

PROPOSAL — discussion draft. No agency or company named is involved or has endorsed it. Not an emergency service: in danger call 911; report cybercrime at ic3.gov.

Personal Cyber & TSCM Defense Service

Free at the point of use for every victim, funded by federal grants, corporate sponsors and philanthropy

America First: free the American people first, then go from there.

A public-private proposal to protect individual Americans' whole digital lives from illegal state-sponsored hacking (APTs) first, and also from stalkerware, call interception and physical bugging

Author: Masud Uddin, Founder, personaltscm.com **Prepared for:** SpaceX / xAI leadership and prospective federal partners **Date:** October 2026 · **Status:** Discussion draft

Headline: we're not asking for a case, we're asking for help

Victims need someone to **come gather the evidence and clear it, or a place to go. Agencies can take the cases from there.** Help-first means a vetted team comes on site, or the victim walks into a **regional walk-in help center** (*proposed*), and the team gathers evidence and clears and secures their devices. **No case needs to be opened first.** Afterward, with the victim's consent, the FBI and other agencies take the documented evidence and pursue whatever cases they find.

Emergency-response model (proposed targets). Run like a real emergency service: a **24/7 hotline and app**, immediate triage, a **responder callback within 1 hour**, and **same-day dispatch** of a team or a clean-channel kit (Section 7.1) for active or urgent compromise. *Proposed service targets, not guarantees.*

Independence from local police (design principle). Victims can get help without involving their local police department. Intake is independent; out-of-area responders are assigned on request; any conflict of interest is flagged and the person recused; complaints go to the independent board or an inspector general, not to a local department. This is a neutral safeguard for trust, not a judgment about any agency.

Human cost (victims' reported experience). Victims report that when they cannot afford an estimated **\$10,000–\$50,000+** for forensics, sweeps, replacement devices and legal help (*our estimate; more for persistent targeting*), the damage compounds: lost work, debt, bankruptcy and in some cases homelessness, their lives effectively destroyed. *This is victims' reported experience, not a measured statistic.*

Early detection (proposed). Victims often realize they are targeted too late. The service would offer a **free self-check** listing warning signs (unexplained account lockouts or password resets, unknown logins or devices, new configuration profiles or apps, router settings changed, unexpected location-sharing, threat notifications from Apple, Google or Meta), a **quick phone and router scan** run by responders using CISA guidance and Amnesty's open-source MVT, and an **opt-in early-warning service** that alerts enrolled people when new published indicators match what was seen on their devices, so help arrives before the damage is done.

AI-assisted defense (proposed). Frontier AI models (for example xAI's Grok and others) could help responders triage cases, analyze device logs and assemble evidence packages faster, cutting cost per victim so the service can stay free. A human always reviews findings; no client data goes to model training. *No AI company has been approached or has agreed.*

Strategy: America First. Free the American people first, then go from there. Go after the operators, not patch work

Helping victims one at a time is necessary but will never keep pace with state-backed hackers and corrupt criminal groups who reuse cheap tools at scale. The core of this proposal is to turn every victim case into evidence that lets **U.S. law enforcement go after the people, infrastructure and money behind the attacks**, domestic first, and only through lawful channels. This service never "hacks back"; it documents and refers.

Terminology. Throughout, "state-backed hackers and corrupt criminal groups" is the general term for attackers. *Advocacy framing (Masud Uddin's term, not an agency finding):* such groups seek the "digital enslavement" of individuals. Specific actors are named only where U.S. agencies have publicly attributed them: Volt Typhoon, Salt Typhoon, APT27/i-Soon (China); Star Blizzard (Russia); Kimsuky (North Korea); IRGC-affiliated actors including "CyberAv3ngers" (Iran); and the Intellexa spyware consortium.

Verified precedents show this approach works: - **Disruption:** In Dec 2023 a court-authorized DOJ/FBI operation removed Volt Typhoon's "KV Botnet" malware from hundreds of U.S. home and small-office routers (DOJ, announced Jan 31, 2024). - **Indictments and seizures:** On March 5, 2025 DOJ charged 12 Chinese contract hackers and officers (i-Soon and APT27) and seized domains and servers; victims included U.S.-based critics and dissidents. DOJ said i-Soon charged \$10,000–\$75,000 per hacked inbox (DOJ press release). In Oct 2024 DOJ seized 41 Star Blizzard domains alongside a 66-domain Microsoft civil action (Microsoft, Oct 3, 2024). - **Sanctions:** Treasury (OFAC) sanctioned the Intellexa commercial spyware consortium on March 5, 2024, citing spyware used to target Americans including officials, journalists and policy experts, and sanctioned more enablers on Sept 16, 2024.

What this service adds: individual victims rarely produce evidence agencies can use. Chain-of-custody forensics, linked across many cases (shared infrastructure, indicators, tooling), gives investigators patterns a single case can't show.

Why it fits an efficiency-first approach (our framing, not anyone's endorsement): small expert teams, one standard evidence format, minimal paperwork for victims, competing vetted vendors, published outcome metrics, and a privacy-first design (no client data sold or used for model training). It protects people's ability to communicate freely without being surveilled.

Scope: a person's whole digital life

America First here means every American's own digital life comes first: phone, accounts, home network, and the connected technology people now live with. Documented risks: - **Iran (IRGC-affiliated actors), alongside China, Russia and North Korea.** IRGC-affiliated "CyberAv3ngers" compromised at least 75 U.S.-based Unitronics controllers, including at least 34 in water and wastewater systems, Nov 2023 to Jan 2024, often through default or missing passwords (CISA AA23-335A). An FBI-led advisory (Sept 27, 2024) says IRGC actors take over **personal** accounts by impersonating contacts, journalists and family members, targeting officials, think-

tank staff, journalists, activists and people tied to U.S. political campaigns. The same day DOJ indicted three IRGC employees for a hack-and-leak operation against an identified 2024 U.S. presidential campaign. Other 2024 advisories describe Iranian password spraying and MFA "push bombing" against critical infrastructure (AA24-290A, Oct 2024) and Iran-based actors working with ransomware affiliates (AA24-241A, Aug 2024). - **Medical implants and devices.** FDA has issued cybersecurity safety communications and recalls, e.g. a firmware update for about 465,000 Abbott (St. Jude) pacemakers (Aug 2017) and a recall of certain Medtronic MiniMed insulin pumps that could be wirelessly hijacked (June 2019). In Jan 2025 FDA and CISA warned that Contec CMS8000 patient monitors contained a backdoor and leaked patient data (FDA safety communication; CISA ICSMA-25-030-01); FDA said it knew of no injuries. *Brain-computer interfaces and other bioimplants:* we found no documented attacks, so they are listed as a forward-looking risk area, not a current threat. - **Vehicles and self-driving systems.** NHTSA publishes *Cybersecurity Best Practices for the Safety of Modern Vehicles* (2022 update). Commerce's Jan 2025 rule bars PRC- or Russia-linked connected-vehicle and automated-driving software (from Model Year 2027) and connectivity hardware (from MY2030), citing data extraction and remote manipulation risks (BIS final rule, effective Mar 17, 2025). - **Robots, industrial and connected devices.** CISA publishes industrial control system (ICS) advisories on vulnerable controllers and devices, and its Apr 2026 advisory describes China-nexus covert networks built from compromised home routers, IoT and smart devices.

The service triages these when a victim is affected, refers device defects to FDA, NHTSA or CISA, and refers crimes to the FBI.

1. Summary

The main threat is illegal, state-sponsored hacking. U.S. agencies have publicly documented foreign state-sponsored advanced persistent threat (APT) groups compromising U.S. networks. CISA, the FBI and NSA describe PRC-sponsored "Volt Typhoon" pre-positioning in critical infrastructure using hijacked home and small-office routers, and "Salt Typhoon" compromising telecom networks. CISA now tells highly targeted individuals to assume their mobile communications may be intercepted. Other joint advisories describe Russian and North Korean state actors spear-phishing individual Americans, including academics, journalists, think-tank staff and NGO workers. Their tools and access are reused against many targets at almost no extra cost. An individual victim, though, has no corporate security team and usually can't afford the forensic response needed to prove it, stop it and report it.

Consumer-grade threats such as stalkerware, cheap bugs, trackers and hidden cameras, rogue Wi-Fi and IMSI-catcher-style devices add a second layer. Corporations and governments can hire forensic examiners and technical surveillance countermeasures (TSCM) teams. Ordinary people mostly face two choices: pay thousands of dollars privately, or get no help at all.

This proposal sets up a **Personal Cyber & TSCM Defense Service**. Vetted expert teams would investigate a client's own devices and premises, remove what they find, and preserve evidence to chain-of-custody standards so that law enforcement and courts can use it. **Every tier, from triage to forensics to in-person sweeps to the advanced-threat track for lone civilians, is free at the point of use for victims.** Federal victim-service grants, corporate sponsors and philanthropy pay for it, and the client never sees a bill. To keep that affordable, the service is designed to scale cheaply, as attackers do. The service is **strictly nonpartisan**. It serves any victim of any background, and no one can ever use it for political tasking. We ask for partners to back a **nationwide launch, free to every American victim (America First)**.

2. The problem

Core problem: it's too hard to get actual assistance today, and victims fall through the gap. Local police and 911 generally lack cyber capability: in a PERF survey of local agencies, only 42% of respondents had a computer or cybercrime unit, and the top barriers were lack of staffing (54%), funding (31%) and in-house expertise (29%); 66% referred cyber cases to the FBI (PERF, *The Role of Local Law Enforcement Agencies in Preventing and Investigating Cybercrime*, 2014; survey from 2013, so dated). Meanwhile the FBI's IC3 does not investigate complaints and says the FBI cannot respond to every one (below). *Victims' reported experience* is being passed between the two with no one providing hands-on help. Victims are asking for **help**, not for a case. Yet the main federal channel is built for reporting, not helping. In 2025 the FBI's IC3 received **1,008,597 complaints** reporting **\$20.877 billion** in losses (FBI, *2025 IC3 Report*). (*This covers only reported, direct losses, so it is a floor, not the true total.*) IC3 says: "Due to the volume of complaints received, the FBI is unable to respond to every complaint," complainants "will not hear from the IC3," and "investigation and prosecution are at the discretion of the receiving agencies" (ic3.gov FAQ). A 2019 DOJ Inspector General audit found the FBI's cyber-victim notification data "incomplete and unreliable," some notifications came too late to help, and victims in national-security cyber cases were not informed of their rights as required (DOJ OIG Audit 19-23). *Our inference, not an official statistic:* a lone individual targeted by state-backed hackers and corrupt criminal groups, with no company or lawyer behind them, is the least likely to get hands-on help.

Help first. Getting help requires **no case, no proof and no prosecution**. Protection, cleanup, clean devices and safety come first. Evidence is documented along the way, and afterward, with the victim's consent, the FBI and other agencies take the evidence and pursue whatever cases they find.

Guaranteed-response commitment (proposed). Every request for help is triaged within 24 hours (*service target*). Nobody is turned away for lacking evidence. If the victim opts for referral and an agency declines, the service keeps helping and documenting, and re-refers when new evidence emerges, telling the victim each step.

2.0 Hidden losses: the true cost is far higher

The FBI IC3's **\$20.877 billion** (2025) covers only **reported, direct** losses, so it is a **floor**. Most victims never report. The FTC estimates that 2023 fraud losses, **adjusted for underreporting, were \$158.3 billion** (or \$23.7 billion under a more conservative assumption), against just over \$10 billion actually reported to it, and cites a study finding only **2.6%** of fraud victims reported to a government agency (FTC, *Protecting Older Consumers 2023–2024*, Oct 2024). Neither figure counts lost businesses and startups, careers, future earnings, or harm to health and families.

Losses no one counts. Victims often can't put a provable number on what was destroyed (startups, careers, future earnings, health) because no one does the forensic work to connect the damage to the attack. Without that evidence, their losses are dismissed and never counted in any statistic.

Lifetime cost to one person (NPV)

A person's true loss is the present value of everything the targeting takes over time: **lost earnings**, the **risk-weighted value of destroyed ventures** (probability of success × value), **direct costs** (forensics, devices, legal help, relocation), **health and time** costs, and **compounding** (money and opportunities lost early can't grow).

$$NPV = \sum CF_t / (1 + r)^t$$
 where CF_t is the loss in year t , r is the discount rate and t runs from 0 to N years.

EXAMPLE numbers only, not data about any real person: $r = 5\%$. - Lost earnings: \$60,000/year for 10 years → about **\$463,300** - Destroyed venture: 10% chance of being worth \$2,000,000 in year 5 → \$200,000 risk-weighted → about **\$156,700** - Direct costs now ($t = 0$): **\$15,000** - Health and time: \$5,000/year for 10 years → about **\$38,600** - **EXAMPLE total NPV $\approx$ \$673,600**, about 30 times the \$10,000–\$50,000+ estimated cost of the forensic help that could have prevented much of it.

Founder's note, in Masud's own words: “Due to targeting for countless years by criminal and corrupt groups, and no help from anyone I've contacted, it has not been possible for me to build or complete this project, or anything else, or even to earn any basic income whatsoever. That is why I'm asking partners to take it on.” — Masud Uddin, founder (his own account)

2.1 Primary threat: illegal state-sponsored APTs

- **State-sponsored groups have compromised U.S. networks, and some target individuals directly.** These are documented by U.S. government advisories, not speculation:
- *Volt Typhoon (PRC).* CISA, NSA and the FBI assess that PRC state-sponsored actors are pre-positioning on U.S. critical-infrastructure networks for possible disruptive attacks. They route their activity through hijacked, end-of-life home and small-office routers (CISA Advisory AA24-038A, Feb 2024). The agencies also observed the actors targeting the personal email of key network staff. In December 2023 a court-authorized DOJ/FBI operation removed the "KV Botnet" malware from **hundreds of privately owned U.S. routers** the group had hijacked (DOJ, Jan 2024). In April 2026 CISA warned again about China-nexus covert networks built from compromised home routers, IoT and smart devices.
- *Salt Typhoon (PRC).* A joint advisory from CISA, the FBI, NSA and more than a dozen allied agencies describes PRC state-sponsored APT actors compromising telecommunications and other networks worldwide, including in the U.S., for persistent espionage access (CISA Advisory AA25-239A, Aug 2025). Whether the actors are still inside U.S. networks is unconfirmed: the FBI's cyber chief called them "largely contained" in mid-2025, while an FBI official said in Feb 2026 the threat is "still very, very much ongoing" and that Salt Typhoon stole information from "well over a million Americans" (CyberScoop; Nextgov, Feb 2026). After that telecom intrusion, CISA advised highly targeted individuals to **assume all mobile communications may be intercepted or manipulated** (CISA, *Mobile Communications Best Practice Guidance*, Dec 2024).
- *Spear-phishing of individuals (Russia, DPRK).* The FSB-linked "Star Blizzard" uses tailored spear-phishing, impersonated contacts and fake social profiles against individuals in academia, defense, government, NGOs and think tanks, with U.S. and UK targets most affected (CISA Advisory AA23-341A, Dec 2023). North Korea's "Kimsuky" impersonates real journalists and academics to compromise individuals at think tanks, universities and news outlets (FBI/State/NSA advisory, June 2023).
- *Commercial spyware markets.* Google's Threat Analysis Group tracks about **40 commercial surveillance vendors** and attributes to them **half of known zero-day exploits** against Google products and Android devices (Google TAG, *Buying Spying*, Feb 2024). Citizen Lab and Amnesty's Security Lab have repeatedly documented mercenary spyware on the phones of private individuals. Federal policy restricts U.S. government use of commercial spyware that poses risks (Executive Order 14093, March 2023).
- *Leaks put advanced tools in many hands.* A government-developed exploit published by the "Shadow Brokers" group in April 2017 was reused within weeks in the worldwide WannaCry ransomware outbreak (CISA Alert TA17-132A).
- **The APT asymmetry.** Attackers reuse tools, exploit chains and hijacked infrastructure across many victims, and commercial vendors resell turnkey capability. Each extra target costs the attacker little. Each

victim, meanwhile, faces the full cost of a forensic response alone. Advisories are written for organizations with security teams. A lone civilian whose phone, email or home router is compromised by a state-level actor typically has no one to examine the devices, preserve evidence, or turn findings into a referral the FBI can act on.

2.2 Secondary layers: consumer spyware, cheap hardware and rogue networks

- *Consumer stalkerware is sold openly and cheaply worldwide.* The FTC brought its first case against "stalking" app developers in 2019 (Retina-X, more than 15,000 subscriptions sold). In 2021 it **banned a stalkerware company and its CEO from the surveillance business** (Support King/SpyFone), alleging the apps let purchasers secretly monitor photos, texts, web history and GPS location. Widely sold stalkerware apps list prices of roughly **\$12–\$35 a month on annual plans, about \$140–\$420 a year** (vendor list prices compiled by consumer review sites, Oct 2026).
- *The stalkerware industry leaks victims' data again.* TechCrunch counts **at least 27 stalkerware operations since 2017** that were hacked or exposed customers' and victims' data. One held records on almost 2 million people, and another exposed data from about 26,000 victims' phones (TechCrunch, 2025–Feb 2026).
- *Cheap surveillance hardware.* Consumer location trackers, hidden cameras and covert microphones sell globally online for tens of dollars (*our estimate from retail listings*). The problem is serious enough that Apple and Google jointly published an industry specification for unwanted-tracker alerts in 2024, and Airbnb banned indoor security cameras in listings in 2024. Federal law already prohibits making, selling or advertising devices primarily useful for covert interception (18 U.S.C. § 2512).
- *Rogue networks and IMSI-catcher-style devices.* Look-alike or rogue Wi-Fi access points and compromised home routers can expose a victim's traffic. Cell-site simulators are a further layer: according to DHS, the FCC authorizes the sale of cell-site simulators only to public-safety and law-enforcement agencies. In 2018 DHS told Congress it had observed "anomalous activity" consistent with IMSI catchers in the National Capital Region and other U.S. cities, called malicious use "a real and growing risk," and said it had no current capability to detect such devices (DHS letter, March 26, 2018).

2.3 "Cyber enslavement," and why victims are left alone

- **"Cyber enslavement."** Whether the adversary is a state actor reusing a professional toolchain or an abuser paying the cost of a streaming subscription, they can take over a person's whole digital life:
- **persistent device control**, through planted stalkerware or a compromised phone;
- **account takeover** of email, cloud and social media (phishing/spoofing was the most-reported crime type to IC3 in 2025);
- **round-the-clock monitoring** of messages, calls, photos and location;
- **coercion and sabotage**, using what they learn to harass, extort, impersonate, lock the victim out of accounts or cut them off from help.

Masud Uddin calls the victim's resulting condition "cyber enslavement." Every message, movement and contact is visible to someone else, and escape feels impossible. Escaping costs far more than the attack. *Our estimates, not survey data:* forensic examination of devices, a home and vehicle sweep, replacement devices and rebuilt accounts, and possibly legal help add up to roughly **\$2,500–\$10,000+** per victim. The attacker pays **about \$140–\$420 a year** in listed subscription fees plus tens of dollars of hardware, so by these rough figures the defender pays roughly 6 to 70 times more, before counting lost work or relocation. One attacker tool is reused against thousands of victims. Defense today happens one victim at a time, at full professional rates. - **Expert help is**

expensive and hard to reach. Private TSCM and forensic services are priced for businesses. *Our estimates, based on typical market quotes and not on a formal survey:* a residential TSCM sweep costs about **\$1,500–\$5,000+**, a professional mobile forensic exam with a written report about **\$500–\$3,000 per device**, and expert-witness time is extra. Few people can pay that, and quality varies widely because the industry has no uniform licensing. - **Victims fall through the cracks.** Police often lack the capacity to examine a private citizen's phone unless a case already exists. Without proof, victims can't open a case. Without a case, nobody examines their devices. - **Good free help exists but is small.** CETA (New York City, by referral only), Access Now's free **Digital Security Helpline** (for civil society), **Citizen Lab** (University of Toronto) and **Amnesty International's Security Lab** (author of the open-source Mobile Verification Toolkit) do excellent work, but none of them is built to serve the general U.S. public at scale or to do in-person sweeps. - **Honest triage matters.** Many people who fear surveillance turn out to have no compromise. In other cases the cause is ordinary, such as a shared cloud account, a location-sharing setting or a data broker. A credible service must find real threats, clearly and respectfully explain negative results, and refer people to supportive services when that's appropriate.

2.4 The cost gap at a glance

Threat layer	Attacker's cost	Victim's cost to detect, escape and document
1. State-sponsored APT (phishing, spyware, compromised router or telecom access)	Low <i>marginal</i> cost per extra target: tools, exploit chains and hijacked infrastructure are reused across many victims and sold turnkey by commercial vendors (Google TAG; CISA AA24-038A, AA25-239A)	Advanced multi-device forensic and incident response, often \$10,000–\$50,000+ (<i>our rough estimate of private rates; no published individual-victim benchmark found</i>), plus replacement devices and accounts
2. Consumer stalkerware	About \$140–\$420 a year at listed subscription prices (Oct 2026)	Device forensic exam about \$500–\$3,000 per device (<i>estimate</i>)
3. Bugs, trackers, hidden cameras	Often tens of dollars per device (<i>estimate from retail listings</i>)	Residential TSCM sweep about \$1,500–\$5,000+ (<i>estimate</i>)
4. Rogue Wi-Fi / IMSI-catcher-style devices	Varies; not estimated here	RF and spectrum analysis, typically part of a professional TSCM sweep (<i>estimate as above</i>)

Across all layers, the defender pays many times what the attacker does, and pays it one victim at a time.

2.5 Why the defense must scale cheaply too

Paying private-market rates one case at a time can't fix a structural asymmetry. The service is built so that each case makes the next one cheaper. Everything below is defensive only:

- **Shared threat intelligence across cases.** Every confirmed finding feeds an anonymized indicator library shared across all vendors and partners, with client consent and no personal data. Examples are indicators matching CISA/FBI APT advisories, malicious app identifiers, stalkerware infrastructure and recurring tactics. Once a tool is found on one client's phone, it can be detected quickly on the next.
- **Free self-check tools first.** Tier 1 guides people through built-in protections such as Apple Safety Check, Google Security Checkup and Lockdown Mode, plus reputable mobile security apps and CISA's public mobile-security best practices (end-to-end encrypted messaging, phishing-resistant authentication, no SMS-based codes). Independent AV-Comparatives/EFF testing in 2025 found the best products detected most stalkerware samples. Many cases end here, at almost no cost.
- **Reuse of open detection signatures.** Examiners standardize on open tools and shared indicator sets, such as Amnesty's **Mobile Verification Toolkit (MVT)** and published indicators of compromise from CISA/FBI

joint advisories, Citizen Lab, Amnesty and the Coalition Against Stalkerware. The service contributes new defensive indicators back to them.

- **Volunteer-trained responders.** Following Cornell Tech CETA's model (trained volunteer technologists under professional staff, with a public clinic toolkit), the service trains advocates, IT professionals and students to handle Tier 1 triage under supervision. Senior paid experts are reserved for forensic, TSCM and advanced-threat work.
- **Standardized playbooks and reporting.** Shared intake forms, examination checklists and evidence-report templates cut examiner hours per case and keep quality consistent across vendors.

3. Case Procedure: how every case runs

Every case follows the same nine steps, whatever the threat layer, and all of them are free to the victim.

Step	What happens	Standard
1. Free confidential intake	Phone, web or encrypted channel; a pseudonym is allowed. The client receives a case number and a named responder who stays with the case.	Same-day acknowledgment (<i>target</i>)
2. Triage within 24 hours	The case is classified as APT / state-level, spyware / account compromise , or physical (bugs, trackers, cameras, RF), or a combination. A safety plan is made first in abuse cases.	Within 24 h of intake (<i>target</i>)
3. Secure first	The client gets clean loaner devices (e.g. a phone running GrapheneOS, or an iPhone in Lockdown Mode) and new accounts with phishing-resistant authentication, so they can communicate safely before anything is touched.	Before evidence work begins
4. Evidence collection	Forensic imaging of the client's devices and accounts, plus a premises, vehicle and RF/spectrum sweep where needed. Every item is hashed (SHA-256), timestamped and logged in a signed chain-of-custody record.	NIST SP 800-86, ISO/IEC 27037, SWGDE best practices
5. Analysis	Findings are checked against published indicators from CISA and FBI joint advisories, Citizen Lab and Amnesty Security Lab (including Amnesty's MVT), plus the service's shared indicator library.	Second-examiner review for APT cases
6. Findings report	A plain-language report for the client covering what was checked, what was found and what it means, plus a sealed technical package (images, hashes, logs, custody record) for law enforcement or court.	Delivered with the client's consent
7. Tracked referral	With consent, the case is referred to the FBI (field office; Counterintelligence Division for suspected state-level cases), CISA and IC3 . The referral is tracked, and the client is told its status.	Follow-up with the agency within 30 days (<i>SLA target</i>)
8. Remediation and hardening	The team removes or isolates threats where safe (physical devices are preserved as evidence), rebuilds devices and accounts, and gives hardening guidance. Check-ins at 30 and 90 days.	Re-check offered on any new sign of compromise
9. Independent audit and appeal	A sample of closed cases is independently audited. The client can appeal findings or switch to another vetted provider at any point.	Annual audit; appeal answered within 14 days (<i>target</i>)

3a. How a victim activates help (proposed one-page flow)

Low barrier to help. Victims never have to prove they are being targeted or bring evidence up front. A victim's own account, given in good faith, is enough to start triage; the team collects and documents the evidence itself.

The service is trauma-informed and never dismissive. A light good-faith screen (identity check, consent, a simple attestation) guards against abuse, such as attempts to use the service to surveil someone else.

1. **Activation and consent.** The victim contacts the service (phone, web, encrypted channel) and signs **written informed consent** covering **only the devices, accounts and network they own or control**. They can withdraw consent at any time.
2. **Protection and cleanup first.** Immediate safety steps, account lockdown, clean loaner devices where needed.
3. **Consent-based traffic monitoring.** With that consent, the team installs a home network sensor or provides a monitored VPN, using open-source tools such as **Zeek** and **Suricata** matched against CISA and FBI published indicators. Monitoring covers only the victim's own traffic.
4. **On-site visit or regional walk-in help center** (*proposed*). Device spot checks; a **detect-only** RF and hidden-camera sweep; forensic imaging of devices with **chain of custody**.
5. **Hand-off to agencies afterward, with the victim's consent.** Findings go to the FBI (field office) and IC3 as a standard evidence package, tracked as in Section 3. Agencies pursue whatever cases they find; help continues either way.

Legal guardrails. - Wiretap Act consent. Federal law permits interception when one party to the communication consents (18 U.S.C. § 2511(2)(d)), but not for a criminal or tortious purpose, and consent covers only communications the consenting person is party to. - **All-party-consent states.** About a dozen states (including California, Florida, Illinois, Maryland, Massachusetts, Pennsylvania and Washington) require every party's consent; the stricter state rule applies, so procedures default to all-party standards. - **Third parties on shared networks.** Family members, roommates or guests are filtered out of collection, or their consent is obtained. - **No jamming and no hack-back.** Jamming is illegal under the Communications Act (47 U.S.C. § 333) and FCC rules; accessing an attacker's systems is barred by the Computer Fraud and Abuse Act (18 U.S.C. § 1030). The service detects, documents and refers only. - **Licensing.** Some states (e.g. Texas and Michigan) can require a private-investigator license for certain digital forensic work; responders hold licenses where required. - **Data privacy and retention.** Minimum necessary collection, encrypted storage, access logs, a published retention limit, deletion on case close unless the victim or a legal hold requires otherwise, and no data used for any company product or model training.

4. The model: federally led, privately operated, insulated from politics

Proposed structure (not an existing program). - **Federal lead and oversight: the FBI**, which already investigates cyber intrusions, runs IC3 and has a Victim Services Division that supports crime victims. The FBI would set evidence standards, receive referrals and oversee the contractor's performance. - **CISA** contributes threat indicators, advisories and technical guidance, consistent with its role as the national coordinator for cyber defense. CISA is not a law-enforcement agency. - **DOJ** handles prosecution, seizures and forfeiture through U.S. Attorneys and the National Security Division. - **Responders:** a separate private company under federal contract (see table). Agencies interact with it **only through formal, documented referral agreements**; no informal tasking. - **Operator options (options only; none of these companies has been approached or has agreed):** the separate company could be operated or sponsored by large technology firms such as Google, Microsoft, Apple or SpaceX/Starlink, singly or as a consortium, always under the Section 5 conflict-of-interest firewall. **Fallback:** if no suitable private operator emerges, a dedicated federal unit or task force, modeled on the FBI's existing Cyber Task Forces in its field offices and the FBI-led National Cyber Investigative Joint Task Force (NCIJTF), which

brings multiple agencies together on cyber threats. - **Insulation from partisan politics:** apolitical charter, ban on political tasking, independent board, outside audits, every victim served regardless of party, no political appointees in case decisions, and mostly private funding so the service survives budget fights.

Component	Role
Federal referral pipelines	FBI IC3 and field offices, plus CISA public guidance channels, can direct individuals to the service. Cases that show crimes go back to law enforcement as evidence packages.
Funding: free to victims, insulated from politics	Mainly private sponsors and philanthropy , so the service does not depend on annual appropriations. (1) Corporate sponsors: technology, telecom and security companies give money or in-kind support (tools, hardware, connectivity) under a strict firewall: no case access, no influence. (2) Philanthropy: foundations and individual donors. (3) Federal grants as a supplement only , e.g. Victims of Crime Act (VOCA) victim-service sub-grants through state administrators where eligible. No single source may exceed a set share, <i>proposed at 40%</i> .
Private operator (proposed)	A separate private company, not SpaceX itself , chartered as strictly apolitical with a binding ban on political tasking. It employs or contracts the vetted responders and runs intake, vetting, quality control and the evidence vault under a federal contract and formal, documented referral agreements with the FBI and CISA . SpaceX/Starlink could be a partner or sponsor only, under the Section 5 conflict-of-interest firewall. It takes every victim regardless of party, and no political appointee has any role in case decisions.
Vetted vendor network	Several competing, credentialed forensic and TSCM firms, paid per case by the program at set rates (never by the client).
Nonprofit partners	Access Now Digital Security Helpline, Citizen Lab, Amnesty Security Lab, CETA (clinic toolkit), the Coalition Against Stalkerware, and local victim-advocacy organizations. <i>These are proposed partners. No partnership exists yet.</i>
Possible SpaceX/xAI contributions	Starlink connectivity for field teams and rural clients; secure infrastructure; AI-assisted triage that a human always reviews. No client data goes to model training or to any company product.

5. Anti-corruption and civil-liberties safeguards

1. **Independent board.** Includes victim advocates, a digital-rights organization, a former prosecutor, a defense or civil-liberties attorney, and a forensic scientist. No current elected official or party officer may serve.
2. **Inspector-general-style audits.** An outside auditor reviews finances, case handling and vendor performance every year. If federal funds are involved, the relevant Office of Inspector General keeps full audit rights.
3. **Multiple competing vendors and client choice.** The client picks from at least two or three qualified providers, which prevents a single-vendor monopoly. Vendors are rotated and scored.
4. **Warrant and privacy safeguards.** Work happens only with the client's informed written consent. The service never shares client data with government without that consent or valid legal process, and it publishes its policy for handling legal process.
5. **No political tasking.** The charter permanently bars any government official, donor, partner or company from directing, prioritizing or blocking a case for political reasons. Cases are accepted on need and evidence alone.
6. **Transparency reports.** Twice a year the service publishes aggregate case counts, findings by category, government requests received, and audit results, with no identifying details.
7. **Conflict-of-interest rules.** Funders, including SpaceX/xAI, get no access to case data and no say in individual cases.

6. Service tiers

All tiers are **free at the point of use**. Vendors are paid by the program at set rates, never by the client. Higher tiers are triggered by findings or risk factors, not by ability to pay.

Tier	What the client gets	Cost to client
1. Free triage	Phone, chat or web intake. Guided self-checks (Apple Safety Check, Google Security Checkup, account and location-sharing review). Safety planning with an advocate, because removing stalkerware can alert an abuser.	Free
2. Device forensic check (program-funded)	A vetted examiner images and analyzes phones, laptops and accounts using accepted tools (e.g. Amnesty's MVT plus commercial forensic suites). The client receives a written findings report.	Free
3. In-person TSCM sweep	Physical, RF and wiring inspection of the home, vehicle or small office. Countermeasures are limited to removal and documentation.	Free (when Tier 1–2 findings or risk factors warrant it)
A. Advanced-threat track	See Section 7.	Free

7. Advanced-threat track (lone civilians facing state-sponsored or other sophisticated surveillance)

This is the service's **priority track**, because illegal state-sponsored APTs are the main threat (Section 2.1). It follows the Case Procedure in Section 3 with senior staff, faster timelines and a direct referral path.

Some individuals show signs of highly capable surveillance. Indicators include an official threat notification from Apple, Google or Meta, forensic indicators that match published spyware research, or a pattern no ordinary stalker could produce. These people are often isolated, with no employer security team, newsroom or organization behind them. This track is **free** and open to anyone who meets evidence-based criteria, whatever their background or views.

- **Confidential intake.** A separate, encrypted intake channel staffed by senior analysts and a trained advocate, designed for people with no support network. Clients can use a pseudonym until they consent to share more.
- **Rapid-response senior team.** Target first contact within 24 hours and on-site within 72 hours where warranted. *These are service-level goals, not guarantees.*
- **Hardened loaner devices.** A clean phone and laptop for the duration of the case: for example a Pixel running **GrapheneOS**, or an iPhone with Apple **Lockdown Mode** turned on, plus fresh accounts and setup guidance. The client keeps working safely while their original devices are examined.
- **Full device and premises sweep.** Forensic imaging of every client device, a review of accounts and cloud data, and a complete physical TSCM inspection of the home, vehicle and workspace.
- **RF and spectrum analysis.** Passive spectrum monitoring and analysis to detect transmitters, rogue cellular or Wi-Fi activity, and hidden devices. The team **detects and documents only. It never jams**, since jamming is prohibited under 47 U.S.C. § 333.
- **Evidence preserved for a counterintelligence referral.** Where findings suggest foreign or state-level activity, the team assembles a hashed, chain-of-custody evidence package for referral, with the client's consent, to the **FBI** (field office, which can engage the Counterintelligence Division).

- **Direct line to expert researchers.** A pre-arranged, consent-based escalation channel to **Citizen Lab** and **Amnesty Security Lab** for independent analysis and attribution research. *This is proposed. It depends on those organizations agreeing and keeping their full independence.*
- **Honest outcomes.** If the team finds no evidence of compromise, it says so clearly and with care, explains what it checked, gives practical hardening steps, and offers support referrals.

7.1 Proposed "clean channel" kit for isolated, smeared victims

Some victims of suspected state-level targeting are also isolated or publicly discredited. They may have nowhere trustworthy to communicate from. A home ISP connection or router may itself be compromised, as the Volt Typhoon router botnet showed (Section 2.1). For these clients we propose a low-cost, program-owned **clean channel kit**, lent for the life of the case and then wiped and reissued:

Component	Purpose	Cost (<i>see notes</i>)
Starlink terminal (e.g. Starlink Mini) on a Roam plan	An independent internet path that bypasses a possibly compromised home ISP connection or router	Service: Roam 100GB \$55/month (starlink.com service-plans page, Oct 2026). Hardware: about \$149–\$199 (<i>third-party 2026 reports; not verified on starlink.com, so treat as an estimate</i>)
Clean loaner phone and/or laptop	A device the adversary has never touched, e.g. a Pixel running GrapheneOS or an iPhone in Lockdown Mode	About \$300–\$900 per device (<i>estimate</i>); reused across cases
End-to-end encrypted messaging (e.g. Signal)	Private channel to the response team and, with consent, investigators, in line with CISA's mobile guidance	Free

Estimated kit cost: roughly **\$500–\$1,300 in reusable hardware plus about \$55/month of service** per active case (*estimate*). That is a small fraction of a single advanced forensic engagement.

Limits, stated plainly. The kit gives a separate network path and clean devices. It does **not** make anyone invisible or immune: account security, device hygiene and safe behavior still matter, and the response team provides setup and training. **This is a proposed pairing by personaltscm.com, not an existing Starlink product or offering.** Any SpaceX/Starlink role (donated terminals, service credits) would be part of the nationwide launch partnership in Section 11.

Note on Muon Space Halo. Muon Space has announced that it will integrate Starlink mini laser terminals into its Halo satellite platform, with the first Starlink-enabled Halo satellite planned for Q1 2027 (Muon Space press release, Oct 21, 2025). That is satellite-to-satellite backhaul infrastructure for spacecraft operators, **not a consumer product and not a victim tool**. At most it is a possible future backhaul layer and plays no part in this launch.

7.2 AI-assisted defense for people who can't pay \$10k–\$50k+

A private advanced forensic response can run **\$10,000–\$50,000+**, and persistent, repeated targeting can cost a victim far more over time (*our estimate; no published benchmark for individual victims*). Few people can pay that. Frontier AI models should be built and deployed to help individual victims close that gap.

What AI does (first pass only): - Triage of incoming requests and symptoms, prioritizing urgent and active compromise. - Log and network-anomaly analysis over Zeek and Suricata outputs, Mobile Verification Toolkit

(MVT) results and published CISA/FBI indicators. - Drafting evidence reports in the standard package format. - Guiding victims step by step through cleanup and account lockdown.

Human experts check every finding before anything is referred. AI output is never treated as sole proof; every conclusion in an evidence package is verified and signed by a qualified examiner.

A call to AI labs (no lab has been approached or has agreed). We invite xAI and other labs to offer models, compute credits and safety-tuned defensive tooling for victims, free at the point of use.

Public precedents (verified): DARPA's AI Cyber Challenge (2023–2025), run with ARPA-H and frontier AI labs, ended at DEF CON 33 in Aug 2025. Team Atlanta won, and the finalists' AI systems found 54 of the synthetic vulnerabilities and patched 43, also finding 18 real vulnerabilities. The finalists' systems are being released as open source (DARPA, Aug 8, 2025). Large firms also ship AI security tooling, e.g. Microsoft Security Copilot and Google's AI-driven vulnerability research (Big Sleep); these show the technology exists, not that it is built for individual victims yet.

Privacy guardrails. AI processes data only with the victim's written consent and only for their own case; minimum necessary data; encrypted processing and storage with access logs; deletion under the retention policy; **no training on victims' data without explicit opt-in**; no data shared with any company product.

8. Evidence handling

- **Hash everything.** Every acquired image, file and log is hashed (SHA-256) when collected and again whenever it is transferred.
- **Timestamp and log.** Trusted timestamps, a photo and video record of the scene and any physical device found, and examiner notes.
- **Chain of custody.** Every handoff is recorded in a signed custody log. Physical items go in tamper-evident bags. Digital copies are stored in an access-controlled, audited evidence vault.
- **Recognized standards.** Procedures follow established guidance such as NIST SP 800-86, ISO/IEC 27037 and SWGDE best practices. Examiners must be prepared to testify.
- **Law-enforcement-ready package.** A standard report and evidence bundle formatted for IC3 submission, local police, prosecutors or civil protective-order proceedings.

9. Legal and ethical frame

- **Defensive only.** The service works only on the client's **own devices, accounts and premises**, or those the client is lawfully authorized to consent for. It **never hacks back**, never accesses a suspected perpetrator's devices or accounts, and never intercepts communications. That keeps it clear of the federal Wiretap Act (18 U.S.C. § 2511), the Computer Fraud and Abuse Act and state equivalents.
- **Found devices are evidence.** A hidden bug or tracker is documented and preserved for law enforcement, not destroyed.
- **Survivor safety first.** Teams coordinate with advocates before removing anything when doing so could escalate danger.
- **Data minimization.** Teams collect only what the case needs, keep it no longer than the client and the case require, and destroy it securely at closure unless it is held for legal proceedings.
- **Licensing.** Vendors meet each state's private-investigator and forensic-licensing requirements.

10. Nationwide launch plan (free to every American victim)

- **Coverage:** Nationwide from launch. Intake is open to every American victim in all 50 states and territories from day one, by phone, web and encrypted channel; remote triage and forensics reach anyone, and Starlink connectivity helps reach rural clients. Field capacity grows through rapid onboarding of vetted responders, not by limiting which states are served.
- **Internal phasing (capacity, not geography):** Months 0–4: governance, board, vendor vetting, evidence vault and nationwide intake. From month 5: live service nationwide, with continuous onboarding of vetted responders and partner firms. Month 18: first independent evaluation and public report, then annually.
- **Indicative launch-capacity budget (estimate, to be refined):** About \$3–5 million for initial capacity of roughly 3,000 triage contacts, 600 device exams, 150 TSCM sweeps and 25–50 advanced-threat cases, plus staff, the vault, audits and evaluation. *The full nationwide operating budget has not yet been modeled; it scales with demand and responder onboarding.* All of it is free to clients. *Target funding mix (estimate):* federal and state victim-service grants, corporate sponsors and philanthropy, with no single source above 40%.
- **Metrics:**
 - Time to first contact and to resolution
 - Share of cases with confirmed compromise, by type
 - Evidence packages accepted by law enforcement or courts
 - Client safety and satisfaction scores
 - Cost per case compared with private-market estimates
 - Audit findings
 - Equity of reach (rural, low-income, language access)
 - Zero substantiated cases of misuse or political tasking

11. The ask

1. **A nationwide launch partnership.** In-kind or financial support from SpaceX/xAI, such as Starlink terminals and service credits for clean-channel kits (Section 7.1), secure infrastructure, loaner hardware and seed funding, under the conflict-of-interest firewall in Section 5.
2. **Federal and state engagement.** Exploratory talks with FBI IC3 and field offices on referrals and evidence intake, with CISA on public guidance, and with state VOCA administrators on eligibility for victim-services grants.
3. **Nonprofit partners.** Introductions to, and agreements with, Access Now, Citizen Lab, Amnesty Security Lab, CETA and local victim-service organizations.

Contact: Masud Uddin · personaltscm.com

Sources: FBI IC3, 2025 Internet Crime Report (ic3.gov); FTC, Protecting Older Consumers 2023–2024 (Oct 2024); Kaspersky, The State of Stalkerware in 2023 (securelist.com); FTC press releases on Retina-X (Oct 2019) and SpyFone/Support King (Sept 2021) (ftc.gov); Google TAG, Buying Spying (Feb 2024); Executive Order 14093 (2023); CISA Alert TA17-132A (WannaCry); CISA, Mobile Communications Best Practice Guidance (Dec 2024); DHS NPPD letter to Congress on IMSI catchers (Mar 26, 2018), citing FCC equipment authorizations; 18 U.S.C. § 2512; TechCrunch, "Hacked, leaked, exposed" (Feb 2026) and related 2025 breach reports; consumer review-site compilations of stalkerware list prices (Oct 2026); Apple–Google unwanted-tracker specification (2024); Airbnb indoor-camera policy (2024); Cornell Tech Clinic to End Tech Abuse (ceta.tech.cornell.edu); DOJ

Office for Victims of Crime, Crime Victims Fund (ovc.ojp.gov); Access Now Digital Security Helpline; Citizen Lab; Amnesty International Security Lab / Mobile Verification Toolkit; AV-Comparatives & EFF, Stalkerware Test 2025; CISA Advisories AA24-038A (Volt Typhoon, Feb 2024), AA25-239A (Salt Typhoon-overlapping PRC APT activity, Aug 2025), AA23-341A (Star Blizzard, Dec 2023); FBI/State/NSA Kimsuky advisory (June 2023); DOJ, KV Botnet disruption (Jan 2024); CISA, China-nexus covert networks advisory (Apr 2026); starlink.com service plans (Oct 2026); Muon Space press release (Oct 21, 2025). All prices, budgets and service targets are estimates unless a source is cited.
