Harnessing and Securing 5G Networks: Insights From Booz Allen and Federal Technology Leaders

NEWS RELEASE BY **BOOZ ALLEN HAMILTON**

Northampton, MA | June 30, 2021 08:01 AM Eastern Daylight Time

Booz Allen leaders Cedric Sims, Chris Christou and Kelly Rozumalski joined industry experts for the Billington 5G Security Summit to discuss the power of 5G and how the technology can be used by federal agencies.

The federal government has made 5G a top priority, as demonstrated by initiatives like the Secure 5G and Beyond Act of 2020 and the National Strategy to Secure 5G Implementation Plan. Yet there are complex security issues to consider as agencies adopt and operationalize 5G in their missions.

How can 5G networks help agencies protect critical areas like ports and borders—and decrease vulnerabilities? What security protocols do agencies need to consider when designing products and working with the private sector? And how can organizations achieve interoperability across carriers, devices, and systems?

At the inaugural **Billington CyberSecurity 5G Security Summit**, Booz Allen—serving as the event's knowledge partner—along with lead underwriters Cisco and AWS, convened federal and industry leaders to discuss these questions and more. Highlights follow.

The interoperability imperative

The virtual event featured a fireside chat with Booz Allen Vice President **Chris Christou** and Dr. Joe Evans, inaugural Technical Director for 5G, reporting directly to the Under Secretary of Defense for Research and Engineering within the Office of the Secretary of Defense. During this discussion, Dr. Evans shared his insights on open 5G from his work with the Department of Defense's 5G to Next G research and development portfolio, where his team is testing out supply chain and risk management principles in real deployments.

Just as the same 4G network that currently supports Uber also works for OpenTable, Google, and a host of other applications, similar technologies and approaches can be used to make 5G an interoperable platform, Evans said.

His team is exploring and encouraging the use of open interfaces for achieving this interoperability, so that organizations can leverage capabilities and systems from different vendors when they deploy solutions over 5G networks.

Efforts like this by DoD have "spurred those in industry—vendors, carriers and integrators—to think about this new technology, how it can be used, how it can be deployed, how mature it is," said Christou. "It's not only doing a service for our country and the DoD, but really the Federal government and industry at large."

As 5G supports new types of capabilities and technologies, not all of the old standards will fit, Evans cautioned. Shared standards in areas such as network slicing and network security will be essential, and his team is supporting several initiatives as these standards take shape.

Christou also emphasized the importance of interoperability: "You want to make sure devices can connect to the network irrespective, and that different networks can interoperate irrespective of the OEM vendor or carrier that is in use," Christou said.

Heightened visibility, monitoring and vulnerabilities

During a panel moderated by **Dr. Cedric Sims**, Booz Allen Senior Vice President and leader of the firm's Justice, Homeland Security, and Transportation business, panelists involved in port and border security discussed where 5G holds the potential to strengthen preparedness and protection, plus the cybersecurity concerns federal agencies must keep in mind as they roll these solutions out across 5G networks.

One area of focus was 5G's ability to enhance visibility and threat monitoring.

For example, ships and ports handle more than 90 percent of the world's trade, and within the United States, the maritime transportation system accounts for 25 percent of U.S. GDP, according to Rear Admiral John W. Mauger of the U.S. Coast Guard. A comprehensive sensor network powered by 5G could strengthen oversight of both lawful and illegal trade.

Federal agencies can also use advanced 5G-powered solutions to monitor threats on the networks themselves.

"Booz Allen is looking at the ways in which artificial intelligence and machine learning can be applied to detect anomalies and malicious behavior," Sims said. "So when networks aren't performing or they're performing in a way that indicates a compromise, they can put out the proper alerts and warnings."

Securing connected devices in a complex and changing world

Always assume that adversary knows everything about your systems, Dr. Kevin Fu advised in a discussion with Booz Allen Vice President **Kelly Rozumalski**, leader of the firm's secure connected health work.

Fu, the FDA's first director of medical device security, talked about the importance of cybersecurity for device manufacturers and steps they must take to protect the safety and effectiveness of their products in a 5G world.

"When we look at our broad digital ecosystem, things such as 5G are enabling the market to grow at an extremely fast pace," Rozumalski said. Yet rapid growth brings heightened security risk.

As 5G continues to catalyze the development of new products, systems, and technologies, including connected devices, panelists advised that federal agencies and their private-sector partners mitigate the risks by:

- Conducting threat modeling
- Considering OT (operational technology) as well as IT
- Maintaining appropriate software updates
- Using tools like a software bill of materials and cybersecurity plans through the complete product lifecycle, from device design through the launch and beyond

Learn more about **Booz Allen's 5G work** and read the firm's latest 5G research:

View additional multimedia and more ESG storytelling from Booz Allen Hamilton on 3blmedia.com