MASTER PROJECT SUMMARY // v1.0 // CONFIDENTIAL

Born Between 2 Generals

The SENTINEL Cyber-Defense Ecosystem & Sovereign AI Cluster

One doctrine across every layer: track-back, never hack-back. A lawful, local-first family of systems that watch your own network, catch intruders, preserve the evidence for the authorities, and govern exactly what data is ever allowed to leave — from a single family to critical national infrastructure.

DEFEND + DOCUMENT

GOVERN WHERE DATA GOES

LAWFUL BY DESIGN

Prepared for the founder · Brandon, Florida · A Legacy of Faith, Family & Service

EXECUTIVE SUMMARY

What this is, in one page

Born Between 2 Generals is a family of connected security and sovereignty systems built on a single, simple promise: defend, document, and hand the evidence to the authorities — never attack back. Every module runs locally, keeps its own tamper-evident record, and is designed to be sold in clear tiers from families up to government and critical infrastructure.

The ecosystem has two halves that work together. SENTINEL is the active cyber-defense layer: it catches intruders in decoys, scans email, text and links, verifies who is really calling, traces ransomware without touching it, and packages court-ready evidence. The Sovereign AI Cluster is the foundation it can run on: your own private AI and data, with no default path to the open internet, strict identity for every node and person, and disciplined recovery.

The through-line

- Track-back, never hack-back. The system watches your own network and follows the trail — it never breaks into anyone else's.
- Local-first & zero-egress. Sensitive workloads have no path to the open internet; all cryptography, logs and databases stay on your machine.
- Real, not theater. Every module in this summary actually runs and is verified — with honest labels wherever something is indicative or simulated.
- Sold in tiers. The same doctrine scales: Family, Business, and Government / Critical Infrastructure.

At a glance

10	3	45/45	0
SENTINEL modules	tier market (Family→Gov)	automated checks passing	outbound network calls

45/45 = the platform's three automated verification harnesses (Identity Fabric 20/20, Critical-Infra Air-Gap 13/13, Forensics Lab 12/12) all pass.

PART ONE // ACTIVE DEFENSE

SENTINEL

Catch the intruder, verify who is calling, trace without touching, and hand court-ready evidence to the authorities.

PhishBot 3.0

SCANNER + GATEWAY

Scans incoming email, text messages, and links. Dangerous links are rewritten into safe ones before they can reach you, and anything suspicious is captured at the track-back gateway for evidence — not sent back at the attacker.

`gateway + phishbot`

Cyber Caller ID

IDENTITY VERIFY

Every caller carries a typed, rotating token — PSN- for a person, BIZ- for a business, GOV- for government. The system verifies the token type, jurisdiction and rotation against the Identity Fabric before a call is trusted, so no one can pretend to be someone they are not. One clean call log shows ALLOWED / SCREENED / DENIED / BREACH.

`forensics_lab_unified/caller_id.py`

VigilantGuard

HONEYPOT + DECEPTION

Self-contained decoy containers and a deception grid lure intruders into an isolated sandbox where they can be watched safely. Nothing they touch is real, and everything they do is recorded.

`honeypot/ (34 files)`

Forensics Lab

EVIDENCE PIPELINE

The unified lab ties the pieces together: it collects, hashes and time-stamps evidence into a tamper-evident record and prepares a clean package suitable for a digital lab or the authorities.

`forensics_lab_unified/ (87 files)`

Ransom-Trace

TRACE, DON'T TOUCH

Follows the money and the trail of ransomware activity for reporting — strictly observing, never interfering with or attacking the source.

`ransom_trace/ (11 files)`

Air-Gapped Vault

ENCRYPTED CUSTODY

An AES-GCM encrypted, tokenized vault that stays disconnected except during controlled backup and restore — the safe place for the most sensitive material.

`vault/ (22 files)`

Sovereign Packet Layer

JURISDICTION CRYPTO

Real HMAC-SHA256 tokens mark whether traffic is DOMESTIC or INTERNATIONAL, forming the cryptographic backbone the Identity Fabric builds on.

`packet_layer/ (10 files)`

Phishing Trainer

PEOPLE HARDENING

A safe phishing-simulation trainer that teaches families and staff to recognize the exact tricks PhishBot blocks — because people are part of the perimeter too.

`trainer/ (7 files)`

PART TWO // IDENTITY, EGRESS & AIR-GAP

The Sovereign Layer

Three new, fully verified modules that decide who is real, watch everything that leaves, and physically wall off the most critical systems.

Sovereign Identity Fabric

20/20 VERIFIED

Rotating, typed identity tokens for everyone — person, business, and government — split further by domestic vs. international. Because the token constantly rotates, no one can ever claim to be someone they are not. Even the cloud gets a token going in and a different token coming out, so data in transit can never be quietly touched.

GOV-DOM · GOV-INT · BIZ-DOM · BIZ-INT · PSN-DOM · PSN-INT · CLD-IN · CLD-OUT

`sovereign_fabric/ (16 files) · 14 fabric + 6 egress checks`

Outbound Egress Guard

TOKENIZED & TRACED

The same idea as Caller ID, but for everything leaving your system. Sensitive data is tokenized and tracked on the way out (EGR- tokens), so it can never be hijacked in transit and can always be traced back to where it came from. The most sensitive material rotates fastest.

`sovereign_fabric/egress_guard.py`

Critical-Infra Air-Gap

13/13 VERIFIED

For nuclear, grid and industrial control systems: true isolation — not on any network whatsoever. A one-way data diode lets approved information cross in one direction only, an air-gapped vault sits on the protected 'high side,' and separate zones (reactor-control, grid-SCADA, records-vault) are managed apart. Any forged crossing triggers instant lockdown and token rotation, written to a tamper-evident breach log.

`air_gap_infra/ (30 files)`

How they connect

» The Identity Fabric is the source of truth for who is real; Cyber Caller ID checks inbound callers against it.

» The Egress Guard stamps and traces everything outbound, so 'very sensitive stuff' can never leave untracked.

» The Air-Gap is the physical wall around the crown jewels; the vault on its high side stays sealed until a valid, verified crossing.

» All three keep a hash-chained record, so tampering is detectable and a breach instantly locks things down.

PART THREE // THE FOUNDATION

BB2G Sovereign AI Cluster

Your own private AI and knowledge base — no default path to the open internet, strict identity for every node, and disciplined recovery. (Design v0.3.)

This is the sovereign hardware, software and AI foundation the rest of the ecosystem can run on. Its prime directive: protected workloads and data in 'U.S.-Sealed' mode have no path to the wider internet, and sitting on the local network alone earns no trust — every node, service, workload and person must prove identity and be explicitly authorized.

Seven trust zones

- User / Admin — the local console and operator UI.
- Guardian control plane — policy, inventory, audit, node admission, cluster health.
- Compute fabric — the AI nodes, with no default route to the internet.
- Knowledge fabric — documents, SQL, vector search and a knowledge graph, each fact tagged with source, jurisdiction and date.
- Quarantine — where new models, containers and datasets are vetted before they ever see real data.
- Management / import — the one controlled path for signed, offline updates.
- Offline backup vault — encrypted and disconnected except during backup and restore drills.

Discipline built in

- Node admission: a machine is untrusted until it passes a 20-point check (encryption, secure boot, no internet route, container least-privilege, mutual certificates) and a final human approval.
- Identity / PKI: an offline root CA signs an intermediate that issues short-lived certificates; keys are hardware-backed and never live in code.
- Tamper-evident audit chain: every action is hash-chained so later alteration is detectable, with periodic checkpoints to write-protected storage.
- Disaster recovery & break-glass: three protected copies (live, nearline, offline), quarterly rebuild drills, and a sealed two-person break-glass procedure — with no permanent hidden backdoors, ever.

Build roadmap (6 phases)

Prove one machine → two-node cluster → knowledge fabric → multi-model local team → multi-node single-model inference → enterprise hardening (HSM/TPM keys, signed updates, HA Guardian, documented recovery).

PART FOUR // BUSINESS & DOCTRINE

How it ships, and the one rule

The same protection sold in three tiers — and the promise that governs every line of it.

Three market tiers

FAMILY	BUSINESS	GOVERNMENT / CRITICAL INFRA
Protect a household: scan email, text & links, verify callers, and keep a private vault. Simple, local, and safe.	Add deception honeypots, the forensics evidence pipeline, staff phishing training, and tokenized, traced outbound data for the whole organization.	Full sovereign stack: Identity Fabric across domestic/international, the Sovereign AI Cluster, and the Critical-Infra Air-Gap for nuclear, grid and industrial control.

The one rule: track-back, never hack-back

Every module in this document was built to a single, non-negotiable standard in the founder's own words: "I'm not gonna hack anybody — never, ever, in a million years. It's a track-back." The system watches your own network, follows the trail, and preserves the evidence for the digital lab or the authorities. It never attacks, never breaks in, and never sends anything back at an attacker.

Track-back	Zero-egress	Local crypto	Real & verified
Follow & document the trail on your own network.	Sealed workloads have no path to the open internet.	HMAC-SHA256, JSON & SQLite — all on-device.	45/45 automated checks pass; honest labels throughout.

Honest notes

- Enforcement is boundary-level: real cryptography, not magic — it cannot force foreign systems to honor tokens or re-plumb the internet.
- A true air-gap is guaranteed by physical deployment; the software enforces the posture and proves it in simulation.
- Demo entities, secrets and passphrases are synthetic sample data; the AI Cluster is a production-minded design and scaffold, not a claim of certified security.

Born Between 2 Generals · A Legacy of Faith, Family & Service · Prepared by Perplexity Computer