



ATARC WEBINAR EXECUTIVE SUMMARY

# Making **it** Happen

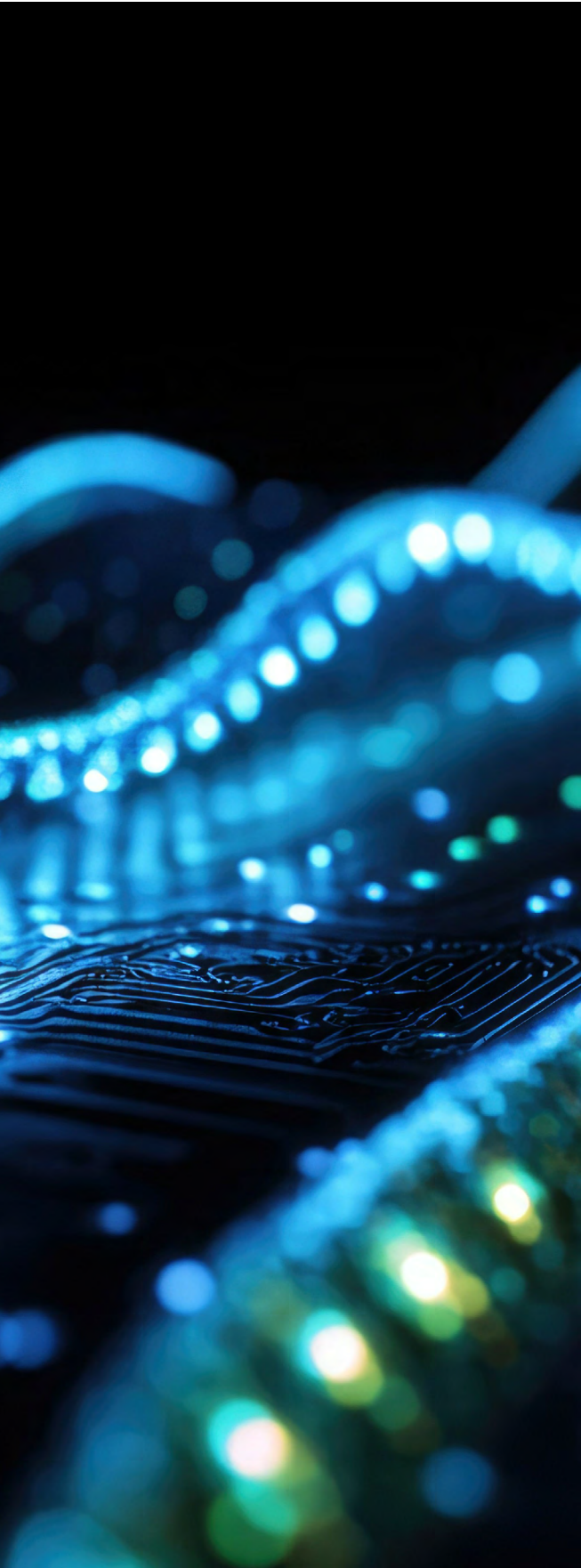
How One United States Government  
Organization is Implementing  
Mobility in Secure Spaces



*ATARC Threat Intelligence Working Group*

## Table of Contents

Introduction _____	<b>3</b>
Background _____	<b>3</b>
Drivers for Secure Mobility _____	<b>4</b>
Technology Initiatives _____	<b>4</b>
Challenges and Solutions _____	<b>5</b>
Implementation Guidance _____	<b>7</b>
Security and Future Considerations _____	<b>8</b>
Conclusion _____	<b>8</b>



# Introduction

The rapid evolution of workplace technology and the increasing demand for secure, flexible work environments have driven organizations—especially those operating in sensitive or classified domains—to rethink their approach to mobility and security. The “Making it Happen: How One United States Government Organization is Implementing Mobility in Secure Spaces Webinar” provided a comprehensive exploration of the challenges, solutions, and future directions for secure mobility, with a focus on aligning technology, policy, and workforce needs. This executive summary distills the key themes, lessons learned, and actionable guidance discussed during the session, offering a roadmap for organizations seeking to enable secure work from anywhere.

**On June 10, 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.

# Background

As organizations modernize, the imperative to support remote and mobile work has intensified. The shift is not merely technological but also cultural and operational, requiring a holistic approach that addresses risk, compliance, and workforce expectations. The session highlighted that the journey toward secure mobility is shaped by both external pressures—such as evolving threats and regulatory requirements—and internal drivers, including workforce demands and mission effectiveness.

# Drivers for Secure Mobility

The adoption of secure mobility solutions is rooted in two primary drivers: secure mission effectiveness and workforce enablement. Organizations operating in non-secure and secure environments face unique challenges in balancing the need for operational agility with stringent security requirements. The demand for mobile solutions often originates from the workforce itself, particularly new hires who expect seamless access to technology as a baseline for productivity and engagement.

This grassroots demand is complemented by strategic leadership, which recognizes that enabling secure mobility can yield significant benefits in terms of efficiency, recruitment, and retention. The convergence of bottom-up and top-down pressures creates a powerful impetus for change, compelling organizations to explore innovative solutions that address both security and usability.

## Technology Initiatives

A range of technology initiatives were discussed as part of the secure mobility transformation. These include:

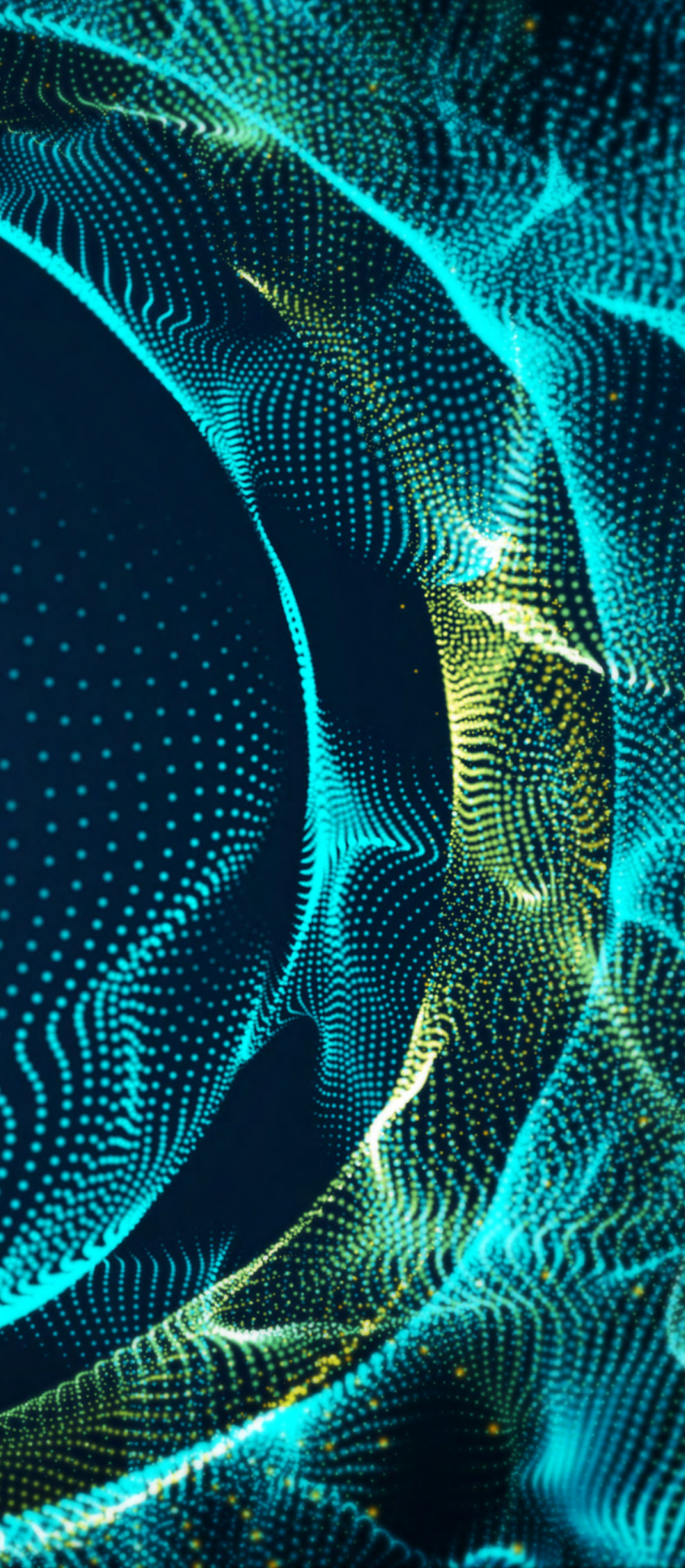
- **Classified and Unclassified Wireless Solutions:** Deployment of wireless

networks in both classified and unclassified spaces, enabling secure communication and data access while maintaining compliance with security protocols.

- **RFID Projects:** Implementation of radio-frequency identification (RFID) technology to streamline inventory management and asset tracking, resulting in substantial improvements in accuracy and efficiency
- **Digital Procedures:** Transition from manual, paper-based processes to digital workflows, leveraging mobile devices to enhance productivity and reduce errors
- **Secure Mobile Device Cases:** Introduction of specialized cases for mobile devices that enforce security controls, such as disabling cameras and wireless radios, to permit their use in sensitive environments without compromising security.
- **Wireless Detection Systems:** Investment in systems that monitor and control the presence of unauthorized wireless devices, further mitigating the risk of data leakage or unauthorized access. These systems increase cybersecurity and control, which can lead to cost savings by reducing risk and unauthorized device proliferation.

These initiatives are not isolated projects but part of a broader strategy to modernize operations and create a more agile, responsive organization.





# Challenges and Solutions

The journey toward secure mobility is fraught with challenges, many of which are cultural as much as technical. Key challenges and corresponding solutions discussed include:

## Cultural Resistance

Institutional risk aversion and resistance to change are common obstacles. Overcoming these barriers requires a combination of leadership support, clear communication, and a willingness to challenge established practices. Change agents within the organization play a critical role in advocating for new approaches and building consensus among stakeholders.

## Cost and Return on Investment

Secure mobility solutions often entail significant upfront costs, both in terms of technology acquisition and implementation. To justify these investments, organizations must develop robust business cases that articulate the expected return on investment (ROI). Examples cited include dramatic improvements in inventory accuracy (up to 90%) and reductions in inventory processing time (up to 80%), as well as increased manufacturing throughput and workforce productivity.

A leadership decision and investment accelerated the adoption of RFID technology by an estimated five years within their mission space.

## Risk Management

A pragmatic, project-based approach to risk management is essential. Rather than applying blanket refusals to new technologies, organizations are encouraged to conduct thorough risk analyses and implement targeted mitigation strategies. This approach enables informed decision-making and allows for the controlled introduction of new capabilities.

## Policy and Reciprocity

Navigating complex approval processes and inconsistent standards across agencies can impede progress. Efforts to streamline these processes and promote reciprocity—whereby security approvals are recognized across different parts of the organization or between agencies—are ongoing. Such initiatives are critical to reducing friction and accelerating the adoption of secure mobility solutions.

## Technical and Operational Hurdles

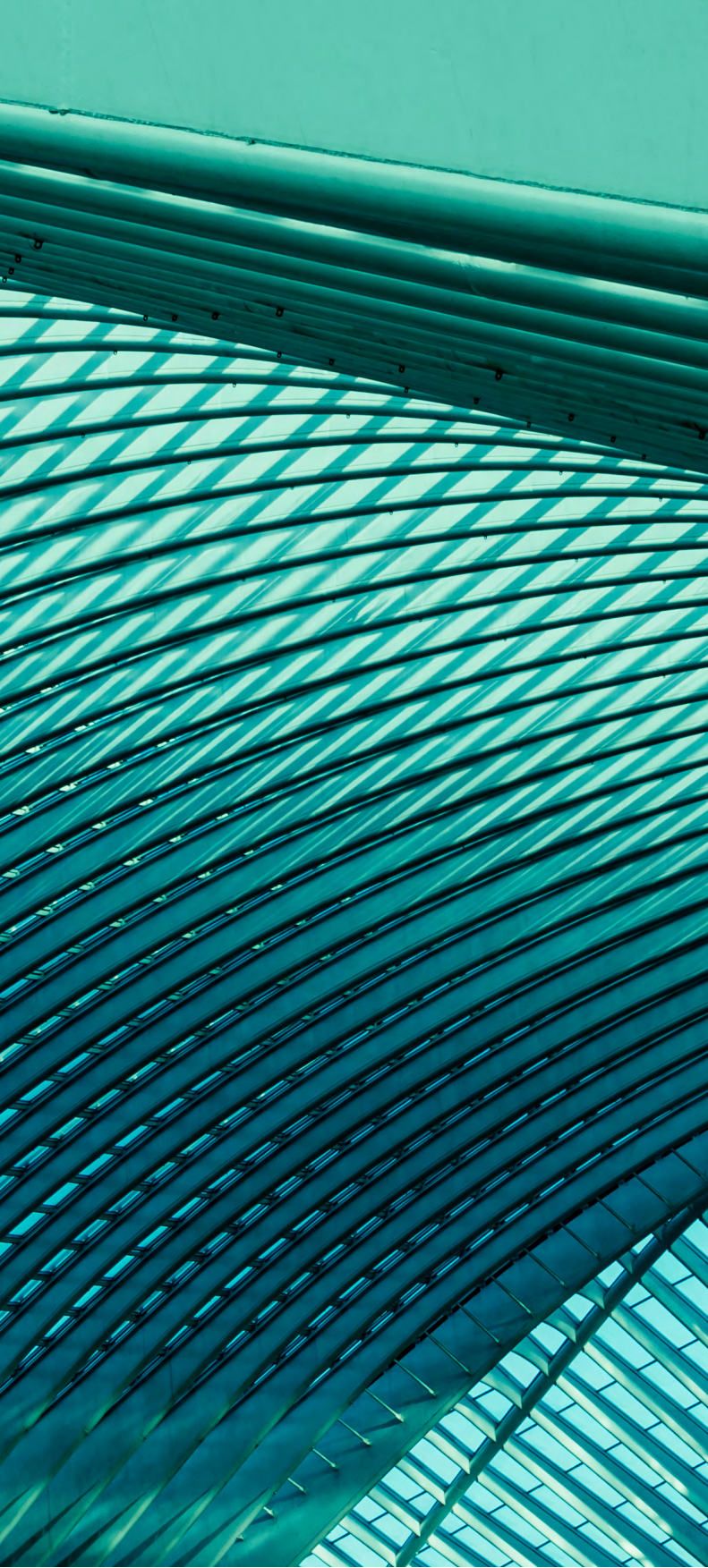
Technical challenges, such as integrating new devices into existing infrastructure and ensuring compatibility with legacy systems, must be addressed through careful planning and pilot testing. Operationally, organizations must balance the need for security with the imperative to maintain mission continuity and workforce satisfaction.

## Workforce Impact

The impact of secure mobility initiatives on the workforce is profound. By enabling employees to access the tools and information they need, regardless of location, organizations can drive significant gains in efficiency and job satisfaction. Notable outcomes include:

- **Enhanced Productivity:** Mobile solutions have enabled faster, more accurate completion of critical tasks, such as inventory management and manufacturing processes.
- **Recruitment and Retention:** The ability to offer flexible, technology-enabled work environments is increasingly important for attracting and retaining talent, particularly among younger employees who expect seamless access to digital tools.
- **Workforce Engagement:** Involving employees and listening to their needs can be foundational to the successful adoption of mobility solutions, fostering both ownership and engagement throughout the process.





# Implementation Guidance

Drawing on the experiences shared during the session, several best practices emerge for organizations seeking to implement secure mobility:

## Engage the Workforce

Successful initiatives begin with a clear understanding of workforce needs and preferences. Organizations are encouraged to solicit input from employees at all levels, using surveys, focus groups, or informal feedback mechanisms to identify pain points and opportunities for improvement.

## Secure Leadership Sponsorship

Secure mobility is most effective when championed by leaders who can provide strategic direction and remove obstacles. Securing sponsorship from senior leadership ensures that mobility initiatives receive the necessary resources and attention.

## Develop Robust Business Cases

Investments in secure mobility must be justified through clear, data-driven business cases. Organizations should quantify the expected benefits—such as time savings, error reduction, and improved mission outcomes—and use these metrics to guide decision-making.

## Pilot and Iterate

Pilot projects allow organizations to test new solutions in controlled environments, gather feedback, and make necessary adjustments before full-scale deployment. Iterative implementation enables continuous improvement and reduces the risk of costly failures.

## Challenge Assumptions

Many barriers to secure mobility are based on assumptions rather than facts. Organizations should critically evaluate perceived obstacles and seek evidence-based solutions, rather than accepting “no” as the default response.

## Foster a Culture of Innovation

Encouraging experimentation and learning from both successes and failures is essential for driving innovation. Organizations should create environments where employees feel empowered to propose and test new ideas.

# Security and Future Considerations

The evolving threat landscape requires organizations to remain vigilant and adaptable. Key considerations for the future include:

- **Layered Security Controls:** Employing multiple layers of encryption and access controls to protect sensitive information, both in transit and at rest.

- **Wireless Intrusion Detection:** Monitoring for unauthorized devices and signals to prevent data leakage and maintain situational awareness.
- **Emerging Threats:** Staying abreast of developments in artificial intelligence and quantum computing, and adapting security strategies accordingly.
- **Continuous Risk Assessment:** Regularly reviewing and updating risk management practices to address new vulnerabilities and ensure ongoing compliance.

Organizations are also encouraged to collaborate with peers and industry partners to share best practices and stay informed about emerging technologies and threats.

## Conclusion

The experience shared in the “Making it Happen: How One USG Organization is Implementing Mobility in Secure Spaces Webinar” demonstrates that secure mobility is not only possible but also highly beneficial in sensitive environments. By aligning technology, policy, and people, organizations can achieve significant gains in efficiency, security, and workforce satisfaction. The journey requires engagement at all levels, a willingness to challenge assumptions, and a commitment to continuous improvement. As the workplace continues to evolve, secure mobility will remain a critical enabler of mission success.