MAGNA POWER INNOVATIONS CORPORATION

EPOCH SHIELD

Evidence before action. Policy before automation. Human authority where consequences matter.

PHASE 10B	SHADOW	1,600+
COMPLETED BASELINE	ASSURANCE MODE	VALIDATION CHECKS

PUBLIC TECHNOLOGY BRIEF · 2026

MISSION ASSURANCE

Beyond a single security appliance.

Antivirus looks for malicious software. Spam filtering evaluates unwanted messages. Firewalls govern network paths. EPOCHSHIELD is designed to sit above those categories as a mission-assurance and trust-orchestration layer: it evaluates identity, evidence, freshness, confidence, policy, authority, and operational consequence as one governed decision path.

It complements rather than replaces specialized endpoint, messaging, and network controls. The central question is not only whether a signal exists, but whether the evidence is trustworthy, the action is permitted, and the outcome can be independently reconstructed.

Authenticated boundary	Approved identities and authenticated services enter the governed path.
Evidence integrity	Freshness, provenance, schema, size, and integrity checks determine whether evidence can be trusted.
Confidence evaluation	Evidence quality, contradiction, and uncertainty are evaluated before recommendations advance.
Deterministic authority	AI can analyze, explain, and recommend. Deterministic policy and required human authority remain final.
Mission evidence	Decisions, approvals, exceptions, and outcomes become attributable, replayable evidence.

VALIDATION + OPERATIONS

Claims have to earn their status.

1,600+	11 / 11	10B
Automated engineering checks across platform, regression, security, and assurance controls.	Bounded integration controls passed across identity, integrity, replay, privacy, schema, and size.	Mission-assurance implementation completed and validated; administrative baseline freeze remains.

The private command environment consolidates system health, mission-assurance posture, incident metrics, evidence, connectors, cryptographic state, and accountable response. Public telemetry is deliberately sanitized: no operator identities, emails, raw logs, evidence objects, prompts, network addresses, signatures, nonces, keys, internal routes, or vulnerability details.

Shadow assurance	The current Magna integration observes privacy-safe events and produces advisory assessments. It does not block public traffic or operate physical equipment.
Failure behavior	Missing evidence, failed integrity, stale requests, replay, unsupported fields, or insufficient authority stop the governed path.

CRYPTOGRAPHIC POSTURE

Layered protection with controlled migration.

CAPABILITY	PURPOSE	PUBLIC SECURITY PROPERTY
AES-256-GCM	Authenticated encryption	Confidentiality plus integrity
HKDF-SHA-256	Key derivation	Purpose-bound derivation
SHA-256	Integrity digests	Artifact and evidence integrity
HMAC-SHA-256	Request authentication	Authenticated event contracts
Ed25519	Digital signatures	Attributable record verification
ML-KEM capability	Post-quantum transition	Controlled migration path
TLS	Protected transit	Encrypted approved service paths
Nonce + time windows	Replay prevention	Stale or consumed requests fail closed

Quantum / Moat status	Core capability: implemented. Credentials: securely held. Managed-edge subset: under development. Edge activation: intentionally deferred while the approved runtime-compatible subset and integration controls are completed and validated.

No keys, cryptographic parameters, custody procedures, internal profiles, implementation topology, or source code are included in this brief.

CONTROLLED ROADMAP

Completed foundation. Governed evolution.

PHASE 10B	PHASE 11	PHASE 12
COMPLETED · VALIDATED Mission assurance, evidence certification, confidence evaluation, runtime integration, federation, administration, dashboards, and audit export.	CHARTER DEVELOPMENT Model governance, evidence-linked advisory intelligence, multi-model adjudication, compute-agnostic trust adapters, and adversarial validation.	PROPOSED · CHARTER REQUIRED Enterprise lifecycle assurance, platform validation, resilience, independent assurance, release evidence, and operator documentation.

Deferred backlog

Retained work is promoted deliberately rather than treated as unfinished Phase 10B work. Public categories include governed intelligence, emerging-compute adapters, production cryptographic migration, independent and long-duration testing, disaster recovery, authority restoration, release profiles, clean removal, and operational runbooks.

Release integrity

Phase 10B engineering validation is complete. The public release checksum remains pending until the signed administrative baseline freeze binds the accepted release manifest, source commit, and evidence record. EPOCHSHIELD uses SHA-256 for public release integrity identifiers.

RESPONSIBLE PUBLIC DISCLOSURE

Strong engineering. No borrowed authority.

EPOCHSHIELD is not represented as government authorized, independently certified, approved for classified processing, or approved for life-safety actuation. The architecture is designed to support rigorous compliance evidence and controls that may extend beyond minimum baselines; formal claims require the applicable independent process and authorization.

Intellectual-property boundary	This brief intentionally omits source code, internal terminology, control relationships, component thresholds, cryptographic keys and parameters, authority-store details, protected routes, vulnerability details, and reconstructable implementation information.

Certain capabilities shown are in development, staging, validation, or advisory operation. Technical descriptions are intentionally limited to protect confidential and proprietary intellectual property.

RESEARCH CONTACT

research@magnapowerinnovations.com