

CogniMind AI™

WEEKLY INTELLIGENCE BRIEF

ISSUE 02 • SEPTEMBER 28, 2026

BIG NEWS • U.S. PATENT PENDING

Protecting the architecture behind adaptive, accountable intelligence.

Founder and CEO Sara Spencer has filed a U.S. provisional patent application covering elements of CogniMind AI's adaptive artificial-intelligence architecture. The work centers on **Verified Outcome-Gated Contextual Plasticity (VOCP)**—a context-aware graph approach designed to form, evaluate, strengthen, and retire connections based on verified outcomes.

The filing is an important milestone for ANT™ and the CogniMind AI™ platform portfolio. Our public research overview covers temporary and persistent connections, outcome-gated learning, explainability, control matrices, and potential use across cybersecurity, critical infrastructure, and autonomous systems.

[EXPLORE THE RESEARCH →](#)

"Patent pending" refers to a filed U.S. provisional patent application. No patent has yet been issued, and the scope of any future protection is not guaranteed.

FROM THE FOUNDER

From concept to protected research.

The past two weeks have been about turning momentum into infrastructure. We protected a core technical idea, opened our research to serious readers, strengthened the VALKERIE™ path to market, and created a clearer way for qualified investors to learn about the company.

The common thread is accountability. Whether an AI system is helping defend a network, monitor critical infrastructure, support a drone mission, or organize compliance evidence, intelligence only matters when people can understand the context, verify the outcome, and act with confidence.

— Sara Spencer, Founder & CEO

THE SIGNAL

What is moving in AI and cybersecurity

1. NIST is bringing AI into CSF 2.0 analysis

NIST released a draft quick-start guide showing how structured prompts can support Cybersecurity Framework analysis, current-state profiles, gap documentation, and target-state planning. The comment period runs through October 15, 2026.

[READ THE SOURCE →](#)

2. AI evaluation is getting harder to game

NIST's Artificial Intelligence Technology Evaluation program uses blind data in a sequestered environment to reduce train/test contamination. Its first tasks cover vision-language models in quantum science, genomics, and public safety.

[READ THE SOURCE →](#)

3. Europe's AI transparency rules are now operational

The EU AI Act became broadly applicable on August 2, 2026, and its transparency requirements are now in effect. The framework emphasizes disclosure, traceability, human oversight, robustness, cybersecurity, and documentation.

[READ THE SOURCE →](#)

4. Identity and access tokens remain a high-value target

NIST finalized guidance in September on protecting online identities and access tokens from misuse. AI agents and integrations inherit the risk of every credential they can reach.

[READ THE SOURCE →](#)

PRACTICAL AI SECURITY

Five controls to put around AI agents now

1

Give every agent its own identity.

Do not let agents inherit a user's broad permissions or share long-lived credentials.

2

Separate reading from acting.

Use distinct permissions for retrieval, drafting, execution, deletion, and financial or operational changes.

Verify tools, models, and dependencies.

Track versions, provenance, approvals, and changes across models, plugins, APIs, and knowledge sources.

4

Log the decision chain.

Capture the request, context, evidence, tool calls, approvals, outputs, and resulting action.

5

Build a tested stop mechanism.

Suspend agents, revoke tokens, isolate integrations, and restore a known-safe state.

COGNIMIND AI™ FIELD NOTES

What changed since our last brief

Patent and research milestone

A U.S. provisional patent application has been filed, and the VOCP research overview is now available for technical readers, partners, and investors.

VALKERIE™ for MSPs

The MSP motion now emphasizes multi-client visibility from one dashboard—connecting customer risk, compliance, assets, findings, evidence, and prioritized action without losing tenant context.

Investor conversations are opening

Accredited investors who want to learn more can contact CogniMind AI™ or schedule an introductory conversation with Sara before receiving additional offering materials.

Partner conversations are expanding

We are inviting MSPs, MSSPs, assessors, systems integrators, researchers, critical-infrastructure operators, and autonomous-systems teams into demonstrations, pilots, and channel discussions.

INVESTOR UPDATE

Start a conversation about what we are building.

CogniMind AI™ is preparing a public Rule 506(c) offering for verified accredited investors. Current proposed SAFE terms include a **\$20 million post-money valuation cap** and a **15% conversion discount**, subject to final documentation, company acceptance, and legal review.

If you are an accredited investor and the mission resonates with you, begin with a private introduction. Contact CogniMind AI™ or book a short meeting with Sara to discuss whether the opportunity may be a fit.

CONTACT COGNIMIND AI™ • BOOK AN INTRODUCTORY MEETING →

For informational purposes only. This is not an offer where unlawful. Any Rule 506(c) offering will be available only to verified accredited investors through definitive documents and approved procedures. Investments are speculative, illiquid, and may result in total loss. The SEC has not approved or endorsed any offering.

One operating view across every client or business unit.

VALKERIE™ is being positioned as the holistic cybersecurity platform for organizations and service providers that need real-time insight across compliance, risk, assets, findings, evidence, and remediation. For MSPs and MSSPs, that means managing multiple customer environments from one intelligent dashboard while preserving tenant separation and customer-level context. For the enterprise, it means bringing business units, systems, owners, controls, and risks into one connected operating picture without losing the context each team needs.

- Direct demonstrations with regulated and defense-sector organizations
- MSP and MSSP channel relationships built around repeatable multi-client delivery
- Design-partner pilots connecting real workflows, evidence, and operational data
- Land-and-expand growth from priority compliance and security use cases

[BOOK YOUR DEMO TODAY →](#)

STARTUP SECURITY JOURNEY

Build customer trust before the first security questionnaire arrives.

Startups do not need an enterprise-sized security program on day one—but they do need a credible foundation. CogniMind AI™ is beginning outreach to founders who want to protect what they are building, demonstrate responsible operations, and earn the confidence of prospective customers, partners, and investors.

START WITH THE ESSENTIALS

Know your assets and sensitive data, define ownership, secure access, document key policies, and create an achievable risk roadmap.

TURN SECURITY INTO CREDIBILITY

Respond to customer diligence with organized evidence, show measurable progress, and prepare for SOC 2, ISO 27001, NIST, or CMMC when the market requires them.

The goal is not compliance theater. It is a right-sized security journey that grows with the company and helps founders close opportunities without promising controls they cannot yet prove.

[BOOK A STARTUP SECURITY INTRO →](#)

BUILD WITH US

Strategic and Channel Partnerships

We are looking for partners who can help validate, integrate, deploy, and scale secure Situational AI across the defense industrial base, regulated enterprise, critical infrastructure, and autonomous systems—including drone operations.

STRATEGIC PARTNERS

Research, integrations, data, pilots, critical infrastructure, government, defense, universities, and autonomous systems.

CHANNEL PARTNERS

MSPs, MSSPs, assessors, compliance advisors, systems integrators, cloud providers, and implementation firms.

[START A PARTNERSHIP CONVERSATION →](#)

FROM SARA'S KITCHEN

Salted Espresso Chocolate Chunk Cookies

Deep chocolate, crisp edges, soft centers, and just enough espresso for the final sprint.



INGREDIENTS

- 1 cup unsalted butter, softened
- 1 cup packed dark brown sugar
- ½ cup granulated sugar
- 2 large eggs
- 2 teaspoons vanilla extract
- 2¼ cups all-purpose flour
- 1 tablespoon instant espresso powder
- 1 teaspoon baking soda
- ¾ teaspoon fine salt
- 10 ounces chopped dark chocolate
- Flaky salt, for finishing

METHOD

- 1 Heat the oven to 350°F and line two baking sheets.

- 2 Beat the butter and both sugars until light. Beat in the eggs one at a time, then add vanilla.
- 3 Whisk the flour, espresso powder, baking soda, and fine salt separately.
- 4 Fold the dry mixture into the butter mixture, then fold in the chocolate.
- 5 Chill 20–30 minutes. Scoop two-tablespoon portions onto the sheets.
- 6 Bake 10–12 minutes until the edges are set and centers are soft. Finish with flaky salt and cool on the pan for 5 minutes.

[CogniMindAI.net](#) • [Research](#) • [VALKERIE™](#) • [Contact](#)

Where Intelligence Meets Defense™