## Introduction

- Chairman Murkowski, thank you for convening the Committee today to talk about cybersecurity efforts in the energy industry.
- This hearing is particularly timely because just a few weeks ago our Director of National Intelligence, Dan Coats, publicly warned of two potential energy cybersecurity attack scenarios: a Russian cyber attack that could disrupt an electrical network for a few hours, and a Chinese cyber attack that could disrupt a natural gas pipeline for weeks.
- These threats are not just theoretical: we know that in 2015 and 2016, Ukraine suffered two devastating power outages as a result of cyber attacks.
- And according to the New York Times, a petrochemical plant in Saudi Arabia was hit with an even more serious type of cyber attack in 2017.
- That attack was not designed to shut down the plant, like the Ukraine power outages. It was meant to "sabotage the firm's operations and trigger an explosion."
- In other words, the attack could have taken human lives, but luckily it did not.
- I cannot overstate how serious this threat is, and I am pleased that Secretary Perry has given this the attention it deserves by

elevating cybersecurity to an office of its own, the Office of Cybersecurity, Energy Security, and Emergency Response, or CESER (Caesar) for short.

- On a personal note, I'm also pleased that the first Assistant Secretary to run the office is Karen Evans, who has not one, but two degrees from West Virginia University.
- I'm also especially pleased to have Major Keber (KEE-ber) of the West Virginia National Guard here to share the great work the Guard has done for West Virginia in the cybersecurity space.

**National Security Perspective**

- My current position as the Ranking Member on the Senate Armed Services Subcommittee on Cybersecurity, and my time serving on the Senate Intelligence Committee, further convinced me that we need to look at this as a national security priority.
- Energy cybersecurity IS national security. Period.
- In fact, there are two items I raised in the Armed Services Committee in our first Cybersecurity hearing that are equally relevant in the energy space.
- First, supply chain security has emerged as a significant focus.

- We have to make sure the companies that build components for our grid are secure. We have to protect against vendors' remote access of the grid being exploited, and we have to make sure that attackers don't insert malware into a vendor software update.

## Cyber Workforce

- Second, our cyber workforce is in crisis. We simply do not have enough cyber workers to fill the positions.
- Forbes reports that by 2021, there may be as many as 3.5 million unfilled positions.
- Yes, a big part of this is about getting training, but let's not put the cart before the horse.
- It's also about bringing these jobs to the areas that need them.
- And I think that's where there's an opportunity here for states like West Virginia to fill the gap.
- I know that Major Keber will speak to this a bit more, but the West Virginia National Guard is one of the few National Guard units with access to a decommissioned power plant for workforce training, and they are increasing their workforce development efforts.

- I look forward to hearing from our witnesses about how the nation can rise to this challenge while strengthening the economies of places like southern West Virginia.
- I think it will require collaboration between all entities, including those represented by our witnesses here today, to get where we need to go.

## Conclusion

- My little state of West Virginia has been a leader on energy supply and reliability for the country.
- But, unless cybersecurity challenges are addressed head on, it won't matter how much supply we have.
- We must do everything we can to protect and ensure the security of our infrastructure.
- As we kick off that conversation in this new Congress, I'm glad to have this great panel here today to share their outlook for cybersecurity in the energy industry.