FORWARDEDGE

OCTANS SPACE AFRICA

White Paper

Isidore Quantum® - 1 (Edge Device)

All-in-One Cybersecurity and Drop in PQC Solution

Securing the Grid: Defending Public Infrastructure from Cyber and Quantum Collapse

Why Isidore Quantum - 1:

Affordable: 70% faster to implement and 60% lower total cost of ownership

Quantum-Resilient Security: Protects wireless logistics data against present and future quantum decryption threats

Low-SWaP Efficiency: Compact, lightweight, sub-5W module ideal for vehicles, drones, and edge devices

AI-Driven Defense: Predicts, detects, and mitigates cyber threats in real time across fleet networks

Public infrastructure and utilities, including electric power, natural gas, water, sewer, telecommunications, rail, and transportation, are facing intensifying attacks from cyber adversaries exploiting legacy systems never designed for modern threats. Critical networks depend on SCADA, PLC, and IoT devices built for reliability rather than resilience, leaving them open to ransomware, remote-access exploitation, and lateral movement across interconnected operational technologies. As attackers increasingly focus on shared OT dependencies, a single compromised endpoint can set off cascading failures that threaten national security and public safety.

The countdown to Q-Day continues, marking the moment when quantum computers will break the encryption that secures every control system and render RSA, ECC, and PKI obsolete. Nation-state actors are already executing Harvest Now, Decrypt Later (HNDL) campaigns, capturing encrypted infrastructure data today for future decryption and weaponization. The fusion of ongoing cyber intrusions and the imminent quantum decryption threat has created a perfect storm capable of undermining the digital trust that sustains the world's most vital services

Isidore Quantum, developed by Forward Edge-AI in partnership with the National Security Agency, provides a comprehensive cybersecurity and post-quantum encryption platform engineered to protect critical infrastructure from both present and emerging threats. The system integrates zero-trust architecture, autonomous key management, and AI-powered anomaly detection to secure SCADA, PLC, and telemetry networks across power grids, gas pipelines, water utilities, and transportation systems

without requiring expensive retrofits. Fully compliant with CNSA 2.0 and equipped with quantum-resistant encryption algorithms, Isidore Quantum removes PKI dependencies and outdated key loaders, delivering real-time, self-healing protection at every network node. Proven in deployments with the NSA, U.S. Air Force, and U.S. Navy, the platform offers unmatched resilience and scalability. Infrastructure operators gain the ability to strengthen defenses against current cyberattacks while ensuring continuous, quantum-safe operations for decades to come.

The Situation

56%	**70%**	**$5.6M**	**60%**
SCADA/ICS operators reported a breach in 2025	Water and wastewater utilities use legacy encryption and unsegmented OT networks	Average cost per cybersecurity incident in the energy sector	Transportation operators have experienced attempted or successful cyber intrusion

Power, water, natural gas, and transportation systems make up the unseen infrastructure that supports modern life, and all are under attack. Every major utility now functions within a hyperconnected digital ecosystem of SCADA, PLC, and IoT devices built for reliability rather than cybersecurity. Legacy systems, many still operating on decades-old firmware, are increasingly targeted through ransomware, remote access exploitation, and data manipulation.

Such events are not isolated but instead reflect a collapsing security framework built on trust and encryption that cannot withstand the approaching quantum era.

Isidore Quantum: All-in-One Cybersecurity PQC Solution

Isidore Quantum is a compact cybersecurity and post-quantum encryption platform engineered by the NSA to protect critical utilities, including electric power, natural gas, water, sewer, telecommunications, rail, and transportation systems, from both current and emerging cyber threats. The platform delivers zero-trust, CNSA 2.0-compliant protection through autonomous key management and AI-powered anomaly detection that can immediately identify and isolate intrusions. Designed for seamless integration with legacy SCADA, PLC, and OT networks, Isidore Quantum removes PKI dependencies and installs without costly infrastructure modifications. Proven in both defense and commercial utility environments, the system provides a unified and scalable solution that strengthens essential services against present cyberattacks while preparing them for future quantum decryption challenges.

Capability	What It Delivers
Quantum-Resilient Encryption	Replaces RSA/ECC with ML-KEM and AES-256-GCM, securing SCADA, PLC, and telemetry traffic from quantum and classical attacks
Zero-Trust by Default	Enforces cryptographic pairing between every endpoint—no device or user is trusted by default
AI-Driven Threat Immunity	Detects and isolates anomalies across power, water, and rail networks in real time, reducing mean time to respond from hours to seconds
Autonomous Key Lifecycle	Self-generates and rekeys ephemeral session keys—eliminating PKI, key loaders, and certificate renewal cycles
Red/Black Isolation & Quantum Entropy	Hardware-enforced segmentation + Quantum Random Noise Generation for provably random, one-time keys
Plug-and-Play Integration	Deploys in minutes over Ethernet, SATCOM, fiber, or radio—no downtime or system redesign required

Relying on AES-256 alone creates a dangerous illusion of safety. The cipher itself remains strong, but the scaffolding around it is already crumbling. Quantum algorithms will tear through key exchanges, side-channel attacks will siphon secrets in real time, and AI-driven exploits will adapt faster than any patch. Defenders who cling to "AES-256 is enough" risk guarding an empty vault while intruders walk through unseen doors. The era ahead demands more than brute-force resistance; it demands architectures built for resilience against quantum speed, physical leakage, and machine-intelligent adversaries.

The Urgency for Public Infrastructure

Delaying migration to post-quantum cryptography invites cascading failure across energy, water, and transportation systems. As the NSA, NIST, and DHS have made clear, systems that fail to modernize by 2027 will no longer meet national security or regulatory standards.

Act now to:

1. Audit OT encryption dependencies—identify RSA, ECC, and PKI exposure.
2. Deploy Isidore Quantum® across SCADA gateways, substations, and control nodes.
3. Adopt zero-trust, PQC-compliant architectures to meet CNSA 2.0 mandates.
4. Protect your data now—before adversaries decrypt it later.

The Takeaway

Public utilities are the foundation of civilization—and the next frontline of cyberwarfare.
Isidore Quantum® is the first and only drop-in, quantum-resilient cybersecurity platform proven across defense, energy, water, and transportation systems.

Variants and Specifications:

Isidore-1: IoT/OT/SCADA

Isidore 50MB/s – 2 GB/s

One-Way-Data Diode

CubeSat

Enterprise

	50 Mb/s	480 Mb/s	1 - 2 Gb/s	10 Gb/s	68 Gb/s	1 Tb/s
Size, Weight & Power	~140 x 89 x 39 mm (5.5 x 3.5 x 1.5 in); 450 g (16 oz); ~7 W	~140 x 89 x 39 mm (5.5 x 3.5 x 1.5 in); 450 g (16 oz); ~10 W	~140 x 89 x 39 mm (5.5 x 3.5 x 1.5 in); 450 g (16 oz); ~12 W	Available Q3 2026	Available Q3 2026	Available Q4 2026
Environmental:	–40 °C to +85 °C; shock and vibration qualified					
Cryptography:	AES-256 GCM and ML-KEM					
Quantum Entropy:	Integrated Quantum Random Number Generator (QRNG) subsystem; validated per NIST SP 800-90 A/B/C and BSI AIS-31					
Topologies:	Point-to-point, point-to-multipoint, mesh, and hub-and-spoke; supports wired, wireless, and hybrid topologies					
Certifications and Compliance:	NSA CNSA 2.0, FIPS 140-3 (Level 3), NIST SP 800-90 A/B/C, BSI AIS-31, ECCN 5A002 (License Exception ENC)					
Latency:	<90 µs (estimated)					
Security Architecture	Hardware-enforced Red/Black separation with galvanic isolation; zero-trust, zero-touch operation; covert posture (no network announcements or responses to probes)					
AI / Autonomy	Embedded AI engine trained for real-time anomaly detection, and self-healing response					
Management System:	Cassian™ for fleet orchestration, provisioning, telemetry, and policy governance across distributed deployments					

1. Specifications listed are subject to change without prior notice.

Contact: octans@inhub.world | forwardedge.ai | octanspace.com