**HST Global, Inc. Files Provisional Patent for Breakthrough Cryptographic Key Management Technology for Use in DDIL Environments**

*Virginia Beach, VA March 21, 2026*

*"First-of-Its-Kind Architecture Delivers Quantum-Resistant Encryption with No Message Exchange Required Engineered for Disconnected, Denied, Intermittent, and Limited (DDIL) Environments"*

HST Global, Inc. (OTC:HSTC), the parent company of Virginia-based cybersecurity innovator Qwyit, LLC, today announced the filing of a U.S. Provisional Patent Application for a novel cryptographic key management architecture invented by R. Paul McGough. The technology is purpose-built for Disconnected, Denied, Intermittent, and Limited (DDIL) environments and represents a fundamental advance in how encrypted communications are secured and maintained across the world's most demanding operational conditions.

**A New Paradigm for Encryption in the Most Challenging Conditions**

Every encryption system in use today, from military communications to enterprise software, shares one critical structural flaw: two parties must exchange messages to keep their shared encryption keys synchronized. If communication is disrupted, severed, or denied, security breaks down. HST Global's patented architecture eliminates that dependency entirely.

Two parties holding a shared key can independently derive an identical updated encryption state through local computation alone, transmitting nothing. The result is a system that remains fully secure even when communication is impossible, unreliable, or actively denied the precise conditions under which all prior approaches fail.

The technology provides unconditional resistance to quantum computing attacks not through computational complexity that more powerful machines may one day defeat, but through the structural mathematics of modular arithmetic. It is quantum-proof by construction, not by assumption.

*"Every protocol in existence today whether military, commercial, or otherwise shares one critical structural flaw: you cannot advance your encryption state without sending a message. We have eliminated that dependency entirely. This architecture does not merely improve on existing solutions; it removes the vulnerability at the foundation of all prior approaches. For the warfighter who has lost comms, the enterprise system that has gone offline, or the IoT device operating at the network's edge, this means security that holds."* R. Paul McGough, Inventor, HST Global, Inc.

**Purpose-Built for DDIL: How It Works**

The patented architecture is defined by two core functions: a Pseudo-random Data Augmentation Function (PDAF) and a One-Way Computation (OWC) function, each operating entirely within modular-16 arithmetic. Together, they enable both parties to update their shared encryption state in perfect synchronization with zero communication required.

The system supports two key update methods, each suited to different operational requirements:

**Method 1: Backward Secrecy:** Protects all past encrypted communications, even if a current key is compromised, through the irreversibility of the OWC function.

**Method 2: Forward and Backward Secrecy:** Adds protection against future compromise by incorporating external entropy, making each state update independently unpredictable.

Ciphertext length is identical to plaintext length, with no per-message authentication tag required for structured payloads, a significant advantage in bandwidth-constrained DDIL environments. Implemented in a parallel hardware pipeline at 400 MHz, the architecture delivers throughput of up to approximately 12,800 MB/s and runs identically on hardware ranging from 8-bit microcontrollers to FPGAs. Its keystream output passes all 15 NIST SP 800-22 statistical randomness tests.

**Applications Across Defense, Enterprise, and Critical Infrastructure**

The DDIL key management architecture addresses a broad and growing set of operational scenarios where existing encryption solutions fail or are operationally impractical:

**Defense and Military Operations:** Secure communications for forces operating beyond reliable network coverage - dismounted warfighters, autonomous systems, forward operating bases, and contested airspace.

**Critical Infrastructure:** Power grids, water systems, and transportation networks requiring continuous encrypted control and monitoring even during network disruptions or active cyberattacks.

**Enterprise and Edge Computing:** Distributed, intermittently connected systems including remote facilities, field operations, supply chain endpoints, and IoT deployments.

**Financial Services and Healthcare:** High-assurance encryption for regulatory-sensitive data across environments that cannot guarantee persistent connectivity.

*"The filing of this provisional patent marks an important milestone for HST Global and for the broader security community. Building on the foundation of Qwyit's more than 25 years of patented cryptographic breakthroughs, Paul's DDIL architecture resolves a structural vulnerability that has never been solved, only worked around. We are committed to bringing this technology to the defense, enterprise, and infrastructure markets where the need is most acute, and we look forward to sharing our commercialization roadmap in the months ahead."*

Michael P. Fortkort, Chief Executive Officer, HST Global, Inc.

**About HST Global, Inc.**

HST Global, Inc. is a Virginia Beach, Virginia-based technology holding company specializing in advanced cryptographic and cybersecurity solutions for defense, government, enterprise, and critical infrastructure markets. HST Global is the parent company of Qwyit, LLC, a cybersecurity innovation firm with a portfolio spanning more than 25 years of patented breakthroughs, including the Fast Unbreakable Cipher, Real-Time Trust protocols, Provably Secure Authentication & Encryption (PSAE) engine, and Universal Unbreakable Encryption technologies. Together, HST Global and Qwyit continue to advance the global state of digital security across hardware, firmware, software, financial, communication, and government sectors. For more information, please visit www.HSTGlobal.com

**Forward-Looking Statements**

This press release may contain "forward-looking statements" within the meaning of Section 27A of the Securities Act of 1933 and Section 21E of the Securities Exchange Act of 1934. Such statements reflect current expectations regarding future events, including anticipated commercial performance, regulatory outcomes, and distribution expansion. Actual results may differ materially due to risks and uncertainties, including regulatory delays, market acceptance, manufacturing capacity, and other factors described in the company's public filings. The company undertakes no obligation to update or revise any forward-looking statements except as required by law.

**Contact:**

**HST Global, Inc.**
www.HSTGlobal.com
509 Old Great Neck Road, Suite 105
Virginia Beach, VA 23454
Email: info@hstglobal.com