.

OPERATIONAL TECHNOLOGY (OT) interacts with the physical world or manages devices which interact with the physical world. OT examples include everything from Energy Management Systems and Supervisory Control and Data Acquisition (SCADA) to pipeline pumps and compressor stations.

INFORMATION TECHNOLOGY (IT) refers to equipment or systems used in the automatic acquisition, storage, management, or manipulation of data. Broad deployment of, and reliance on, both IT and OT render the energy sector particularly vulnerable to malicious cyber-attacks, as digital incursions can translate into serious consequences in the physical world.

IT and OT in the Energy Sector

While cybersecurity vulnerabilities exist in every critical sector, a potential cyber incursion of the energy system could disrupt huge swathes of the economy. Securing the energy system is particularly challenging not only due to the omnipresent need for energy to power commerce and interdependent critical infrastructure systems, but also the highly distributed nature of energy infrastructure. To operate effectively, energy companies must leverage distributed infrastructure to generate and move energy (in the form of electricity, oil, gas, etc.) to meet demand in real time. In the case of the electric grid, real time supply and demand must be balanced virtually second-by-second. To reliably meet demand, energy companies rely on a complex blending of information technology (IT) and operational technology (OT), further complicating the sector's ability to cybersecure energy systems.

Over the last decade a number of significant cyberattacks have affected energy infrastructure OT around the world and within the United States.

- In 2015, attackers penetrated a Ukrainian regional distribution company's system and used unauthorized access to electric power SCADA systems to shut off power to more than 200,000 Ukrainians. Recovering from this outage required a manual black start of the electric system.[3] Beyond the disruption to Ukraine, this was the first successful cyberattack on an energy system and demonstrated the viability of this tactic.
- The following year attackers gained access to an Industrial Control System (ICS) that forced an hour-long power disruption in the Ukrainian capital Kiev. This attack does not appear to have accomplished its full goal but did demonstrate that malware can affect multiple infrastructure systems remotely.
- In 2017, a petrochemical facility in Saudi Arabia was temporarily shut down because a safety instrumented system (SIS) was affected by malware that forced a safety instrumented system (SIS) to falsely indicate life threatening danger within the facility for workers. Preventing safety mechanisms from performing their intended function can result in physical consequences to workers and infrastructure.
- In 2017, researchers found they could remotely hack wind farms to slow or paralyze turbines, thus, impacting the amount of electricity generated from a wind farm. Rapidly decreasing electricity generation can unbalance the grid and potentially cause brownouts or blackouts.
- In 2019, an unnamed attack on the U.S. electric grid exploited blind spots between a control center and remote energy generation sites. While this attack did not cause widespread energy disruptions, it demonstrated that the U.S. is vulnerable to cyber incursion.
- In arguably the most famous cyberattack to affect the American energy sector, ransomware targeted the IT network of Colonial Pipeline in 2021. Though this attack did not overtly impact OT, the company chose to proactively shut down the flow of fuel in the pipeline until it better understood the extent of the incursion. As a result, substantial fuel shortages affected the southeast and MidAtlantic regions and caused some consumers to panic buy fuel, further exacerbating shortages.

While attempted cyber incursions into U.S. energy systems are growing, the energy sector is struggling to find qualified cyber talent. The National Institute of Science and Technology (NIST) found only 20% of electric utility companies reported feeling confident that they have the cybersecurity talent they need. As the cyber incidents discussed above demonstrate, both IT and OT have vulnerabilities that can be exploited by malicious actors. To prevent and respond to this risk, state governments, regulators, and energy companies need a reliable pool of qualified cybersecurity talent that can confidently navigate both IT and OT systems.

OPPORTUNITIES FOR GOVERNORS TO CONSIDER

Ensuring that the energy industry has access to a trained, qualified workforce is a critical component of protecting systems from cyber threats. To grow the talent pipeline in this space, Governors may call on key stakeholders including employers, workforce and economic development policymakers, institutions of higher education, and energy officials to develop a statewide strategy for this key issue. Opportunities for Governors to consider include:

I. **Spur Interagency Collaboration:** Governors may consider prompting workforce development experts and state energy officials to co-determine the road ahead for developing the energy cybersecurity workforce. Specific opportunities include but are not limited to:

1) **Workforce Innovation and Opportunity Act Planning**: Governors are required to submit strategic plans for workforce development to the U.S. Department of Labor every four years. Governors may consider leveraging this strategic planning process to develop initiatives related to the energy cybersecurity workforce.

2) **Maximize Recent Federal Investment in Workforce and Cybersecurity:** The Infrastructure Investment and Jobs Act (IIJA) and Inflation Reduction Act (IRA) include several opportunities for states and territories to invest in the energy cybersecurity workforce. Governors may consider calling upon workforce development and energy officials/experts to devise a holistic strategy for pursuing and deploying competitive grant funds and other federal opportunities to develop the energy cybersecurity workforce.

   The IIJA also created the State and Local Cybersecurity Grant Program. Over a span of four years, this program will allocate $1 billion in funding to support targeted cybersecurity investments in state, local, and territorial government agencies with the goal of enhancing the security of critical infrastructure and addressing workforce shortages.

3) **Include Workforce Development in Broader State Energy Planning:** The IIJA requires, as a condition of grant funding through the State Energy Program, that states submit annual State Energy Security Plans (SESP) by September 30 through 2025. In addition, at the direction of their Governors, states frequently undertake energy planning, resilience planning, or other energy sector reviews. Though energy plans are unlikely to directly reference workforce issues, Governors may consider how, if at all, they should charge relevant entities with considering workforce development strategies as a part of their SESP or other state plans.

II. **Build Relationships with Energy Sector Companies:** Much of the energy infrastructure in the US is owned by private companies who employ their own personnel and have a vested interest in maintaining a strong cyber posture. Governors and state partners should focus on building relationships with energy sector companies. Industry stakeholders can provide invaluable insight into key skills and abilities needed to develop energy cyber workforce.

When building these relationships, it is important to remember that electric utility companies vary significantly in size and resources. Rural electric cooperatives and municipal electric utilities will have different capacities and risk profiles than larger investor-owned utilities (IOUs). Building close partnerships and having open lines of communication with all types of utilities will allow Governors to better identify and understand the cybersecurity talent needs of the electric sector.

States with a significant upstream and midstream oil and natural gas sector may also seek to partner with major oil and gas companies, associations, and/or trade groups to improve understanding between the public and private sectors, as well as share resources on cybersecurity issues.

III. **Strengthen the Talent Pipeline for the Public Sector:** Roles in the energy cybersecurity space require a specific skillset; therefore, having a concerted strategy for worker recruitment and retention is critical. Specific opportunities include but are not limited to:

1) **Devote Resources to Training Incumbent Workers**: The detail-oriented and high-risk nature of energy cybersecurity roles require employers to dedicate considerable resources to on-the-job training. Governors may consider supporting employer efforts to retain employees.

2) **Consider Recruiting Former Military Personnel**: Former military personnel may have skills that are transferrable to the energy cybersecurity space. Governors may consider directing agency leaders to create clear pathways from military service into energy cybersecurity.

3) **Create a Strategy to Engage Youth:** Youth labor force participation remains at a relatively low rate in virtually every industry, including energy. Governors may consider calling on programs designed to increase youth labor force participation to engage 16-24 years olds (or even younger students) in the energy cybersecurity workforce.

   a. The New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) is situated within the New Jersey Office of Homeland Security and Preparedness and provides a wide array of cybersecurity services. As the principal cybersecurity agency in New Jersey, the NJCCIC has a voracious need for qualified cybersecurity talent. However, like many public agencies with limited budgets and employee positions, NJCCIC often struggles to attract and retain talent. To overcome this barrier, NJCCIC has implemented an informal strategy that 1) places its mission-driven work front and center, and 2) intentionally reaches out to young people with opportunities for career development. NJCCIC leadership explained that attracting

a high school student to an internship helps the student become aware of cybersecurity as a field and begins to develop their skillset. As the student graduates and attends university, NJCCIC can provide additional internships, training, and flexible paid work. Once a student finishes their degree, they have significant experience in the field and may seek to join NJCCIC on a full-time basis. As this student reaches mid-career level, they are often highly sought after and may leave state service to join the private sector, thereby strengthening the overall cybersecurity posture of the state and country. Since outreach efforts to high school and college students are ongoing, NJCCIC has a steady pipeline of cybersecurity talent in various stages of their careers.

b. The U.S. Department of Energy's CyberForce® Program "seeks to inspire and develop the next generation of cyber defenders for the energy sector through hands-on competitions, webinars, learning resources, and career fairs." In 2023 alone, more than 1,600 students from 44 states and territories participated in CyberForce programming. Governors can encourage their university systems and students to participate in this and similar programs to leverage the training resources and career opportunities such programs provide.

4) **Expand Funding to Public Agencies:** Given the evolving threat of cybersecurity incursions to the energy sector, traditional funding streams to State Energy Offices, Public Utility Commissions, and Cybersecurity Offices may not be sufficient. Flexible pay incentives for employees with demonstrated cybersecurity skills could help retain talented workers and incentivize other workers to grow their skills. Governors may choose to work with their state legislatures to review staffing levels and compensation structures for agencies tasked with overseeing cybersecurity. While adding staff to state payrolls can be difficult, the potential upside of improving cyber readiness can pay significant dividends.

IV. Establish Programmatic Priorities that Address Energy Cybersecurity Workforce Needs:

There are multiple pathways into the energy cybersecurity sector that Governors can leverage to develop this talent pipeline. Specific opportunities may include but are not limited to:

1) **Leverage Registered Apprenticeship Programs:** Registered apprenticeship programs – which combine on-the-job training, classroom instruction, and employer-sponsored mentorship – have a long track record of providing return on investment for both workers and employers. Governors may consider calling on this proven model to meet critical needs in the energy cybersecurity space, as well as the needs of state government itself. Additionally, apprenticeship programs can help expose the workforce directly to OT systems used to operate the energy system. As such, graduates of apprenticeship programs will be particularly well-prepared to navigate the threats to the IT/OT systems discussed above.

2) **Include Computer Science in K-12 Education:** Early computer science foundations can help a student prepare early for a career in cybersecurity. While not exclusively cybersecurity focused, allowing K-12 students to access computer science education at younger ages can build core computer skills and raise awareness about cybersecurity careers options.

    a. While every state permits computer science coursework to count toward graduation, some Governors have expanded computer science to be a high school graduation requirement for all students. In 2018, South Carolina adapted its existing technology requirement into a computer science requirement. Since 2018, four additional states -- Arkansas, Nebraska, Nevada, and Tennessee -- have taken similar steps to make computer science coursework a requirement for graduation.

3) **Call on Institutions of Higher Education to Expand Cybersecurity Training and Credentialing Programs:** Both two- and four-year institutions of higher education can offer programs that lead to high-skill occupations in energy cybersecurity. Governors may consider charging their state's institutions of higher education with developing programs to meet growing cyber demand. In addition, Governors can direct their state economic development authorities to partner with institutions of higher education to further develop relevant skills programs.

    a. The Virginia Cyber Range is an initiative led by the Commonwealth of Virginia aimed at enhancing cybersecurity education for students in public high schools, colleges, and universities within the state. The program receives funding, in part, through the Virginia Research Investment Fund, with active participation from 19 colleges and universities. It provides immersive training, offers courses leading to recognized cybersecurity credentials such as CompTIA, and eliminates barriers to entry.

    b. In Maryland, Prince George's Community College offers a program that grants students a Cybersecurity Certificate, which prepares them for entry-level positions in cybersecurity with a focus on systems' security administration and cyber-analytics and operations. Upon completing the certification, students will be equipped to work in Network Operations Centers as well as Security Operations Centers. Additionally, students will have the foundational knowledge required to pursue industry certifications such as CompTIA's Network+, Security+, Cloud+, Linux+, and CySA+. To obtain the certification, students must complete eight relevant courses while enrolled in the program.

This brief was a collaboration with contributions from the NGA Center for Best Practices Energy Team, Workforce Development & Economic Policy Team, and Post Secondary Team. For further information please contact lead authors: Chris Fletcher (cfletcher@nga.org), Jack Porter (Jporter@nga.org) or Amanda Winters (awinters@nga.org).

This material is based upon work supported by the Department of Energy, Office of Cybersecurity, Energy Security, & Emergency Response under Award Number DE-CR0000011.

[1]https://www.nist.gov/system/files/documents/2023/06/05/NICE%20FactSheet_Workforce%20Demand_Final_20211202.pdf
[2] https://www.nerc.com/pa/CI/ESISAC/Documents/2023%20E-ISAC%20End-of-Year%20Report.pdf
[3] https://www.energy.gov/sites/default/files/2022-06/DOE%20CESER%20SESP%20Drop-In%20IT-OT%20and%20Cyber%20Threats%20Overview_FINAL_508.pdf