

BORN BETWEEN 2 GENERALS

ENGLEWOOD, FLORIDA · A FLORIDA LIMITED LIABILITY COMPANY BORN BETWEEN 2 GENERALS.COM

August 31, 2026

The President of the United States
The White House
1600 Pennsylvania Avenue NW
Washington, DC 20500

Re: Sovereign control of American critical infrastructure — working systems, a verifiable standard of evidence, and a request for one briefing

Dear Mr. President,

We are the founders of Born Between 2 Generals, a Florida company. We are writing to put a body of working technology in front of you and to ask for one meeting.

Our premise is simple. American critical infrastructure is no longer protected by owning the machines. It is protected by being able to prove, at any moment, who touched what, under whose authority, and whether the thing that was supposed to stay sealed actually stayed sealed. Compute, networks, hardware, airspace, and ballots are the same problem in different uniforms — a custody problem. We build custody evidence, and we build it so that a hostile reviewer can check our work.

WHAT IS ALREADY BUILT AND RUNNING

Sovereign Control Tower controltower.bornbetween2generals.com

Routes AI workloads by sovereignty rather than by benchmark score. A workload is described in plain language; nine deterministic gates evaluate data classification, jurisdiction, modality, license and commercial terms, egress posture, and hardware fit. Every model that loses carries the exact rule that blocked it. An operator can see not only the decision, but the reason for it.

StrongRoom and Operation Encrypt [private program repositories](#)

Mail-ballot chain-of-custody evidence: append-only inclusion and consistency proofs, dual-control batch sealing by two separation officers, threshold key ceremonies with no trusted dealer, and counter-signed tree heads that make equivocation visible. Paper remains authoritative. This is not a voting or tabulation system, it is not certified under VVSG 2.0, and our public materials say so.

BB2G Election Command [pilot package](#)

Role-based election operations for poll workers, jurisdiction command, security, legal, and audit: procedures with currency metadata, incident reporting, equipment tracking, custody logs, and three tiers of isolation. Consequential actions require human approval. The AI layer is never an election authority.

SENTINEL cybersentinel.bornbetween2generals.com

A local-first defensive platform operating under a strict rule: track back, never hack back. Inert malware forensics, deception, encrypted evidence custody for authorized investigators, and a packet layer that decides *allow*, *inspect*, or *block* on outbound traffic. Critical-infrastructure data crosses a one-way boundary; the platform is never given offensive reach.

Civil resilience [safeperimeter](#) · [resiliencelab](#) · [angelpost](#) · [asvab](#)

A child-safety architecture that warns without building a location history of a child, a parent-and-child digital-resilience curriculum for church-hosted sessions, a family-resource network that moves aid to a household instead of moving the child, and an adaptive preparation platform for young Americans entering military service.

THE STANDARD WE HOLD OURSELVES TO

Every one of these systems separates what has been *observed* from what has merely been *asserted*. Vendor benchmarks are labeled as not independently reproduced. Demonstration telemetry is labeled simulated. Exported evidence packs are described as hash-sealed, never as signed, because the signing key is deliberately kept outside the hosted console. When a control has been designed but not yet proven in the field, it is marked as asserted rather than measured. Our systems fail closed and report the refusal instead of silently degrading. We publish our residual risks — colluding officers, threshold-guardian collusion, print-vendor token access, limited coercion resistance, and the absence of outside cryptographic review — because a documented weakness is an asset to the country and an undocumented one is a liability.

We would rather show you a labeled gap than an unlabeled claim. That discipline is the reason this work can be trusted with infrastructure that matters.

THE DOCTRINE: FIVE SOVEREIGN LAYERS

Sovereign compute and AI. **BUILT AND LIVE** Admission, routing, provenance, quarantine, and export-control gating for models, including air-gapped runtimes with controlled import and export paths.

Sovereign data custody. **BUILT** Cryptographic custody evidence for the records a republic cannot afford to lose — beginning with mail ballots, extending to any chain of physical evidence.

Sovereign networks and egress. **PARTLY BUILT** Policy-controlled egress and identity-class screening are operating today. A national private relay layer for families and institutions exists as specification, not as product.

Sovereign hardware and data centers. **SPECIFIED** Hardware-fit and export-control gating are already enforced in software. Sovereign fabrication and the siting and governance of sovereign data centers are doctrine and design work, not deployed capability, and we will not present them as more than that.

Sovereign airspace and unmanned systems. **SPECIFIED** Custody and authority evidence for drone operations over critical infrastructure — who was permitted to fly, over what, under whose order, and what the record proves afterward — using the same gate-and-reason model that governs our compute layer.

WHAT WE ARE ASKING FOR

1. **A briefing, immediately.** Sixty minutes with the offices you judge relevant — science and technology policy, the National Cyber Director, CISA, the Election Assistance Commission, or the appropriate defense staff. We will bring running systems rather than slides, and we will show the failures alongside the successes.
2. **Implementation where the authority already exists.** A shadow pilot of ballot custody evidence in a single county, running alongside certified systems and touching no tabulation. In parallel, a sovereignty-routing evaluation inside one federal AI environment, using real jurisdiction and license constraints.
3. **Two principles written into federal guidance.** That AI workloads touching national interests be routed by sovereignty and legal authority, not by benchmark score alone; and that any system claiming to secure critical infrastructure be required to distinguish observed evidence from asserted posture in its own interface.

We are not asking you to accept our claims. We are asking you to test them — and we have built these systems so that testing them is possible. Every gate gives a reason. Every refusal is recorded. That is what sovereignty looks like in practice, and we would be honored to bring it to your staff at their earliest convenience.

Respectfully yours,

Mary Flynn O’Neill

FOUNDER

BORN BETWEEN 2 GENERALS, LLC

Kristen Hall

FOUNDER

BORN BETWEEN 2 GENERALS, LLC

ENCLOSURES · Eighty-four-second briefing film (captioned) · Live access to the Sovereign Control Tower, including the intake and routing console · Repository and architecture index, available on request

Born Between 2 Generals, LLC · Englewood, Florida · bornbetween2generals.com