Shareholder Update

Dear Shareholders,

Signal Advance, Inc. continues to make significant strides in positioning its proprietary **Analog Guard®** technology at the forefront of next-generation cybersecurity solutions. In the last year, we have achieved a number of important technical, strategic, and regulatory milestones that further validate our approach and expand our growth potential.

Disrupting the Digital Security Paradigm Across Blockchain, Encryption, and Beyond

Today's digital security systems—including both **blockchain** and **traditional encryption**—share a common foundation: they rely on **computational complexity**. In simple terms, these systems are designed to be secure because the math problems they use (such as factoring large numbers or solving elliptic curve equations) are extremely difficult for current computers to solve in a reasonable time.

- **Digital encryption** uses this principle to protect communications, financial transactions, and sensitive data through cryptographic algorithms like RSA and ECC[1]
- **Blockchain systems**, such as those used in cryptocurrencies and decentralized ledgers, rely on similar principles—employing cryptographic hashing and digital signatures to secure records, authenticate identities, and prevent tampering.

This reliance on complex math has worked—**until now**. The accelerating development of **quantum computing** threatens to upend this model entirely. Algorithms like Shor's[2] and Grover's[3] will enable quantum computers to crack the math that protects both blockchain and encrypted systems. Meanwhile, **AI-driven attacks** are already undermining digital systems by identifying patterns, modeling side-channel[4] behaviors, and exploiting implementation flaws far faster than human-led processes ever could.

What makes this particularly urgent is that these threats **apply equally to nearly all digital security infrastructure**, across industries—from finance and defense to healthcare, industrial control systems, and cloud computing. The broader the reliance on computational complexity, the broader the risk.

1. **RSA and ECC** - encryption methods using complex math problems that are easy to create but extremely hard—and time-consuming—for current computers to solve
2. **Shor's algorithm** lets quantum computers break encryption by solving math problems that are too hard for regular computers
3. **Grover's algorithm** speeds up searching through large sets of data, making it easier to find secret keys.
4. **Side-channel** - a security flaw in which attackers exploit indirect information timing, power use, electromagnetic leaks, or acoustic signals rather than breaking the encryption algorithm itself, to attempt to extract sensitive data such as cryptographic keys

Analog Guard® eliminates the common weakness in both blockchain and digital encryption. Rather than relying on static mathematical structures, it encrypts data at the **physical signal level** using real-time analog modulation, high-entropy waveforms, and non-linear signal dynamics. These continuously shifting analog signals are unpredictable, non-repeatable, and immune to traditional cryptanalysis—whether powered by brute-force, AI, or quantum logic.

For **blockchain**, Analog Guard® can protect wallets, digital signatures, node communication, and oracle data—all at the physical layer.

For **traditional encryption**, it protects hardware and infrastructure from side-channel and signal-layer attacks, even if the underlying algorithms are compromised.

This positions Analog Guard® not merely as an enhancement to today's security protocols, but as a **strategic, architecture-level shift**—a future-resilient solution built to secure digital systems where current methods will eventually fail.

By addressing the **root vulnerability shared across digital encryption and blockchain**, Analog Guard® expands its relevance far beyond traditional IT cybersecurity—reaching into finance, defense, industrial IoT, secure communications, infrastructure, and beyond.

AI Assessment of Analog Guard®

AI attacks face exponential difficulty due to increased entropy, nonlinear feedback interactions, and multi-dimensional signal variation.

Quantum computing decryption is severely hindered by true randomness, unpredictable variation of multiple keys, and complex feedback dynamics.

Side-channel vulnerabilities are mitigated through physical and signal-based complex modulation techniques.

This latest, two or more key, architecture makes the Analog Guard® system **one of the most resilient encryption methodologies** against advanced AI and quantum threats.

Strategic Engagement with Federal Stakeholders

In a major development, Company leadership held private meetings with U.S. Congressmen **Pete Sessions (TX)** and **Don Bacon (NE)**—both influential voices on defense and cybersecurity issues. These discussions centered on the defense, government, and critical infrastructure applications of Analog Guard®. The outcome was highly encouraging, and efforts are now underway to explore specific engagement opportunities with relevant federal agencies and defense contractors.

National Science Foundation Recognizes Innovation Potential

The **National Science Foundation (NSF)** formally invited Signal Advance to submit a proposal for non-dilutive seed funding to support Analog Guard® technical development and validation. This is a highly competitive program that recognizes and supports early-stage transformative innovations with strong commercial and disruptive potential in national security and cybersecurity.

We are pleased to report that the proposal has been officially submitted. This highly competitive opportunity, if awarded, would materially advance the development of Analog Guard® technology—accelerating prototyping and de-risking our technology path at zero dilution to shareholders.

Expansion and Strengthening of Intellectual Property Portfolio

The Company achieved a major milestone with the **issuance of U.S. Patent No. 12,126,720**, securing critical IP protection for the Analog Guard® platform. This patent covers our novel analog encryption methods that defend against remote hacking, spoofing, and signal interception—risks that increasingly threaten both civilian and military systems.

To further secure global IP rights and extend our technical claims, we have also filed the following:

- **International Patent Application** (PCT/US2024/022278) – initiating global patent coverage under the Patent Cooperation Treaty
- **U.S. Continuation Application** (Application No. 18/922,304) – refining and expanding the claims of the parent patent
- **Continuation-in-Part (CIP) Application** (Application No. 19/220,451) – adding new innovations derived from our ongoing R&D efforts
- **Additional** Continuation and CIP patent applications in preparation

This layered patent strategy not only protects current advancements but provides a legal framework for future developments and licensing opportunities.

Potential Transfer of Analog Guard® Assets to Subsidiary - Strategic Restructuring

To streamline future development and support investor engagement, the Company is considering the transfer of all Analog Guard®-related assets to its wholly owned subsidiary, Analog Guard, Inc. This strategic move is intended to better position Analog Guard® for targeted growth and external investment by creating operational separation, enhancing focus on the encryption business unit, and enabling more flexible investment structuring—while preserving full ownership by Signal Advance and, thus, its shareholders.

This potential restructuring involves asset transfer that includes intellectual property (patents, trademarks), technical documentation, domain rights, and related R&D assets. It would be structured as a capital contribution under Section 351 of the Internal Revenue Code, allowing for a tax-efficient reorganization.

While Signal Advance would initially retain 100% ownership of Analog Guard, Inc., the subsidiary is expected to raise outside capital, which would result in partial dilution of Signal Advance's ownership interest as part of its growth and commercialization strategy. The proposed restructuring aligns with industry best practices for technology spinouts and is designed to maximize shareholder value by enabling targeted capitalization, strategic partnerships, and increased agility in addressing commercial, defense, and government cybersecurity markets.

Summary and Outlook

Signal Advance is entering a pivotal phase in its development, with multiple value-driving milestones achieved and more underway. We've deepened engagement with key federal stakeholders, secured critical patent protections, and officially submitted our NSF proposal for non-dilutive funding—all of which strengthen our foundation and broaden our path to commercialization.

We are also evaluating a strategic transfer of all Analog Guard®-related assets to a wholly owned subsidiary, Analog Guard, Inc. This move is intended to streamline operations, sharpen business focus, and better position the platform to attract targeted outside investment. Importantly, Signal Advance would retain 100% ownership at the outset, preserving shareholder upside while enabling more flexible capitalization and strategic partnerships going forward.

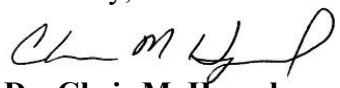
As the cybersecurity landscape shifts toward AI- and quantum-capable threats, traditional digital encryption is becoming increasingly vulnerable. Analog Guard® is built to address this next generation of risks—offering a physics-based, hardware-level encryption solution that conventional math-based systems cannot match.

Our strategy remains clear: protect shareholder value by pursuing non-dilutive capital where possible, maintain control of our core technology, and position Analog Guard® for long-term impact across commercial, government, and defense markets.

We appreciate your continued support as we work to unlock the full value of this breakthrough technology.

For further information, please contact us at: **IR@SignalAdvance.com**
Company updates and regulatory filings are available at www.signaladvance.com and on **OTCMarkets.com** under our ticker symbol **SIGL**.

Sincerely,



Dr. Chris M. Hymel **Date:** July 20, 2025
CEO, Signal Advance, Inc.