FBI Cyber Strategy

September 9, 2026

Overview

Released on September 9, 2026, the FBI Cyber Strategy provides a roadmap for defending the nation's cyberspace and critical infrastructure. Across four pillars, the Federal Bureau of Investigation commits to accelerated threat intelligence sharing, cryptocurrency tracing, industrial control system expertise in every field office, implementation of agentic AI, and preparation for post-quantum cryptography (PQC).

Together, these pillars describe a need for acquisition of commercial products on a multi-year timeline that will weigh evidentiary auditability as heavily as technical performance.

The Strategy

The strategy defines FBI Cyber's mission as imposing cost on adversaries through combined law enforcement, intelligence, and national security authorities. It frames the threat as two major forces: state actors pre-positioning inside U.S. critical infrastructure, and a professionalized criminal marketplace built on ransomware, fraud, and cryptocurrency theft. The Bureau claims sole authority to address both criminal and national security threats domestically, and organizes execution around disruption, victim support, partnerships, and internal capability. The strategy is divided into four pillars:

Pillar	Objective
Pillar 1: Investigate, Disrupt, and Impose Cost	Objective 1.1: Investigate Cyber Intrusions
	Objective 1.2: Prioritize Joint, Sequenced Operations
	Objective 1.3: Attribute Malicious Cyber Activity
Pillar II: Support Victims	Objective 2.1: Share Cyber Threat Intelligence with Urgency
	Objective 2.2: Quickly Engage After Incidents
	Objective 2.3: Deliver Specialized Capabilities to Victims
	Objective 2.4: Facilitate Reporting of Cyber Incidents
Pillar III: Increase Impact Through Partnerships	Objective 3.1: Share Actionable Intelligence
	Objective 3.2: Strategically Partner Across U.S. Government and with Allies
	Objective 3.3: Join Forces with Private Sector
Pillar IV: Enhance FBI's Cyber Capabilities	Objective 4.1: Recruit and Retain Top Cyber Talent
	Objective 4.2: Develop our Cyber Expertise
	Objective 4.3: Implement New Technical Tools and Techniques
	Objective 4.4: Adopt Artificial Intelligence to Scale Operations

Pillar I: Investigate, Disrupt, and Impose Cost

Pillar I structures investigation around four adversary components, the people involved, the infrastructure they use, the funds that sustain them, and the tools they deploy. Objective 1.1 commits Cyber Threat Teams to an intrusion within hours, requiring deployable forensic capability and case management that preserves chain of custody from field office to headquarters. Objective 1.2 sequences criminal and counterintelligence authorities across a campaign and assigns cryptocurrency work to a Virtual Assets Unit, requiring blockchain analytics that trace funds through mixing services and exchanges. Objective 1.3 establishes attribution as an evidentiary standard, requiring fusion platforms that reconcile Bureau evidence, intelligence holdings, allied reporting, private-sector telemetry, and victim submissions into a single assessment. The governing requirement is analytic output admissible in court rather than sufficient only for intelligence purposes.

© 2026 Carahsoft Technology Corp. Proprietary & Confidential

Pillar II: Support Victims

Pillar II defines victim support in terms of speed and reach. Objective 2.1 reduces detection-to-notification from days to minutes, which precludes analyst-mediated distribution and requires machine-readable indicator formats, automated sanitization that removes sensitive sourcing, and delivery directly into partner defensive systems. Objective 2.2 distributes those notifications through 56 field offices and more than 20 attaché posts. Objective 2.3 designates industrial control system personnel in every field office, creating demand for operational technology monitoring suited to environments where computing systems govern physical equipment and standard incident response can interrupt operations. Objective 2.4 accelerates processing of public complaint data, an ingestion and fraud analytics workload tied to the function that freezes fraudulent transfers. Each objective converts a response commitment into a throughput requirement that staffing alone cannot satisfy.

Pillar III: Increase Impact Through Partnerships

Pillar III addresses the interoperability required to sustain relationships across differing authorities. Objective 3.1 delivers intelligence to the National Security Council, the Office of the National Cyber Director, and network defenders simultaneously, requiring tooling that produces releasable versions of classified reporting quickly enough to remain actionable. Objective 3.2 spans a joint task force integrating more than 30 agencies, a ransomware task force co-chaired with CISA, state and local partners, and international channels including Five Eyes and Europol, each operating under a different classification level and handling restriction. Objective 3.3 extends comparable access to industry members holding no federal credential. Meeting these objectives depends on cross-domain transfer controls, secure collaboration environments, and identity management that extends beyond the Bureau's network boundary.

Pillar IV: Enhance FBI's Cyber Capabilities

Pillar IV states acquisition intent directly, committing the Bureau to adopt existing capabilities and to develop or acquire what does not yet exist. Objectives 4.1 and 4.2 recruit and train malware analysts, data scientists, and cryptocurrency specialists through vendor courses, certifications, and hands-on scenarios that imply range and simulation infrastructure. Objective 4.3 expands a computer network operations program supplying court-authorized collection and disruption tools, and begins preparing evidentiary systems for post-quantum cryptography, work that starts with identifying where existing encryption resides. Objective 4.4 applies artificial intelligence, including agentic systems that execute multi-step tasks with limited direction, to dataset triage, malware analysis, notification prioritization, and infrastructure mapping, subject to human review and legal control. That condition sets the evaluation criterion, since any system supporting prosecution must record what it processed and how it reached its conclusion.

What Does This Mean for the FBI?

The Bureau has published measurable commitments against an acknowledged capability gap. Near-term requirements are the following:

- **Automated dissemination infrastructure:** Minutes-scale notification rules out analyst-mediated distribution.
- **Operational technology capability at field scale:** Coordinators in every field office require tooling replicable 56 times.
- **Virtual asset tracing across the caseload:** Cryptocurrency analysis moves from specialist function to enterprise requirement.
- **Auditable artificial intelligence:** Systems supporting prosecution must log what they processed and how they concluded.
- **Cryptographic inventory:** Post-quantum readiness starts with discovery, which precedes any replacement purchase.

© 2026 Carahsoft Technology Corp. Proprietary & Confidential

What Does This Mean for Industry?

The strategy rewards vendors carrying both technical capability and procedural defensibility. Clear opportunity sits with blockchain and virtual asset analytics, open-source intelligence platforms including audio and video analytics, digital forensics and malware analysis, operational technology monitoring built for environments where downtime carries physical consequence, threat intelligence automation, cross-domain and secure collaboration infrastructure, auditable artificial intelligence with human-in-the-loop controls, cryptographic discovery, and cyber training environments.

Positioning determines access. Federal authorization status, criminal justice information handling compliance, and demonstrated chain-of-custody integrity govern whether a product enters an investigative workflow at all. Field-scale deployment favors licensing that supports 56 offices and hundreds of resident agencies over headquarters pilots. Platforms already interoperating with intelligence community and allied systems gain advantage under the partnership pillar. The strategy signals sustained rather than episodic demand, favoring suppliers prepared to support multi-year programs across investigation, notification, and workforce development at once.

Contact Us:

Email: Research@carahsoft.com

See more from the Carahsoft Team:
To explore our catalog of federal, state, and local technology policies, executive orders, and directives shaping public sector modernization scan this QR code.

© 2026 Carahsoft Technology Corp. Proprietary & Confidential