ZeroEyes Security & Compliance Capabilities

Federal-Grade Security for Commercial Deployments

At ZeroEyes, we recognize that our customers demand the highest level of security, regardless of whether they are a commercial enterprise or a federal agency. While our commercial platform operates independently from our FedRAMP environment, it directly benefits from the same engineering discipline, advanced security architecture, and rigorous compliance expertise.

Expertise Transfer

- **Federal Standards:** Built by the same engineering team that designs to strict Federal Risk and Authorization Management Program (FedRAMP) standards.
- **Advanced Threat Modeling:** We bring federal and defense-level security thinking into every product we build, designing systems to withstand nation-state-level threats rather than just typical enterprise risks.
- **High-Assurance Insight:** Our team's background in regulated, high-security environments provides practical insight into military-grade and federal security requirements, translating into robust architecture rather than simple checkbox compliance.

Customer Benefits

Most vendors prioritize convenience; we build with security constraints in mind from the ground up. Our deep experience means fewer blind spots in critical areas:

- Data handling and privacy
- AAdvanced encryption (FIPS compliance)
- Strict access control
- Continuous auditability

Our customers benefit from lessons learned in the most demanding security environments, without needing a full federal deployment.

ZeroEyes Certifications & Validations

Certification/Standard	Description	Value to Customers
FedRAMP Moderate (Ready)	A U.S. government standard for cloud security used by federal agencies.	We are pursuing the same security benchmark required for federal systems handling sensitive but unclassified data.
DHS SAFETY Act Designation	Formal designation by the Department of Homeland Security for effective anti-terrorism technologies.	Provides federal liability protections in the event of an act of terrorism. Independently validates our technology's effectiveness beyond marketing claims.
SOC 2 Type II	Independent audit of security, availability, and data handling controls over time.	Ensures continuous monitoring of security controls in production. Trusted by enterprise IT, risk, and compliance teams.
ISO/IEC 27001	Global standard for information security management systems.	Demonstrates structured, repeatable security processes and continuous risk assessment aligned to international standards.
RapidSOS Integration	Direct integration with emergency response infrastructure.	Enables direct data sharing with emergency services for faster response, reducing time from detection to dispatch. Fits seamlessly into existing emergency workflows.
Independent Cyber Rating (BreachBits)	Third-party security posture scoring.	Provides external, independent validation of our real-world security posture and ongoing measurement of risk exposure.

Cohesive Security Narrative

ZeroEyes combines federal-grade security (FedRAMP Moderate alignment, FIPS encryption), independent validation (SOC 2, ISO 27001), and real-world liability protection (DHS SAFETY Act). This means you are not just buying an AI solution—you are investing in a platform that is trusted, audited, and built to operate in the most demanding environments, from schools to critical infrastructure to government.

Key Value Drivers

- Built to federal security standards, not just commercial best practices.
- Audited, certified, and federally recognized—not just AI claims.
- Security, compliance, and liability protection are completely covered.
- From detection to 911 integration, we close the loop.