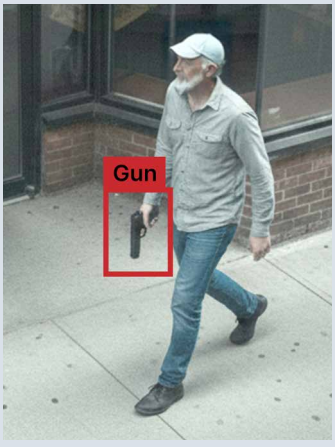
EAGLE EYE NETWORKS | A Brivo Solution

DATA SHEET

Implementation Services for Gun Detection

Get peace of mind knowing your system is optimized for maximum effectiveness.

Our Triple-Layer Verification process ensures you have the most advanced firearm detection system on the market. That accuracy requires that the system be designed, deployed, and aligned with response protocols in order to ensure effective escalation.



Two Robust Programs to Ensure System Readiness

Implementation Services includes **two mandatory programs**. One is performed by Brivo Specialists; the other is performed by a certified security risk assessment provider. Together, these programs ensure both technical system readiness and site-level security readiness.

Brivo Eagle Eye Gun Detection Implementation Services

This service ensures that the system is configured and operating correctly within the customer's video infrastructure for optimal detection of brandished firearms under expected operating conditions.

Brivo specialists perform verification of the system:

- Camera positioning and viewing angles
- Camera health checks (image quality, frame rate, and configuration)
- AI analytics configuration validation (range settings, regions of interest)
- Network diagnostics, including bandwidth and latency testing
- AI bridge / CMVR configuration and optimization
- Alert and automation configuration
- System training for response personnel
- Final confirmation that the system is operating and responding as intended

This is a mandatory service that is billed for each site, up to 25 cameras per service fee.

PART NUMBER

EN-COM-012	Eagle Eye VMS Gun Detection Implementation Service & Training

Readiness Assessment and Response Protocol

In addition to technical deployment verification, customers must complete a site-level security readiness assessment conducted by a qualified third-party security consulting firm.

Brivo will introduce customers to a list of recommended security assessment providers. Customers may select the provider that best fits their organization. These firms specialize in physical security consulting and threat risk assessment.

The assessment includes a minimum of four components:

1. Site & Technical Readiness Assessment

A certified security risk assessment provider conducts an on-site facility survey to evaluate camera coverage, lighting, entry points, and response workflows, and delivers a deployment blueprint for optimal gun detection performance.

- **Infrastructure audit**: Evaluation of existing CCTV (resolutions, FPS, RTSP streams) and lighting conditions (Lux levels/glare) to meet AI detection standards.
- **Physical survey:** Mapping of ingress/egress points, high-traffic "choke points," and perimeter blind spots.
- **Integration mapping:** Identifying how electronic access control (locks/gates) can be programmatically tied to Gun Detection alerts for automated containment.

2. Threat Intelligence & Compliance

Technology is most effective when informed by local context and legal guardrails.

- **Risk profiling:** Analysis of local crime stats and industry-specific threats to prioritize detection zones.
- **Regulatory alignment:** Ensuring video surveillance and AI monitoring policies comply with GDPR, CCPA, and state-specific privacy laws.
- **Data governance:** Establishing retention policies and ethical AI monitoring standards.

3. Response Orchestration & Protocol Design

Detection is only as fast as the human response. The consultant builds the playbook, which informs how the solution is architected.

- **Chain of command:** Documenting escalation hierarchies and direct-to-police notification paths.
- **Actionable protocols:** Developing specific procedures for automated lockdowns, PA announcements, and pre-mapped evacuation routes.
- **Unified communication:** Defining how security teams receive and interpret mobile/SOC dashboard alerts.

4. Validation & Lifecycle Management

To ensure immediate readiness and long-term efficacy, the consultant provides rigorous testing and documentation.

- **Scenario simulation:** Real-world walkthrough testing, including armed intruder simulations and false-positive stress tests (e.g., tool detection).
- **Deployment blueprint:** A phased rollout strategy including hardware specs, edge AI requirements, and staff training programs.
- **Post-installation audit:** A final "as-built" verification to benchmark detection rates against performance metrics and schedule 30/90-day reviews.