MOBILE INNOVATION

IN FEDERAL GOVERNMENT

New mobile technology advances are enabling innovations in immersive training, mobile productivity and security at civilian and defense agencies.

The federal government may have its challenges implementing new technologies, but that doesn't mean there's a lack of vision for how mobile technology capabilities can help agencies innovate and meet objectives more effectively from the office to the mission edge.

That was one of the central messages from top government officials and industry experts at the recent Federal Innovation Summit produced by FedScoop and sponsored by Samsung.

Rapid advances in mobile technology and the rollout of 5G networks, capable of delivering broadband-equivalent download speeds to wireless devices, promise to give federal agencies new tools for innovating, according to experts speaking at the summit.

In particular, officials from federal civilian, defense and intelligence agencies pointed to recent advances in immersive training, workforce productivity and security as just some of the ways agencies can expect to build on the transformative nature of mobile technologies.

"Our ultimate objective is to provide government with the structural capacity for change management," Matt Lira, special assistant for innovation policy and initiatives at the Office of American Innovation in the Executive Office of the President, told a standing-room-only crowd of more than 350 government and industry leaders.

"Technology is continually changing. [Even] if we could modernize the government in an instant, some kid would come up with a new technology," he said. That's why "the government has to not only

be able to modernize in an instant, it has to be able to continually, incrementally modernize itself on an ongoing basis."

At the same time, new technology doesn't guarantee innovation, said former Federal CIO Tony Scott, now senior data privacy and cybersecurity adviser with Squire Patton Boggs.

"Distinguish innovation that matters from innovation that doesn't matter or can't scale," he implored. "One of the mistakes we make, as most institutions do sometimes, is think that all innovation is important."

He also stressed the need for IT leaders "to focus on digital architecture" and find ways to create "common cloud platforms for agencies" to support commonly used processes across government, such as case management.

Steve Rice, the Department of Homeland Security's deputy CIO, echoed the need for "more harmonistic approaches to managing devices" and for "common architectures so you can safeguard citizens' information across agencies." He also pointed to ways DHS might continue to innovate through greater "elasticity" — for instance, "extending passenger checkpoint screening out further, to the airplane."

5G — THE NEXT MOBILE INNOVATION

Many of the innovations emerging in the commercial sector that offer potential value for federal agencies will likely gain added traction from the introduction of 5G networks, the next generation of mobile communications coming to selected markets in the U.S. this year.

Bryan Schromsky, Verizon's managing partner for connected solutions, said that current bandwidth and latency limitations will disappear on a 5G network. Using a 3G network to download "Wonder Woman" at 4K resolution would take 30 hours, he said; on a 4G network it would take 3.5 minutes. By comparison, on a 5G network, it would take just 3.5 seconds.

The advent of ultra-fast, ultra-capacity 5G networks will unleash new capabilities for applications like a smart base or connected battlefield. Much like a smart city in the commercial realm, 5G could enable autonomous vehicles, the Internet of Things, streaming video and virtual, augmented and mixed reality (VR/AR/MR) applications that, for instance, would facilitate immersive medical care and warfighter training.
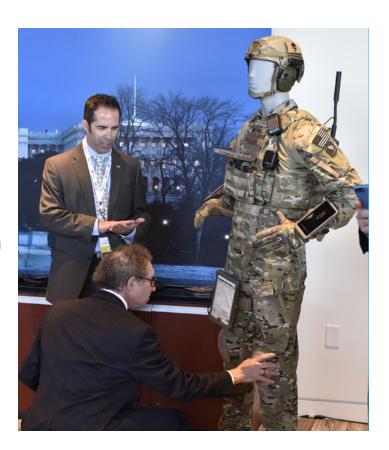
This would be of major value to the military, said Charles Booth, vice president-government of HARMAN, a Samsung company. "There are countless apps we've thought of," he said, such as "games and things we can't do in real life." Augmented reality training modules, for instance, would give law enforcement teams experience to interdict a shooter who is barricaded in place. "There could be infrared images that can be overlaid on their glasses — adding a richness in their environment that right now they don't have."

While Verizon is launching 5G this year in three U.S. markets, Gerald Caron, acting director for enterprise network management at the Department of State, cautioned that adopting such innovations must be balanced against the practical issues many federal agencies face supporting personnel in far-flung international outposts.

"For us based in Washington, it'll be great to take advantage of [5G], but diplomacy takes place in the countries...and there's no fiber or anything in many of these countries," Caron said.

Booth noted, however, how "countries have leapfrogged technologies by putting in wireless." His advice to federal agencies? "You've got to have that part of your organization that's looking ahead" at how 5G will affect their operations.

Schromsky said telecoms such as Verizon will continue 4G deployments for quite a long time precisely because of those kinds of limitations. But the advent of 5G will also have an impact on human capital, Schromsky said. "There's an arms race among

cities," for talent, and modern technology will play an important role in attracting workers, he said.

IMMERSIVE TRAINING INNOVATION

Mobile technology is already transforming how the military thinks about training, through its embrace of VR/AR at the U.S. Army Training & Doctrine Command, according to Tony Cerri, TRADOC's director, data science, models, simulations.

"It's basically on the verge of explosion," he told the audience. "Any time I can get virtual reality in the hands of soldiers, from major on down, I can't get them to give it back," he said.

Thanks to mobile technology, VR/AR can deliver training experiences to personnel in the field instead of forcing personnel to return training centers, he said. Cerri's biggest challenge is getting enough training content for soldiers and finding procurement professionals "who aren't traditionalists," he said. "We need different companies, different experiences to get engaged."

Young Bang, senior vice president at Booz Allen Hamilton, noted that many simulators used by warfighters today are still a couple of decades old. Alternatively, gaming technology — such as first-

person shooter games being used by teenagers today — is far more sophisticated and realistic, he said. The gaming community also uses common tools and products and develops code that others can use. "That needs to come into the government," Bang said.

Both Cerri and Bang suggested that VR/AR for government should be based on open APIs, open data and an open architecture, so code can be reused, leveraged, and expanded. Cerri said simulations should be built that are "data-ready," rather than the government's current emphasis on producing simulation-ready data, and take advantage of mobile technology platforms.

"Samsung's [smartphone] has got more power than your laptop," Bang added. "Every soldier, every law enforcement agent, every person out there, has at least one phone, if not two. We're not using our cellphones enough."

SECURITY INNOVATION

If agencies have been slow to innovate using mobile technology, a contributing factor has been lingering concerns around security. A recent study by FedScoop, underwritten by Samsung, found that more than half of agency IT officials worry about cyberattacks involving endpoint devices as a means of accessing agency networks. Yet many agencies aren't taking advantage of technology they may already have to reduce their risks, the study found.

The Defense Information Systems Agency's mobility capabilities branch chief, Neil Mazuranic, is working on narrowing security concerns by rolling out a "purebred" derived credential certificate that "once installed, will CAC-authenticate users into SIPR (Secret Internet Protocol Router) network sites." DISA is also working on ways at the network layer to verify that a user's wireless signal hasn't been intercepted by deceptive, man-in-the-middle cell networks.

The bigger challenge for agencies, however, is linking mobile technology to legacy systems.

"Honestly, we're still struggling how to use mobile solutions in the security space and have the data security," said Mike Lamont, NSA's associate deputy national manager, national security systems. "When you're talking about how to secure [data], it's legacy technology that doesn't have the built-in security," he said. "Because of that, government is slow to adopt mobile technology."

Lamont highlighted four other security challenges that government and industry need to address:

1 **Ease of physical access.** "It's easy for these small, powerful devices to be stolen," he said, recounting when he witnessed a man on a Baltimore subway train walking by someone talking on their cell phone and he simply snatched it out of their hand and walked off the train.

2 **Lack of end-to-end encryption.** Devices can become targets for malware looking to steal data. "Hopping from network to network, doesn't work," Lamont said. "Sensitive government information has to be secure at all times."

3 **Poor update management.** Smartphones are only as secure as the managers and users who do their updates. Mobile doesn't push out its updates. And relying on device owners is problematic: Four in 10 people only update when it's convenient, and another one in 10 say they never update their cellphones, he said, citing findings from an unnamed study.

4 **Securing the supply chain.** That includes not only understanding where the parts that go into mobile devices come from, but the security measures put in place every step of the way. "It's a very complex challenge to solve," Lamont said. "Getting it right isn't a luxury, it's a necessity."

Above: Mike Lamont at the Federal Innovation Summit produced by FedScoop and sponsored by Samsung.

But new technology capabilities are making mobile devices more secure. Samsung's Knox, which has security baked-in from the hardware level up, can isolate data on mobile handsets, for instance. This type of solution can help make mobile devices more secure than many PCs and enable greater productivity for federal workers who need their data protected no matter where the mission takes them.

INNOVATION AND WORKFORCE TRANSFORMATION

While much of the talk about digital transformation of the government appropriately concentrates on enabling agencies and improving citizen services, another area where innovation is both desperately needed and holds great promise is in human capital management and workforce transformation, experts at the summit said.

With the government facing "a large number of folks eligible for retirement," and a real shortage of new employees, finding ways to incorporate new and emerging technologies becomes a priority, said Veronica Villalobos, principal deputy associate director, Employee Service, Office of Personnel Management.

OPM, as part of a 2018 priorities report, scanned across agencies to find what tools agencies are using to foster more effective collaboration and create databases of shared knowledge, Villalobos said. GSA, for instance, is using Slack, "which is helping them do work across regions of the country. [The Department of] Energy and the intelligence community – they've set up systems very much like Wikipedia...so people have access to the latest information."

Towanda Brooks, Chief Human Capital Officer for the Department of Housing and Urban Development, said the department's Office of the CIO is working closely with her office to reimagine how HUD operates through incorporating up-to-date technology. For instance, the department has held "HUD innovation days," Brooks said.

"A lot of good things have come out of innovation days...We developed apps where you can find apartments or places to live; an employee developed it to find a rental property," she said.

Recruiting young people into government service, especially those who've grown up on mobile technology, remains a common lament.

They are so accustomed to using the latest and greatest technology in their personal lives, said Villalobos, it doesn't make sense why they have to leave their personal devices at the door of their government employer and use older technology.

Learn more about how Samsung, a leader in government-approved mobile technologies, can help your agency update your mobile environment and make it as safe and secure as it can be — today and tomorrow.