1. Executive 2030 PQC & CapEx Attestation — Apex-Edge-Telemetry-Gateway-v4

Work Order: QSA-PQC-2026-002 | Frozen Commit SHA: c5b6ff9 | U.S. Enclave: AWS us-east-2

Engagement Track: Tier 2 — Standalone 2030 PQC & Crypto-Agility Architecture Sprint ($18K-$28K | 5-10 Days)

2030 PQC Readiness Verdict: AMBER (Hybrid / Pre-Hash Required)

Estimated Remediation CapEx Range: $72,000 - $93,600 (320 Engineering Hours)

Executive Adjudication Summary

• Architecture Rationale: Tight headroom (24KB Flash/18KB SRAM); use LMS/XMSS (SP 800-208) boot verify + gateway X25519MLKEM768.

• Statutory Basis: Evaluated against Final NIST IR 8547 (deprecating classical RSA, ECDSA, ECDH, Ed25519, and X25519 after 2030; disallowing after 2035), FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), FIPS 205 (SLH-DSA), NIST SP 800-208 (LMS/XMSS), Executive Order 14412 / OMB M-26-15 (Dec 31, 2030 Key-Establishment & FAR Contractor Gate; Dec 31, 2031 Signature Gate), and NSA CNSA 2.0.

• Immediate Commercial Gate: Historical FIPS 140-2 module detected (CMVP Historical List sunset Sept 21, 2026) - blocks new VA/DHA/Federal system procurements & ATOs until upgraded to CMVP FIPS 140-3.

2. CycloneDX v1.6/1.7 CBOM & Stripped-ROM OID Audit

1. Symbol-Table & Source Cryptographic Asset Inventory (CycloneDX v1.6 / v1.7)

Symbol	Library	Algorithm & OID	Q-Lvl	Final NIST IR 8547 RAG Status	Prescribed FIPS 203/204/208 Target
mbedtls_ecdsa_verify	mbedTLS	ECDSA-P256 1.2.840.10045.4.3.2	Lvl 0	AMBER — Deprecate 2030 / Disallow 2035	ML-DSA-65 (FIPS 204) or Pre-Hash LMS (SP 800-208)
crypto_sign_ed25519	libsodium / TweetNaCl	Ed25519 1.3.101.112	Lvl 0	AMBER — Deprecate 2030 / Disallow 2035	Dual-Sign Ed25519 + ML-DSA-65 (FIPS 204)
EVP_PKEY_X25519	OpenSSL	X25519 1.3.101.110	Lvl 0	AMBER — Deprecate 2030 / Disallow 2035	Hybrid X25519MLKEM768 (TLS 1.3)
SHA1_Init	OpenSSL / Legacy	SHA-1 1.3.14.3.2.26	Lvl 0	RED — DISALLOWED IMMEDIATE	SHA-384 / SHA-512 (CNSA 2.0)
mbedtls_gcm_crypt_and_tag	mbedTLS	AES-256-GCM 2.16.840.1.101.3.4.1.46	Lvl 5	GREEN — Compliant Post-2035	Retain AES-256-GCM (FIPS 197 / CNSA 2.0)

2. Stripped-Binary ROM ASN.1 DER OID & Hardware S-Box Fingerprinting

Executed inside AWS us-east-2 U.S.-Sovereign Cleanroom (EAR ECCN 5A002 / ITAR 22 CFR 120.62 compliant) to uncover hidden classical primitives inside -Os -s stripped binaries and third-party silicon blobs.

Flash Offset	Detected Primitive / Constant	ASN.1 OID	Type	Q-Lvl	2030 Shor Vulnerable
0x014220	ECDSA/ECDH secp256r1 (P 256)	1.2.840.10045.3.1.7	pke	Lvl 0	AMBER — YES (Deprecate 2030)
0x0148a0	Ed25519 Signature	1.3.101.112	signature	Lvl 0	AMBER — YES (Deprecate 2030)
0x019400	AES Rijndael SBox Table	2.16.840.1.101.3.4.1	block-cipher	Lvl 3	GREEN — NO (Quantum-Resilient)

3. Silicon Memory Headroom, Federal OMB M-26-15 & CNSA 2.0 Gates

Target Sector Profile: Regulated Embedded Systems, PE Technical Diligence, MedTech & EAR ECCN 5A002 Supply Chain

1. Embedded MCU / Edge Memory Headroom vs. NIST PQC Stack Benchmarks

Hardware / Federal Gate	Measured Target Value	2030 PQC Threshold	Adjudication
Flash Memory Headroom	24 KB free / 256 KB total	>=48 KB (ML-KEM-768 + ML-DSA-65)	CONSTRAINED (Use LMS/Gateway)
Free Runtime SRAM	18 KB	>=24 KB peak stack budget	CONSTRAINED (Pre-Hash LMS ~6KB)
Bootloader Immutable RoT	Field-Upgradable Stage-2	Mutable PQC Stage-2 Required	PASS
CMVP FIPS 140-3 Posture	Historical FIPS 140-2 Hit	Sept 21, 2026 FIPS 140-2 Sunset	FAIL (Blocks New Fed/VA ATOs)
Federal EO 14412 / OMB M-26-15	REMEDIATION REQUIRED	Dec 31, 2030 KEM / 2031 Sig Gate	ACTION REQUIRED
NSA CNSA 2.0 (NSS / DIB)	NON-COMPLIANT	Jan 2027 New NSS / 2030 Enforce	UPGRADE TO ML-KEM-1024/SHA-384

2. Reference PQC Algorithm Footprint Matrix (Cleanroom Sizing Baseline)

Standard & Algorithm	Use Case	Public Key	Ciphertext / Sig	Est. MCU Peak Stack
FIPS 203 ML-KEM-768	TLS 1.3 / Key Establishment	1,184 B	1,088 B	~12 KB
FIPS 204 ML-DSA-65	X.509 / API / AI Weight Signing	1,952 B	3,309 B	~38 KB
NIST SP 800-208 LMS-SHA256	Constrained MCU Bootloader OTA	60 B	~4,500 B	~6 KB
FIPS 205 SLH-DSA-SHA2-128s	Stateless Firmware / Root CA	32 B	7,856 B	~8 KB

4. PE M&A CapEx Valuation & 2030 Crypto-Agility Roadmap

1. Executive CapEx Holdback & Engineering Effort Valuation

Designed for Private Equity Investment Committees, Corporate Boards, and VP Engineering budgeting ahead of the 2030-2031 NIST IR 8547 / EO 14412 deprecation cliff.

Remediation Workstream	Scope Driver	Est. Eng Hours	Est. CapEx Range (USD)
Cryptographic Primitive & PKI Refactor	5 detected symbol primitives	175 hrs	$39,375 - $51,187
CMVP FIPS 140-2 to 140-3 Module Swap	Sept 21, 2026 Sunset Blocker (New ATOs)	90 hrs	$20,250 - $26,325
Bootloader / Silicon Architecture Path	AMBER (Hybrid / Pre-Hash Required)	55 hrs	$12,375 - $16,088
Total All-In Remediation Holdback	Blended Senior Principal Rate + Architecture	320 hrs	$72,000 - $93,600

2. Prioritized 3-Horizon Migration Schedule (2026-2031)

• Horizon 1 (0-90 Days - Harvest-Now-Decrypt-Later & FIPS 140-3 Unblock): Replace Historical FIPS 140-2 modules blocking new VA/DHA/Federal system procurements & ATOs; enable hybrid X25519MLKEM768 on external TLS 1.3 ingress/gateways to neutralize HNDL capture immediately.

• Horizon 2 (6-12 Months - Firmware Boot & AI/Artifact Signing): Deploy stateful hash-based LMS (NIST SP 800-208) on RAM-constrained Stage-2 bootloaders (MCUboot / U-Boot) and transition Ed25519 container/AI model weight signatures to dual Ed25519 + ML-DSA-65.

• Horizon 3 (12-24 Months - NIST IR 8547 & EO 14412 / OMB M-26-15 Cutover): Complete X.509 device identity PKI migration to ML-DSA-65/87 ahead of the Dec 31, 2030 NIST IR 8547 deprecation cliff & FAR contractor key-establishment gate and Dec 31, 2031 EO 14412 signature mandate (2035 full disallowance), protecting the 4-to-5-year PE exit diligence window.