The Future of Work

Highlights from a Government Roundtable, hosted by ATARC, in partnership with Privoro April 2023

Government agencies are increasingly accepting of a fact that enterprise organizations have long known to be true: mobile devices are the future of work. Fortunately, approved secure mobility solutions are now available, enabling agencies to safely leverage mobile devices for countless use cases critical to mission outcomes. But as technology quickly advances, policies inevitably become outdated, challenging agency efforts to adopt secure mobility.

At a recent roundtable discussion hosted by the Advanced Technology Academic Research Center, a group of 30 experts and stakeholders from the Federal government and industry came together to discuss the ins and outs of adopting secure mobility, including how to best navigate the many implementation challenges.

Facing Our Mobile Reality

> **"The reality of the future is more mobility. So we're not really debating the if; we're debating the how and the when we get there."**

Virtually every individual working in the Federal government owns a personal smartphone and relies on it for communication and situational awareness in their personal lives. Furthermore, successful implementations of remote work during the pandemic have laid bare the value these devices provide in enabling personnel to get their jobs done from anywhere.

In light of these two realities, policies that effectively ban mobile devices from being used for work create an increasingly untenable situation for organizational effectiveness. For example, without access to an approved mobile device, personnel may waste precious time printing slide decks for meetings and making handwritten notes. Outside of the office, personnel tend to become effectively unreachable, hampering the speed of decision-making.

In a broader sense, not giving personnel access to the digital tools they know is a recipe for discontentment. Individuals may have a harder time keeping in touch with their family during work hours, for example. And, as younger generations are generally inseparable from their phones, an organization's ability to recruit the next-generation workforce is severely constrained. As one participant stated, "In order to attract the best talent, we have to be more open-minded of where that talent works."

Despite this chasm between reality and possibility, roundtable participants were optimistic about the potential of secure mobility on mission outcomes. Some use cases identified include enabling phones in secure spaces, supporting remote work, facilitating nimble digital access across office environments and supporting emergency operations.

Designing Secure Mobility for the Future of Work

> **"From a technical security perspective, never before have we been closer to being able to implement a robust yet secure solution for mobility."**

Any secure mobility solution first needs to address the legitimate security concerns expressed by security teams within government agencies. The overarching challenge – using unclassified commercial devices for classified operations – is a large one. Risks unique to mobile devices include active espionage via the device's cameras and microphones and data exfiltration via the device's radios.

Participants stated that the secure mobility solution must work off a fundamental assumption: that the device, either purposefully or accidentally, is malevolent. Such an approach not only plays into Zero Trust initiatives but also serves to overcome technical limitations around the lack of visibility into both device health and the broader wireless environment.

Secure mobility solutions are now available that treat the commercial mobile device as untrusted while giving security teams trusted control over individual components like sensors and radios. With the proper controls and technical countermeasures, an organization can greatly mitigate the risks of device compromise or insider threat.

The rise of wearable technology is another important aspect of mobile security for agencies to consider. Many personnel need to connect hearing devices to their phones, for example, or sync personal glucose monitors or insulin pumps to their phone apps.

Agencies should also consider advancements in quantum technology when thinking about mobile security. Panelists seemed confident that quantum security protections will not only change the game for secure mobility, but these advancements are closer than we think.

Navigating the Policy Process

> **"From a counterintelligence perspective, that's always the answer: 'Zero risk. We don't want any risk.' But you can't. We don't live in a zero-risk world."**

Roundtable participants considered a lack of workable policies to be the biggest hurdle to widespread adoption of secure mobility. As one participant put it, "Tech is outpacing our ability to produce policy."

In creating policy that's current and relevant, agencies face a number of challenges.

Culturally, it's much easier and quicker for leaders to just say no to an emerging secure mobility solution. However, risk aversion is not the same as risk management. Said one participant, "If we can't provide our people and our frontline operators the tools, they're going to go around us."

If policy is written to accommodate secure mobility, the internal government legal review process can take months, which means that a policy may already be outdated by the time it's released. And when it is released, different stakeholders may offer different guidance around the policy. Linking all of these different policies and interpretations together is a challenge.

What's needed is an overarching mobility framework – perhaps in the mold of the NSA's Commercial Solutions for Classified (CSfC) – that accommodates new secure mobility solutions and takes into account the various use cases, including travel and remote work. Changing the policies of dozens of agencies takes significant coordination, research and resources. However, the alternative is no longer a viable option.

Final Thoughts

"There's more work to be done, but we have the makings of a start right here, now, today."

Secure mobility adoption is an inevitability, one that promises to modernize how government agencies carry out their missions. But because leaders looking to enable secure mobility run up against hurdle after hurdle in gaining the necessary approvals in line with policy, it's easier to bury one's head in the sand and pretend the problem doesn't exist.

In the short term, this approach may pass muster. But with each passing day, the organization gets slower, less dynamic and less capable of keeping up with the accelerating demands placed on it. Furthermore, without secure mobility solutions in place, security managers lack the active controls they need to mitigate risk. The risks of leveraging secure mobility are ultimately outweighed by the risks of not doing so.

Instead of letting individual leaders go it alone in their pursuit of secure mobility, it's time to work together across agencies to create the framework under which organizations and teams can confidently build and refine their approaches to secure mobility.