The Internet of Things market continues to grow and so do the cybersecurity concerns that come along with millions of connected devices. Government has turned a keen eye onto the ability to disrupt critical infrastructure security as criminals have bring a profit-motive to the disruption with ransomware attacks and wiper technology.

Industries are now working cross-functionally to incorporate global standards to act a s first level safeguard to critical infrastructure vulnerabilities as well as enterprise level concerns.

Support for cooperation over fragmentation is important to ensure growth in the IoT space from the manufacturing level to the consumer.

The main question in our forums this year wee what is the right level and form of governance? Where should the security measure be placed for maximum effect?

Can we have the free flow of information these devices enable without the fear of security concerns?

Are we moving towards a more robust infrastructure at both ends of the spectrum? Are network operators collaborating with device manufacturers for a seamless integration?

Two key events in 2022 addressed these issues:

The IGF-USA's session on IoT: the Glue of Critical Infrastructure.
https://www.igfusa.us/iot-the-glue-of-critical-infrastructure-or-is-it/

And Shane Tews hosted Industry, Government, and Policy experts to discuss what effect IoT security standards would look like a what government and industry leaders are doing to bring them together.

https://www.aei.org/events/where-should-the-security-lie-in-our-networks/