A.1 What technical assistance would States, Indian Tribes, or units of local government need to enhance their security efforts relative to the electric system?

The actions performed at different levels of government are an important precursor to the technical assistance these entities need to best enhance electric system cybersecurity efforts. State governments primarily regulate electric utilities, local governments primarily operate municipal power utilities, and Tribal governments often perform both functions.

"While most utilities have become aware of the risks associated with cybersecurity, inconsistencies still exist in their ability to secure funding to invest in OT and IT cybersecurity controls. In many states, regulators lack the dedicated talent needed to review cybersecurity program budgets, which factor into a utility's billing rates to customers."

– McKinsey & Company, 2020[1]

One of the largest aspects of utility regulation by State & Tribal governments is in approving the rates that utilities charge to consumers, and therefore whether the cost of cybersecurity improvements can be passed onto their customers. However, these State and Tribal agencies often lack the domain expertise to judge the expected efficacy of utility cybersecurity proposals. At the State and Tribal level, technical assistance from DOE in educating and training the appropriate regulatory bodies on Industrial Control System (ICS) cybersecurity best practices would help to build the acumen to properly evaluate these proposals. With this technical assistance, State & Tribal governments could have better awareness during the ratemaking process of how proposed cybersecurity investments by utilities do or don't go far enough in enhancing the resiliency of the electric system and can approve proposals accordingly.

"Additionally, certain municipalities offer energy services independent of a major utility. This may alleviate customer concerns with existing energy players in the market, but many of these municipalities remain underprepared or understaffed to ensure the deployment of enough cybersecurity controls to decrease risk."

– McKinsey & Company, 2020[1]

Many local & Tribal governments are involved in the operation of electric utilities, with the American Public Power Association (APPA) citing that more than 49 million Americans receive their power from public power utilities in roughly 2,000 cities and towns across the country[2]. The OT security teams of these utilities are often under-resourced and lack the domain expertise necessary to meet the growing threats of nation-state adversaries and cybercriminals

[1] McKinsey and Company, 2020 https://www.mckinsey.com/business-functions/risk/our-insights/the-energy-sector-threat-how-to-address-cybersecurity-vulnerabilities#

[2] American Public Power Association (APPA), 2021 https://www.publicpower.org/system/files/documents/January%202021%20-%20Grid%20Security.pdf

that increasingly target control systems, putting American critical infrastructure and human safety at risk and exacerbating the need for automated, scalable solutions.

Congressional legislators and advocates in the industry have stressed the importance of including cybersecurity funding for state and local governments (including municipal utilities) as a necessary component of the Biden Administration's Infrastructure Plan (American Jobs Act), however this legislation is still being debated[3]. The Department should advocate for grant or affordable loan programs for State, Local, and Tribal governments to purchase cybersecurity products, solutions, or training, which would help to dramatically improve the security posture of our nation's critical infrastructure.

In addition to being under-resourced, State, Tribal, and local governments as well as smaller private utilities often lack sufficient expertise in OT security best practices to properly monitor and defend their critical assets. In addition to making sure that critical infrastructure operators in both the public and private sector are properly resourced to address the threats they face, it is also critical to ensure that these entities have the technical direction that serves as a roadmap for how these resources should be applied. While NIST's Special Publication 800-82 rev. 2 "Guide to Industrial Control System Cybersecurity" is a great introduction to ICS cybersecurity measures to adopt, the most recent revision was published in 2015 (Revision 3 is currently being drafted), does not adequately cover security controls for the deepest layers of an ICS (e.g. serial communications monitoring), and does not help OT operators judge the effectiveness of various commercially available technical solutions.

Any Department grant or loan programs should also include specific recommendations for technology stacks that can help State, local, and Tribal governments in implementation and ensure that resource grants are most effectively applied to industrial control system defense. The MOSAICS Program (More Situational Awareness in Industrial Control Systems) is a joint capabilities technology demonstration with the Department of Energy and the Department of Defense, along with private sector stakeholders representing the utilities industry. This program has been developing a solution composed of COTS technology to act as a robust industrial control system cybersecurity platform for both the public and private sector. While this program is still in evaluation phases, the MOSAICS program could be leveraged as an educated starting point for developing and integrating these technology recommendations.

By helping State, Local, and Tribal governments secure adequate resources, develop domain expertise, and procure effective technologies, the Department can encourage robust adoption that helps to enhance the cybersecurity posture and resiliency of the nation's electric grid infrastructure.

[3] White House, 2021 - https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/18/fact-sheet-the-american-jobs-plan-will-bolster-cybersecurity/

A.2 What specific additional actions could be taken by regulators to address the security of critical electric infrastructure and the incorporation of criteria for evaluating foreign ownership, control, and influence into supply chain risk management, and how can the Department of Energy best inform those actions?

As Information Technology (IT) and Operational Technology (OT) systems have converged, cyber adversaries have become increasingly aggressive in pursuing cyber-physical effects such as critical infrastructure downtime, asset damage, and process manipulation. This has put business continuity and human safety at risk, and further ensured that adopting zero-trust visibility at every level of the Industrial Control System (ICS) is critical to an organization's security posture. A particularly acute blind spot is found in the monitoring of serial-connected legacy Industrial Control Systems (ICS) at Level 0/1 of the Purdue Model, where only summary-level visibility exists today.

"The increased situational awareness resulting from the collection and analysis of serial data in Layer 1 would not only provide earlier detection, but it would also help to speed investigation and troubleshooting of unexpected values, thereby allowing a return to normal operations in a more expedient and safe manner."

-Jonathan Baeckel, SANS.edu Research, 2021[4]

This blind spot composes a significant portion of ICS infrastructure and has been largely ignored by electric utilities, undermining the overall security and resiliency of the US electric grid. However, the security risk to these undersecured legacy systems is real - 25% of reported ICS vulnerabilities affected Level 0 or Level 1[5]. To mitigate this risk to critical electric infrastructure, the attention paid to utilities' legacy ICS equipment must be aligned with that paid to their higher-level OT equipment. This can be achieved by establishing cybersecurity standards, guidance, and support for serial-connected legacy ICS.

At a minimum, the following cybersecurity standards for electric utility infrastructure should be introduced to enhance the situational awareness and resiliency of serial-connected electric infrastructure:

- Integrate technologies that bring visibility to Level 0/1 serial communications and enable the detection of anomalous behavior within this legacy ICS equipment that could be caused by an operational incident or cyber attack
- Establish minimum standards for said technologies:
    - Technologies must be passive and fail-safe by design, so they don't affect the integrity of the communications, introduce an attack vector to the network, or compromise operations in a failure situation
    - Technologies must enable operators to baseline normal operations
    - Technologies must include mechanisms for detecting and alerting on anomalous communications

[4] SANS.edu Research, 2021 - https://www.sans.org/reading-room/whitepapers/ICS/paper/40125
[5] Claroty, 2020 - https://security.claroty.com/biannual-ics-risk-vulnerability-report-2H-2020

Technologies that meet these standards will help automate serial network security monitoring, but more importantly, they will significantly increase ICS situational awareness and will help overcome the risks posed by hardware and software supply chains and the sophisticated threat actors that perpetrate them. **Cynalytica's SerialGuard AnalytICS Platform meets these requirements and is commercially available –if embraced at scale it could make a meaningful improvement in US critical infrastructure's Level 0/1 cybersecurity posture.**

The Department of Energy should work with FERC to ensure that the "100-day sprint" goal to "enhance the integrity and security of priority sites' control systems by installing technologies and systems to provide visibility and detection of threats and abnormalities in industrial control and operational technology systems" is met by including legacy serial-connected assets in monitoring requirements, as they still compose a significant portion of our nation's critical infrastructure. If communications are monitored for anomalies at all layers of industrial control systems, cyberattacks can be detected earlier in the attack chain and their effects mitigated – enhancing the resiliency of our critical electric grid infrastructure.