BlackBerry | Secure Communications

Safeguarding National Interests:

A Strategic Guide to Supporting Public Safety Through Secure, Sovereign Technology

Executive Summary

Security of a nation relies on infrastructure that is sovereign-controlled and designed to meet high standards of trust. As cyber, geopolitical, and physical threats escalate, the ability to make decisive calls under pressure has never been more critical. Secure mobile communication isn't a nice-to-have—it's the backbone of mission success.

Public safety agency mandates include safeguarding national security, managing emergencies, protecting borders, and preventing crime. All of this relies on secure, uninterrupted communication that withstands operational pressure, external interference, and adversarial tactics.

Outdated systems pose significant challenges. Legacy infrastructure and weak identity controls can create serious vulnerabilities. Additionally, consumer-grade platforms often lack the oversight, certifications, and resilience needed for mission assurance. Public safety and national security require more careful consideration.

This guide lays out a clear, actionable path forward:

- A deep dive into today's threat landscape and vulnerabilities.
- A compelling case for adopting sovereign, independently operated communication solutions.
- Real-world examples of how insecure systems can derail mission success.
- Practical steps to fortify a national digital infrastructure and sustain public trust.

Governments worldwide rely on BlackBerry® solutions for critical operations. These implementations demonstrate effective ways to address complex challenges. Our certified platforms deliver the resilience and reliability needed for secure, sovereign communication.

Establishing a new standard for trusted communication can enhance national operational continuity, preparedness, and public confidence. BlackBerry provides rigorously validated solutions that align with these objectives, supporting operational continuity and public trust.

A Nation Under Pressure: Threats and the Public Safety Mandate

Governments operate within a risk environment that is both immediate and consequential. State-sponsored actors use advanced cyber tools to penetrate institutional systems, gather sensitive intelligence, and threaten the stability of democratic processes. Orchestrated disinformation campaigns challenge societal cohesion and burden response systems. Targeted attacks on critical infrastructure—including power grids, transportation, and emergency networks—underscore the need for secure and decisive communication.

Public safety agencies are responsible for safeguarding:

- National security
- Emergency management
- Crime prevention
- Border integrity
- Operational continuity

These priorities are deeply interconnected. A single failure can cascade, placing community welfare and national stability at risk.

Effective public trust depends on proven resilience, sovereign control, and transparent operational assurance. Secure communication is foundational to achieving strong public safety outcomes, with solutions like those offered by BlackBerry addressing these needs.

Sovereign, trusted digital systems must:

- Operate independently, free from external or third-party interference
- Maintain operational continuity in crisis scenarios—not just day-to-day operations
- Provide governments with ownership, stewardship, and governance over sensitive public safety information

Gaps in communications erode coordination, waste critical time, and diminish public trust. Robust assurance is imperative for all mission-critical environments.

Case in Point: Signalgate

The vulnerabilities in secure communications were made evident during the Signalgate incident, where a journalist was mistakenly included in a military coordination channel. The core failure was not encryption but inadequate access controls and identity verification.

Consumer-grade applications may offer convenience, but they consistently lack:

- Reliable, independently verifiable audit trails
- Role-based governance for high-sensitivity channels
- Regulatory compliance and sovereign oversight

From this breach, two operational lessons are clear:

- Human error, even if accidental, can lead to immediate and far-reaching exposure
- Capable adversaries exploit both metadata and unseen infrastructure gaps, often without detection

For national security and public safety, reliance on technology not fit for critical operations is a liability.

The lesson: mission assurance is supported by rigorously governed, sovereign, and validated communications. These vulnerabilities can be addressed through solutions that provide robust access controls, identity verification, and independently verifiable audit trails, such as those offered by BlackBerry.

Building Secure and Trusted Communications

Effective government operations and decision-making require technology that is both robust and accountable. In crises or during routine intelligence sharing, leaders must have full confidence that all communications—voice, data, emergency response—are sovereign-controlled and secure.

Government regulatory frameworks requires that communications platforms provide:

- End-to-end encryption covering content and metadata
- Cryptographically enforced identity validation, limiting access to authorized personnel
- Centralized, granular access controls to prevent privilege escalation and segment operational layers
- Comprehensive auditability supporting compliance, transparency, and investigations
- Sovereign deployment using government-owned infrastructure—on-premises, air-gapped, or national cloud

Continued dependency on non-sovereign technologies impedes resilience, weakens crisis response, and exposes critical public safety systems to foreign risk.

BlackBerry® Secure Communications certified solutions, are engineered to address risks such as interception and metadata leaks, providing government agencies with trusted, sovereign-controlled communications. It replaces vulnerable platforms with trusted, sovereign-controlled mobile communications on both enterprise and personally owned mobile devices.

Strengthening Emergency Preparedness and Crisis Response

Emergencies—from wildfires and floods to cyber incidents and public health crises—test the effectiveness of operational frameworks. Fragmented communications introduce the risk of cascading failures, delayed coordination, and reduced public confidence.

Government emergency management principles require communications solutions that enable:

- Real-time, multi-channel alerting—across mobile, desktop, SMS, and public signage
- Role-based, virtual incident management rooms for rapid, intelligence-driven decision-making
- Geo-targeted notifications to ensure timely instructions reach only those affected
- Bi-directional field communication for immediate feedback and intelligence gathering, even under degraded network conditions
- Resilience to maintain operations when conventional infrastructure fails

Experience proves this imperative: During the 2023 Canada wildfires, robust sovereign communications enabled effective mass evacuation and cross-province resource allocation. During the global COVID-19 pandemic, secure networks moved confidential public health directives and logistics directly to the frontline. BlackBerry Secure Communications has also provided situational awareness and crisis response in U.S. federal operations during the January 6 riots.

Protecting Infrastructure and Border Integrity

Safeguarding infrastructure and border operations is a strategic necessity for both public safety and economic security. Disruption of communications at entry points—pipelines, airports, ports, and customs facilities—poses a nationwide risk.

Incidents like Salt Typhoon highlight the urgency for solutions that:

- Keep sensitive communications within government jurisdiction, isolated from foreign-controlled infrastructure and external cloud risk
- Encrypt all strategic coordination among agencies, preventing interception or exploitation
- Enable segmented intelligence sharing through granular controls and reliable audit trails

To uphold operational continuity, legal compliance, and public confidence, public safety agencies cannot depend on vulnerable third-party solutions. Secure communication solutions, such as those offered by BlackBerry, can support trusted, regulated, and scalable communications that adapt to evolving national needs.

Ensuring Continuity and Building National Resilience

Resilience involves maintaining leadership, continuity, and operational capability even when routine systems are disrupted. Programs that ensure national continuity—whether facing disaster, conflict, or critical service interruptions—require sovereign, trusted communications.

Cornerstones of resilience include:

- Functioning independently of compromised or public networks
- Ensuring secure, federated agency handoff to maintain seamless coordination and information flow
- Utilization of failover communication paths for uninterrupted command and control
- Equipping decision-makers with communications assurance so public trust remains intact, regardless of circumstances

Secure mobility solutions and proven deployment models can support continuous control during attacks or outages, enhancing preparedness for future emergencies.

A Shared Responsibility to Protect the Nation

National security and public safety are realized through coordinated leadership across government, trusted technology partners, and operational authorities. For over four decades, BlackBerry has demonstrated its ability to support operational efficiency, digital sovereignty, and leadership in mission assurance.

Public safety agencies play a crucial role in protecting the nation. By collaborating with trusted technology partners, it can enhance operational efficiency, ensure digital sovereignty, and solidify its leadership in mission assurance.

These certifications and deployments demonstrate how BlackBerry Secure Communications is ability to meet the stringent requirements of government agencies.

Current Government and Allied Deployments:

- United States: Over 75% of federal agencies rely on BlackBerry for emergency and classified mobile communications
- Germany: Nationwide adoption for sovereign government mobile
- NATO: Endorsed for NATO Restricted and allied military operations
- G20: Demonstrated capabilities in intelligence and defense environments

Core Certifications:

- Communications Security Establishment (CSE) certified for Canada Secret
- NATO Communications and Information Agency for NATO Restricted
- NSA Commercial Solutions for Classified (CSfC)—Top Secret encryption
- German BSI EAL4, Common Criteria, NIAP, and FIPS 140-2 validations

Modernizing Public Safety Communications: A Strategic Roadmap

A nation's ability to advance operational readiness hinges on strategic modernization and sovereign control. Purpose-driven innovation moves the nation closer to a resilient public safety environment, anticipating threats and safeguarding citizens.

1. Establish Sovereign Foundations

Implementing government-grade communications for all public safety agencies, ensuring sensitive data never leaves domestic jurisdiction or relies on foreign-managed infrastructure.

2. Assert National Control

Maintaining end-to-end ownership of communications infrastructure, identity management, and system access—aligned with government privacy and data sovereignty mandates.

3. Accelerate Readiness

Champion interagency exercises to proactively test resilience, validate operational readiness, and fortify practices under real-world threat conditions.

4. Co-Develop Mission Capabilities

Integrating solutions developed in direct partnership with frontline users and BlackBerry expertise, aligned to the realities of public safety missions.

5. Scale Nationally, Strengthen Innovation

Prioritizing national interests by scaling validated technologies that secure national interests and invest in domestic capacity.

6. Deliver With Urgency, Without Compromise

Utilizing rapid deployment protocols—trusted in urgent, high-stakes scenarios—to close capability gaps at mission speed.

BlackBerry Secure Communications solutions support these modernization efforts by providing government-grade communications and accelerating readiness through secure, interoperable platforms.

Nations deserve systems built for the mission. BlackBerry is ready to deliver.

Let's secure the future together.

Talk to an expert

Contact us today to learn more about BlackBerry Secure Communications, visit blackberry.com/securecomms

ABOUT BLACKBERRY

BlackBerry (NYSE: BB; TSX: BB) provides enterprises and governments the intelligent software and services that power the world around us. Based in Waterloo, Ontario, the company's high-performance foundational software enables major automakers and industrial giants alike to unlock transformative applications, drive new revenue streams and launch innovative business models, all without sacrificing safety, security, and reliability. With a deep heritage in Secure Communications, BlackBerry delivers operational resiliency with a comprehensive, highly secure, and extensively certified portfolio for mobile fortification, mission-critical communications, and critical events management.

For more information, visit BlackBerry.com and follow @BlackBerry.

BB25 | 250206