INDUSTRY INSIGHTS:
5G Summit
Unlock the potential of 5G
5G is expected to eventually revolutionize the ways in which we live and work. For federal agencies whose modernization efforts have been spurred by the pandemic, 5G can also help them reimagine how they carry out their mission.

Better capacity, lower latency and massive device connectivity are key 5G attributes that have received much attention. But how could these translate into benefits for federal government? Consider data-driven insights, massive file transfers for medical or research, drones potentially deployed for mail delivery or site surveillance, and immersive training environments enabled by artificial intelligence—all are ways in which 5G could help transform government operations.

5G technology can also increase the potential uses for Internet of Things (IoT). Lower latency and the ability to support numerous sensors allow for greater data collection and faster processing across an IoT system. The proliferation of IoT devices and the need for remote access to those devices also drives security considerations. Federal agencies will be able to take advantage of security capabilities built into the architecture and functionality of a standalone 5G network.

Federal government is actively researching how to unlock the full potential of 5G and increase security measures. The Energy Department’s national labs and the National Institute of Standards and Technology are testing mission critical applications at scale using 5G networks. Joint Base San Antonio is exploring network slicing and virtualization with telemedicine and medical training pilots. Other agencies are seeing encouraging results from automation, as 5G can enable a wider range of new applications. And 5G combined with edge devices can deliver better performance with more accurate and faster data, which enables agencies to increase operational efficiency, improve citizen engagement and reimagine applications from telehealth to manufacturing—all in the name of mission assurance.

**PANEL OF Experts:**

- Dan Elmore, Executive Director, Wireless Security Institute, Idaho National Lab, Energy Department
- Jody Little, Executive Program Manager, 5G Experimentation, Joint Base San Antonio
- Tao Zhang, Manager, Emerging Network Technologies Group, National Institute of Standards and Technology
- Bob Zapotocky, Bob Zapotocky, Senior Principal Architect, AT&T Public Sector
5G promises revolutionary use-cases, with a critical focus on cybersecurity, standards

5G has a myriad of use cases across government, ranging from research to telesurgery and factory automation. Most use cases rely on its massive capability for lower latency and larger throughput for data transactions. But each application is not one-size-fits-all.

That’s why 5G has created a new service-centric infrastructure, including the concept of network slicing. Applications, performance and security all need to be kept separate, but interoperable at the same time.

For example, the Defense Department is currently running experiments with telemedicine and telesurgery that require the use of augmented reality and ultra-high resolution video. It also involves thousands of medical sensors and even robotics. Each of those requires their own slice of the network, but they also have to work in concert to support the needs of the mission.

They also have to be able to operate across various hardware, software, networks, even telecoms in different countries. All of that requires a close look at security, network slicing and virtualization, and the reliability and redundancy of 5G in those areas.

“You really need to go beyond just security and connectivity,” Tao Zhang, manager for the emerging network technologies group at the National Institute of Standards and Technology, said during the Federal News Network and AT&T 5G Summit. “You really want to introduce, for example, threat handling capabilities in a much more comprehensive and much more natural native manner. So those are newer capabilities that are typically done now over the network by different ways. 5G does provide a range of data collection and data analytics, functionalities that can support those higher level and more comprehensive security capabilities. But that area, I think, is worth looking into a lot more.”

That’s because 5G enhances basic security architecture, but still focuses on securing connectivity. But it opens new channels as well, making the trust relationship more complex. Because 5G is centered on providing new services, you can’t just focus on trust between users and networks anymore. It requires trust between users, services, virtual networks and physical networks. 5G will also introduce new technologies and architectures, including a new virtualized software layer in networks. That requires network slicing to isolate compromises.

But the issue is further complicated by the fact that the 5G edge will increasingly be integrated with user and consumer systems. That makes it difficult to determine which parts of the security need to be provided by the network provider, and which parts by the user.
“For example, how much visibility should the user have into the 5G LAN security configuration and traffic to monitor and to detect threats, and how much of the threat detection and threat handling and threat mitigation capabilities should and can be provided by the network provider, especially at the service level, the network slices,” Zhang said.

One major problem, according to Jody Little, who oversees some of the Air Force’s experiments with telemedicine and 5G security as executive program manager of the 5G Next Gen Program at Joint Base San Antonio, is that there isn’t enough synergy in the 5G industry.

“There’s a lot of training that has to be done,” Little said. “And that training needs to include cybersecurity associated with 5G units. And I’ve seen that most of the universities we’ve been talking to are teaching some 5G. But on the security side, it’s usually something like one module embedded in a course, as opposed to heavily focused.”

Other federal agencies are looking at this security issue as well, including the Department of Energy’s national laboratories. Dan Elmore, executive director of the Wireless Security Institute at the Idaho National Laboratory, said his lab’s been working on developing an assessment program for 5G devices.

“That’s one of the large gaps, as we looked at and surveyed the research world at least in the United States of who’s working on what; the security is a gap area,” Elmore said. “And that’s where National Labs play, looking at problem sets that industry or academia may not be focused on for various reasons. But as the standards roll out 5G has a much richer suite of security features than 4G and the previous versions, but many of those are not mandatory.”

And those standards are coming, from organizations like the 3rd Generation Partnership Program, which is an organization working on protocols around 5G. But the COVID pandemic has delayed much of that work in formulating and releasing those standards, which has cascaded into a delay for original equipment manufacturers to deliver products up to those standards.

“If you think of the impact of being wrong, it’s pretty significant,” said Bob Zapotocky, senior principal architect for AT&T’s Global Public Sector. “So the research, the testing that’s done, the deployment that’s done costs a significant amount of money, billions of dollars. I believe that the R&D budgets on, let’s just say, a worldwide basis for mobile technology is somewhere around $500 billion on an annual basis. So if you happen to move in the wrong direction, as an OEM, or even as a network provider, it can be extremely costly. So this is one of the reasons why development of the standards is critical in order to be able to deploy the services.”

For more information, visit: [www.att.com/Talktech5G](http://www.att.com/Talktech5G)