carahsoft

BlackBerry

Enhancing Officer Effectiveness with Certified Tools

Secure, Policy-Enforced Mobility for Federal Operations

Thank you for your interest in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies through GSA, NASPO ValuePoint, The Quilt and a wide range of other contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with BlackBerry, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.

To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com

Explore More Resources:
carah.io/blackberryresources

Join Events & Webinars:
carah.io/blackberryevents

Discover Technology Solutions:
carah.io/blackberrysolutions

Learn About Procurement:
carah.io/blackberrycontracts

Connect With Our Team:
BlackBerry@carahsoft.com
(855) 346-6346

Enhancing Officer Effectiveness with Certified Tools

Secure, Policy-Enforced Mobility for Federal Operations

Executive Summary

Federal agencies operate in increasingly mobile, distributed, and time-sensitive environments where secure communication and device integrity are critical to mission success. Personnel routinely rely on commercial mobile networks and modern smartphones to coordinate operations, share sensitive information, and maintain situational awareness across locations.

However, traditional communication tools and unmanaged mobile environments can introduce risk. Fragmented workflows, inconsistent device security, and reliance on applications not designed for government use may expose sensitive communications or operational patterns and reduce visibility for leadership during critical events.

BlackBerry® SecuSUITE® and BlackBerry® Unified Endpoint Management (UEM) provide a unified, mobile-first approach to secure communications and endpoint control. Together, they enable encrypted voice and messaging alongside continuous device compliance and policy enforcement—supporting secure coordination without disrupting how personnel operate in the field.

Operational Challenge – 2026 Federal Operating Environment

Federal missions increasingly require:

- Real-time coordination across distributed teams and jurisdictions
- Secure communications over commercial and potentially untrusted networks
- Rapid inclusion of additional personnel as situations evolve
- Reliable access to mission-critical information in dynamic environments

Common approaches can create gaps:

- **Legacy communication tools** may lack interoperability, modern data-sharing capabilities, and centralized visibility
- **Consumer-grade messaging applications** are not designed to meet federal security, compliance, or auditability requirements
- **Unmanaged or inconsistently managed devices** may introduce risk through misconfiguration, data leakage, or lack of enforcement

These gaps compel personnel to choose between speed and security during critical moments. Recent U.S. government advisories further reinforce this shift in risk. In March 2026, the Cybersecurity and Infrastructure Security Agency (CISA) warned that threat actors are actively targeting endpoint management systems and leveraging legitimate administrative tools to disrupt operations, underscoring the importance of strong access controls and policy enforcement.

In parallel, federal law enforcement reporting has highlighted large-scale phishing campaigns targeting commercial messaging platforms, where attackers gain access to accounts by exploiting identity and user trust rather than breaking encryption.

Together, these developments illustrate that risk is increasingly concentrated at the device, identity, and management layers—areas that require coordinated security controls beyond standalone tools.

Integrated Solution Overview

BlackBerry SecuSUITE and BlackBerry UEM work together as an integrated operational layer that combines secure communications with device-level enforcement. Together, these capabilities support secure communications on devices that can be configured and enforced to meet mission-specific security requirements.

This approach allows agencies to:

- Enable encrypted voice, messaging, and data exchange
- Enforce mobile security policies consistently across devices
- Maintain visibility and accountability for operational communications
- Support both government-furnished and bring-your-own-device (BYOD) environments

The solution is designed to operate on standard iOS, Android, and desktop devices, allowing personnel to use familiar tools while security and policy controls are applied in the background. These capabilities are deployed today across global governments and intensely regulated corporate environments.

BlackBerry SecuSUITE – Secure Voice and Messaging Communications

BlackBerry SecuSUITE provides end-to-end encrypted voice, messaging, and file-sharing capabilities designed for sensitive government communications.

Key capabilities include:

- **Supports secure voice and messaging with identity verification tools** across mobile (iOS & Android) helping reduce the risk of unauthorized access
- **Controlled communication environments** that limit exposure of sensitive information and limit metadata exposure
- **Secure group communications**, allowing additional participants to be included as needed
- **Operation across commercial and variable network conditions**
- **Support for deployment in agency-controlled or isolated environments**, enabling secure communications continuity in constrained, disconnected, or high-security operating conditions

SecuSUITE is designed to deliver strong security while maintaining a user experience comparable to modern mobile applications, minimizing training requirements and operational disruption.

BlackBerry UEM – Secure Mobile Foundation

BlackBerry UEM provides centralized endpoint management and security enforcement across mobile devices used in federal environments.

Key capabilities include:

- **Continuous device compliance monitoring** with policy-based enforcement
- **Granular control over applications and data movement**
- **Support for secure containers and application separation**, helping protect mission data while preserving user privacy
- **Remote management capabilities**, including lock and wipe when required
- **Policy-driven device hardening and configuration control,** enabling agencies to restrict functionality, enforce security baselines, and operate devices in tightly controlled environments

UEM enables agencies to manage risk at the device level while maintaining usability for personnel operating in the field and strengthening control over high-impact device management functions and enabling operation within tightly controlled or mission-specific environments.

Operational Value & Impact

When deployed together, SecuSUITE and UEM provide a coordinated approach to secure communications and endpoint management.

For frontline personnel:

- Faster coordination without switching between multiple tools
- Ability to securely communicate in dynamic or high-risk situations
- Confidence that communications are protected while maintaining ease of use

For leadership and command elements:

- Improved visibility into communications workflows
- Support for auditability and post-incident review
- Consistent enforcement of security policies across users and devices

For agencies:

- Reduced reliance on civilian communication surfaces
- Improved alignment with federal security and compliance frameworks
- A scalable approach to securing mobile communications across diverse missions

Security & Compliance Alignment

BlackBerry SecuSUITE and UEM are designed to support alignment with key federal security frameworks and standards, including:

- NSA Commercial Solutions for Classified (CSfC) component-based approaches
- NIAP Common Criteria evaluated components
- FIPS 140-2 and 140-3 validated cryptographic modules
- Federal Zero Trust architecture principles

Implementation and accreditation remain subject to agency-specific requirements, configuration, and authorization processes.

Conclusion

Secure communications and mobile device integrity are foundational to federal communications systems, such as email. As missions become more distributed across mobile devices, agencies require solutions that maintain strong security and policy enforcement. BlackBerry SecuSUITE and UEM provide an integrated approach that supports encrypted communications, device compliance, and operational visibility—without requiring specialized hardware or complex workflows.