



BORN BETWEEN 2 GENERALS · MASTER SUMMARY

Cyber Sentinel

The full story.

Everything built across this project — the doctrine, the live console, the Ballot Fortress, the audit's best catches, pricing, and the roadmap. One complete record.

Prepared for: Kristen Hall · Born Between 2 Generals, LLC

Live at: cybersentinel.bornbetween2generals.com

Date: August 29, 2026

Doctrine: Track-back, never hack-back · Lawful under 18 U.S.C.
§1030

What Cyber Sentinel is

Cyber Sentinel is your umbrella lawful-cyber-defense platform. Its single rule is **track-back, never hack-back**: it never attacks anyone. It operates only on infrastructure you own, lures intruders into decoys, records everything they do, and hands court-ready evidence to law enforcement. It is lawful under the Computer Fraud and Abuse Act (18 U.S.C. §1030), local-first, and denies outbound traffic by default.

13

MODULES

3

SECTORS COVERED

0

MACHINES WE ATTACK

How the pieces connect

Cyber Sentinel is the product — the umbrella that lives on your domain.

VigilantGuard is one module inside it — the live Command Console.

Dexter's Lab (StrongRoomSE/dexters-lab) is where you write code. Edit there → push → Vercel deploys automatically.

The Command Console (VigilantGuard, Sovereign-class)

Built to match and beat the 97/100 Sovereign control-tower. It has three tiers — **Protégé** → **Operator** → **Expert** — and three live tools:

- **Threat triage** — describe an asset or worry in plain English; it scores your exposure out of 100 and recommends deception and response actions.
- **Deception grid** — plan decoys across eight domains with a live coverage ring.
- **Sphere readiness** — a five-ring view from Family → Home → Business → Government → Nation.

It runs a transparent local engine by default and an AI model only if you supply a key — nothing hidden.

Thirteen modules, one console

MODULE	WHAT IT DOES	STATUS
VigilantGuard Console	Live threat triage, deception grid, sphere readiness	Live
Sovereign Identity Fabric	Rotating, typed tokens per identity class	Verified
Outbound Egress Guard	Tokenized, traced outbound; deny-by-default	Verified
Critical-Infra Air-Gap	Nuclear / SCADA / grid isolation, data diode, false-box lockdown	Verified
Honeypot & Deception Grid	Decoy servers and bait files that pull intruders in	Prototype
Encrypted Vault	Air-gapped encrypted storage	Prototype
Forensics Test Lab	Unified sandbox that tears apart a captured copy	Prototype
...plus Filter & Track-Back Gateway, Cyber Caller ID, Ransom-Trace, and more.		

The Sovereign Ballot Fortress

The election-integrity idea you raised turned out to be the beating heart of what Cyber Sentinel already is. It maps directly onto existing modules — the air-gap layer, the sovereign identity fabric, the honeypot deception grid, and the forensics lab.

The one genuinely new piece

A **concurrent "shadow fraud-run"**: when an attacker breaches, they're fed a convincing decoy count they can tamper with all they like — while the real, sealed count stays untouched in the core. Every keystroke is recorded as evidence. This became the interactive breach demo on the site and its own architecture specification.

The breach demo walks through six steps live: outer perimeter → token mismatch → decoy handoff → forensics capture → shadow fraud-run → core intact, ending in a verdict with the real count sealed.

Four great catches from the cluster audit

When your Sovereign AI Cluster was audited, four additions stood out — the exact kind of hardening that turns a strong build into a shippable one. These are worth carrying into every project.

1 · Typed, rotating tokens everywhere

A person's token, a business token, and a government token are structurally different — so a token that doesn't match who's carrying it is flagged instantly. The moment a forged or stolen token appears, its whole type rotates across your systems, so the stolen credential is already useless. This is the "Cyber Caller ID" idea generalized across the platform.

2 · Fill the missing `.env.example` files

Several repos needed secrets that weren't documented — **aegis**, **sovereign-control-tower**, **order-of-battle**, **meridian** — so a fresh deploy silently half-worked. Documenting the required environment variables was the single biggest shared gap across the cluster.

3 · Add a `vercel.json` build command to the static sites

For the build-then-deploy sites (**proofcore**, **guardian-sphere-business**, **sixth-domain**, **lockchain**, **living-interface**), a build command lets Vercel build them automatically instead of relying on a local script being run by hand.

4 · Write READMEs for the two silent repos

lockchain — 403 files with no README at all — and **conductor**. Mature code with no front-door explanation was the most surprising gap in the whole cluster. Every serious repo deserves a door people can walk through.

Plans that cover your whole world

One subscription protects everything under your roof or your organization. Annual is the smart buy — a real discount over paying monthly. Nonprofits and people in a hard season: reach out, we help.

PLAN	WHO IT'S FOR	MONTHLY	ANNUAL	YOU SAVE
Individual	One person (+ optional work add-on)	\$39/mo	\$390/yr	\$78
Couple / 2	Two people	\$69/mo	\$690/yr	\$138
Family of 4 Most popular	A whole household	\$99/mo	\$990/yr	\$198
Large Family 9+	Big households	\$169/mo	\$1,690/yr	\$338
Business	Organizations & teams	\$499/mo	\$4,990/yr	\$998
Nonprofit / Hardship	Anyone who needs help	Contact us — we work with you		

Every plan includes all thirteen modules, the Ballot Fortress, sector coverage, and 24/7 tokenized support with a dedicated AI assistant. As capabilities are added, plans grow with them.

24/7 tokenized support

Because the network is held right in front of us and fully tokenized, no one can tamper with it — so support can help anytime, anywhere. Every operator gets a genuinely smart AI assistant trained on their exact setup, backed by a real human the moment they need one.

Four things, in order

#	ITEM	STATUS
1	Start coding today — the Dexter's Lab guide (Codespaces path A / Docker path B, first 15 minutes)	Done
2	VigilantGuard Sovereign-class console — the live console on the site	Done
3	America's Future → Born Between 2 Generals — email + logo sweep across every repo	Next
4	Passphrase-gate runbook — make every project private-but-shareable	Next

Where it all lives

Live site: cybersentinel.bornbetween2generals.com — deployed on your Kristen's Lab team on Vercel, in your black-and-teal.

Code: written in Dexter's Lab ([StrongRoomSE/dexters-lab](https://github.com/StrongRoomSE/dexters-lab)), auto-deployed on push.

Documents: this master summary, the Sovereign Ballot Fortress architecture spec, and the platform package — all downloadable so you always hold the complete picture.

The through-line

Everything here points at one idea: a defense platform that **watches back** — it never breaks the law, it never leaves your ground, and it turns an attacker's own moves into the evidence that stops them. That's the fortress that watches back.

A Born Between 2 Generals platform

Kristen@bornbetween2generals.com

Track-back, never hack-back • Lawful under 18 U.S.C. §1030 • Local-first, zero egress by default