ATARC powered by GovExec

EXECUTIVE SUMMARY

A Government That Works, Effectively, From Anywhere: A Security Policy and a Mobile Capability Evolution

ATARC Future of Secure Work Working Group

On February 18, 2025, ATARC hosted a webinar that brought together government and industry leaders to discuss how to modernize secure work using existing technologies. Meeting metrics is not the objective—reducing real-world risk is.

The need

Participants understood the need for an evolution of the government's mobile capability.

Today, whenever a decision needs to be made quickly or information must be shared as soon as possible, personnel are tempted to use their mobile devices, even if policy doesn't allow for it. In other situations, such as work inside restricted areas, phones are essentially banned, limiting situational awareness and capability.

Organizations that don't fully utilize mobile capabilities risk sacrificing the mission as the world becomes ever more mobile-centric, falling behind peers and adversaries who have figured out how to move at modern speed.

The vision

Participants shared a vision for the future of secure work, one where each individual is issued an unclassified mobile device – hardened to government standards – that can be used anywhere and for any task, including for travel and unexpected events. Empowered with mobile devices, personnel are better able to meet the mission, doing critical work no matter the situation.

These devices would be governed by a common approach that allows for scalable adoption by disparate organizations.

Mobile devices can potentially even replace laptops and desktop phones, reducing capital expenses while limiting the attack surface to a single device.

ATARC

The challenges

Participants identified the many challenges at driving mobility within government and examined some potential solutions.

One key challenge is the sheer diversity of organizations, use cases, buildings and classifications that must be supported. Each organization has its own set of policies, and the enforcement of standards may vary between organizations. Establishing a common framework that can flexibly accommodate these various requirements is key.

Other challenges include elevated requirements around recordkeeping and protecting classified information, a lack of interoperability among security tools, and the need to protect users from sophisticated mobile attacks and data collection. Participants were confident that industry partners would help tackle these challenges.

A call to action

To flesh out this common mobile framework and meet the moment, participants said that government must shake up its culture, which has a reputation for being risk-averse, insular and slow. Organizations with low appetites for risk must learn to embrace it, with proper mitigations, to support the mission, including by leveraging new technologies that haven't yet reached mass adoption. Organizations must also tear down their silos, both cultural and technical, and learn to share best practices internally and with other organizations, fostering a culture of innovation. And the creation of policies and standards must move quickly enough to account for the latest technologies, enabling industry to better meet the needs of government.

Now is the time for bold action. Rather than cede the mobile turf to competitors, leaders in government and industry must work together to realize a vision for secure mobility, one that advances the mission while keeping sensitive information out of the wrong hands. The future requires nothing less.