Comprehensive Proposal on International Cooperation and Standardization of a Decentralized Emergency Rescue Application

Overview
A lightweight artificial intelligence system is essential, and the application can be developed within three months by a small team of three university-level developers.

Sender: https://mcorpai.org/
Recipients: Ministries of Foreign Affairs, Public Security and Law Enforcement Agencies, Consular Affairs Divisions at Embassies, International Investigation Cooperation Departments, Disaster and Crisis Communication Policy Units, Data Protection Authorities, Mobile and Satellite Communication Providers, Senior Executives of Device Manufacturers, Human Rights and Humanitarian Organizations, Academic, Medical, and Legal Advisory Panels
Date: August 17, 2025
Purpose of Document: This document provides a comprehensive integration of the technical, policy, and governance dimensions of a decentralized emergency rescue application designed to ensure uninterrupted transmission of life-saving signals in environments of communication breakdown, including scam compounds, overseas abduction and confinement, as well as disaster and conflict zones.

The document elaborates practical deployment strategies such as hidden offline storage policies, a triple power button trigger, 15-second delayed activation and 10-minute interval location transmissions, designation of three family contacts, short-range Bluetooth alerts with community relay networks, pre-installed app strategies by manufacturers, region-specific satellite message adaptation, data protection and international governance measures, standardized packages for law enforcement submission, and a phased roadmap for development and deployment at a commercial-ready level.

Additionally, the document highlights recent cooperation trends between Samsung Electronics and Musk-affiliated entities, the progress of global satellite direct-link services, and the legal-technical framework for operating hidden storage in cases of complete communication blackout.

The narrative adheres to diplomatic writing style, structured entirely in prose without tables or bullet symbols.

Preface

This proposal is premised on the ethical use of technology and does not pursue commercial profit. The application will be distributed free of charge on both Android and iOS platforms, with no advertisements or paid features. Personal data collection will be minimized, and end-to-end encryption will be applied. Regional data sovereignty will be fully respected. The ultimate goal of this project is to ensure that survival signals and critical evidence are not lost, even in moments when communication and public authority cannot reach those in danger.

Background and Problem Definition

In recent years, repeated rescue gaps have emerged in regions such as Myanmar, Cambodia, and Laos due to confinement-type crimes known as scam compounds. Escape from such environments is virtually impossible. AI-based statistical analysis estimates the probability of abduction during tourism in Myanmar, Cambodia, and Laos at approximately ten percent. Victims are controlled through violence, while local authorities are either corrupt or inaccessible, and communication networks are frequently disabled by deliberate shutdown or infrastructural failure. Consequently, a system is required that can prepare signals even when the user is unable to operate the device, automatically transmit them once networks are restored, and circulate anonymous alerts safely within close proximity. This proposal presents the minimum and sufficient conditions to achieve this goal through the integration of technology, policy, and governance.

Vision and Principles

The application operates under the assumption that it is always on. Users are protected without requiring deliberate actions. Stealth is prioritized in screen display, sound, and vibration to avoid endangering victims and bystanders. Communication routes are designed with multi-layered backup structures, ensuring functionality even if one pathway is blocked. All data complies with strict purpose limitation and minimal retention principles, with access and submission remaining under the control of victims and their families. Policies will be tailored to regional

laws, cultures, and languages.

First: User Triggers and Automation Layers
The primary trigger is pressing the power button three times in quick succession. This trigger functions even when the screen is off, initiating a fifteen-second delayed activation timer. The user may cancel within five seconds through a long press or predefined gesture, with cancellation patterns being separately recorded. On-device voice recognition is designed to detect multilingual safety words such as “help me” in noisy environments. If the device is powered off or forcibly shut down, the system prepares a summary of the last known location and time. When an external USB connection or unauthorized Bluetooth pairing attempt is detected, the system assumes irregular seizure and prepares a pre-alert. Absence of user interaction combined with reduced motion and abnormal mobility patterns elevates the risk score, leading to automatic activation. All triggers are hierarchical and cross-verified to minimize false positives.

Second: Hidden Storage Policy for Offline Environments
When networks are unavailable, evidence preservation takes precedence. Once the emergency trigger is activated, the smartphone automatically records audio, GPS coordinates, time, and accelerometer data, encrypting them into a secure hidden storage located at the firmware and security-chip level. This storage cannot be accessed through file browsing or standard resets and is isolated in a separate partition. Even if organized crime groups attempt to reset the phone for resale, the stored data remains intact. Deletion or unlocking is only possible through manufacturer account authentication and compliance with legal requirements, handled via official portals. Once the network is restored, the application first transmits a low-data summary signal to three designated family members, followed by sequential uploads of recorded logs. Families may then generate standardized packages for police and Interpol submission. The hidden storage remains invisible on the interface, making it difficult for perpetrators to identify. This policy assumes integration with manufacturers’ firmware and security chips, ensuring consistency throughout the device lifecycle. Even if the user requests deletion, a secure waiting period and family confirmation procedure must precede release. Users may only request deletion via

manufacturer portals with authentication, and no deletion function will be exposed within the app itself.

Third: Adaptive Routing of Communication Pathways

Communication follows a multi-layered backup hierarchy. The first priority is ordinary SMS and data channels to transmit summary signals to three designated family members and trusted contacts. The second priority is international SMS gateways and roaming pathways, with periodic retries in case of failure. The third priority leverages regionally available satellite messaging routes, enabling text transmission directly from existing LTE devices in areas with direct satellite link coverage without requiring additional hardware. The fourth priority applies in complete offline conditions, during which evidence bundles are preserved in hidden storage and automatically uploaded once connectivity is restored. The application autonomously detects device capabilities, carrier policies, and regional conditions to select the optimal route. This architecture balances the use of satellite pathways, activating them immediately where available while avoiding excessive reliance.

Fourth: Proximity Alerts and Citizen Relay Networks

Proximity alerts prioritize anonymity and safety. When the trigger is activated, the device broadcasts a short one-time token via non-connectable Bluetooth signals. Nearby devices with the same application installed or with manufacturer pre-installed consent will detect the token and either display a disguised general notification or quietly relay it to servers. Crowd alerts are only exposed when multiple devices detect the same token within a short time window, thereby reducing false positives. Citizens are encouraged not to intervene directly but to observe, report, and take avoidance measures. This feature is particularly critical in regions such as Laos, Myanmar, and Cambodia where networks are often unavailable. In such cases, smartphones store abduction coordinates and, upon Bluetooth contact with other random devices, relay alerts through a baton-pass mechanism, extending notifications over several kilometers. However, since relying solely on Bluetooth baton-passing has inherent reliability limits, the system is designed so that beacons handle only the first hop, while subsequent relays default to internet-based communication whenever available. In complete offline scenarios, delay-tolerant mesh networks supplement baton-passing,

operating under the constraint of slower transmission speeds.

Fifth: Bluetooth Technology Realities and Design Principles

The effective range of built-in low-energy Bluetooth varies from a few meters indoors to several dozen meters, occasionally reaching around one hundred meters in open outdoor conditions. While Bluetooth 5 long-range mode theoretically extends coverage, performance fluctuates due to operating system, firmware, and environmental interference. Therefore, while short-range alerts are feasible, direct multi-kilometer transmission is not practical. The application employs non-connectable advertising broadcasts to minimize power usage and traceability, with tokens rotated and signed at minute-level intervals to prevent spoofing. Background scanning is optimized with low-frequency windows and event-based activation to reduce power drain. Pre-installation as a manufacturer default app allows access to background permissions and low-power optimization, increasing operational reliability. Although Bluetooth cannot ensure immediate large-scale abduction alerts, it serves as a vital emergency feature when networks are absent. In such cases, the device stores GPS coordinates locally and automatically relays them once another device's Bluetooth is activated, enabling baton-pass style transmissions.

Sixth: Family Dashboard and Operations Center Integration (Lightweight AI Requirement)

The family dashboard clearly displays the last signal time, final coordinates, and recent movement patterns, along with device battery status, transmission path success or failure, and reasons for failure. An automatically generated incident timeline, risk grading, and recommended actions are provided. One-click functions connect families to calls, messages, local police, consular officers, and Interpol points of contact. Standardized report export features allow families to immediately generate law enforcement submission packages. If family members do not respond within a set period, escalation occurs to a pre-designated trusted third party or official contact. Regional operations centers provide follow-up support under family authorization, with data access limited strictly to essential scope.

Seventh: Stealth UX and Safeguards

The application provides a hidden mode where the icon and settings appear under disguised names. During emergency signal transmission, screen, flash, and sound remain inactive by default. Transmission can be canceled within five seconds using a long press or specific gesture, with cancellation patterns separately recorded. Multi-trigger cross-verification and short buffering windows reduce false activations, while citizen alerts are exposed progressively only when risk scores exceed thresholds. If perpetrators attempt to remove the application, safeguards such as removal delays, family notifications, and recovery guidance are automatically activated.

Eighth: Data Protection and DPIA Perspective

Data protection is embedded from the design stage. Rescue signals and evidence bundles are transmitted with end-to-end encryption, with server retention minimized. Clear notices are provided on purpose and retention periods. The citizen network does not share phone numbers, names, or device identifiers. Access rights are restricted to victims and families, and submission to law enforcement requires explicit approval by family members or legal guardians. Regional data sovereignty and cross-border transfer restrictions are fully respected, with high-risk regions prioritizing local storage and delayed uploads.

Ninth: Legal Compliance and International Governance

The application complies with telecommunications and data protection laws of each jurisdiction. In countries where satellite communications are sensitive, operations focus on terrestrial routes with additional minimization and stealth measures. Multilateral agreements with governments, international organizations, and civil society are pursued to ensure that app-generated evidence can serve as valid inputs for official case initiation. Institutionalized channels for cooperation with investigative authorities will include reception gateways and digital evidence verification procedures.

Tenth: Manufacturer Pre-Installation and Implications of Samsung Cooperation

Pre-installation as a manufacturer default app exponentially expands coverage. It ensures background scanning rights and low-power optimization at the system level, while allowing clear opt-in prompts

during initial setup for anonymous SOS detection and relay functions. Default SOS apps cannot be forcibly deleted by perpetrators, nor can they be removed through standard resets, as they are integrated into the smartphone system itself. Hidden storage is securely managed via manufacturer accounts and portals with robust identity verification and legal compliance. Recently, Samsung announced service integration with Tesla in the energy sector and expanded cooperation in semiconductors through major supply agreements. These trends create tangible opportunities for interoperability validation and joint pilots between device manufacturers and satellite communication networks. This proposal requests joint pilots for default app integration and satellite message pathway linkage.

Eleventh: Adaptive Use of Direct-to-Cell Satellite Connectivity

Satellite-based direct-to-cell text services are at varying stages of commercialization by country. Some regions have expanded coverage for text messaging using existing LTE phones, with data and voice planned for gradual rollout. In conflict zones, pilot satellite messaging has been tested as a contingency during terrestrial outages. The application autonomously evaluates device capabilities, carrier policies, and regional regulations to determine when satellite pathways should serve as backup. In supported countries, text and coordinates are prioritized for transmission. In unsupported regions, the application assesses built-in satellite SOS features and guides users accordingly. In jurisdictions where satellite usage is legally sensitive, stealth measures are strengthened and offline evidence preservation is prioritized.

Twelfth: Development Roadmap and Phased Deployment

Development and deployment proceed step by step. At Stage 0, risk scenarios, user research, and legal reviews are conducted. At Stage 1, a minimum viable product is launched including power button triggers, voice safety words, basic BLE beacons, three-family notifications, and hidden storage. At Stage 2, participatory relay networks are established, with always-on listener devices placed in schools, stations, and public facilities to enhance detection and relays. At Stage 3, manufacturer and carrier partnerships are finalized for default app installation, background permissions, and international SMS gateway integration. At Stage 4, satellite message pathways are activated in supported countries, with

integration into device SOS features. At Stage 5, standardized case formats are established with international organizations and investigative bodies, alongside continent-level operations centers for continuous support.

Thirteenth: Quality Assurance and Testing Plans

Functional tests will cover trigger recognition, delay activation, cancellation gestures, and false-positive rates. Performance tests will measure detection rates and delays in dense urban and mixed indoor environments across different seasons and times. Battery tests will evaluate long-term power usage during screen-off scanning and event-based activations. Security tests will regularly assess token signing verification, key protection, and minimal privilege server policies. Field drills will be conducted quarterly in cooperation with NGOs and consular offices abroad.

Fourteenth: Performance and Battery Optimization

Battery consumption is minimized through low-frequency scans and event-based activations, with scanning frequency increased only during risk pattern detection. Voice recognition relies on short keyword spotting models executed entirely on-device, eliminating network dependency, with language packs dynamically loaded by region. GPS toggles between high-precision and low-power modes as needed, with coordinate data separated into summaries and originals for transmission.

Fifteenth: Detailed Security Architecture

Signal tokens rotate and are signed at minute-level intervals to prevent forgery. Key management leverages device security chips and operating system secure zones, while server access is strictly controlled through minimal privileges, short sessions, and audit logs. Encryption keys for hidden storage are managed exclusively within the device, making external extraction impossible. No personally identifiable information is shared across the citizen network, with only anonymous statistics aggregated. Data deletion requests are promptly honored within reasonable scope.

Sixteenth: Data Model and Log Management

Rescue signals consist of headers containing incident identifiers, coordinates, timestamps, route summaries, and risk levels, along with

optional metadata. Logs include transmission time, route selection, success or failure status, retry counts, and battery levels, with automatic expiration policies deleting entries after defined periods. Evidence bundles contain recordings, coordinate continuity, and accelerometer samples, accompanied by hashes and signatures for integrity verification.

Seventeenth: Operational Metrics and Transparency

Key indicators include active installations, automatic transmission counts, successful delivery rates, family follow-up initiation times, and false alert rates. Regional performance metrics such as path success rates, battery impact, and background error frequency are continuously evaluated. A transparency dashboard publishes anonymized metrics to build public trust. External audits and results of simulation drills are disclosed in summary reports.

Eighteenth: Field Deployment and Training

Offline installation kits, multilingual manuals, and short training videos are distributed through local NGOs. Training content covers safety word selection, cancellation gestures, family dashboard use, and ethics of the citizen network. Fixed listener devices and guidance materials are installed in airports, terminals, and public facilities. Embassies and consular call centers establish standardized intake and response procedures for incident reports.

Nineteenth: Funding and Sustainability

Development and operations are supported by public-interest funds, corporate social responsibility initiatives, and international organization grants. Governments may cover the cost of low-volume text transmissions as a public safety measure, while all application features remain free of charge. Manufacturers, telecom providers, and satellite operators can support pilot programs and coverage expansion under ESG frameworks.

Twentieth: Risk Assessment and Mitigation Strategies

In jurisdictions sensitive to satellite communications, risks are mitigated through stealth UX, data minimization, and offline evidence policies. Misuse of crowd alerts is curtailed by multi-detection thresholds and phased exposure. Battery consumption is reduced via low-frequency scans and event-based detection, while attempted removals trigger

hidden mode, removal delays, and family notifications. In high-risk regions, conservative defaults are applied to citizen alerts.

Twenty-First: Country-Specific Pilot Policies

In satellite-friendly countries, satellite message pathways are activated as default backups. In satellite-restricted regions, terrestrial retries and offline evidence storage take precedence. In high-risk zones, higher thresholds are set for citizen alert exposure, prioritizing family and operations center responses. Embassies are integrated into standardized routines for incident intake and evidence submission.

Twenty-Second: Law Enforcement Submission and Chain of Custody

Standardized packages include incident timelines, coordinate continuity summaries, signal path logs, device state summaries, and original recordings. Hashes and signatures ensure integrity verification. Submission channels use encrypted pathways, and law enforcement verifies signatures and time synchronization to confirm evidentiary reliability.

Twenty-Third: Localization and Accessibility

The application supports multiple languages with both Romanized and local scripts. Features for low-vision and hearing-impaired users include enhanced screen contrast, subtitles, and haptic feedback. Voice safety words are trained to recognize local languages and accents, with offline language packs provided.

Twenty-Fourth: Citizen Network Ethics and Educational Messaging

Citizen alerts emphasize observation, reporting, and avoidance rather than direct intervention. Users are guided to prioritize personal and others' safety and to avoid risky confrontations. False reports and misuse are blocked, with repeat violations subject to regional policy sanctions.

Twenty-Fifth: Specific Proposals for Samsung Cooperation

Implementation includes pre-installed apps, hidden storage integrated into firmware and security chips, background scan optimization, opt-in consent for anonymous SOS detection and relay during initial setup, and region-specific satellite message auto-selection linked to Samsung

accounts and portals. Joint interoperability testing between devices and networks can be pursued through semiconductor and AI cooperation channels, with life-saving outcomes reflected in ESG reports. Safety functions serve as decisive factors in consumer purchasing, strengthening trust in regions with security concerns and in markets prioritizing protection for youth, women, and the elderly.

Twenty-Sixth: Communication and Crisis Response Protocols

In emergencies, the family dashboard provides recommended actions and contact sequences. Communications escalate from family to trusted third parties, local police, consular officers, and Interpol if earlier attempts fail. Media responses are managed by operations centers, with victim identities protected. Incorrect alerts are transparently corrected through public notices.

Twenty-Seventh: SDK and Open Interfaces

A lightweight software development kit and open interfaces allow third-party apps and devices to participate in anonymous detection and relays. Participation is opt-in, with all data anonymized. Fixed listener devices operated by governments and public institutions integrate under the same standards.

Twenty-Eighth: Installation and Removal Policies

The application may also be installed offline via files or QR codes. Removal remains under user control but is safeguarded against forced deletion by attackers through hidden modes and removal delays. Families are notified upon removal, and evidence stored in hidden storage is preserved unless explicitly authorized for deletion.

Twenty-Ninth: Developer and Audit Record Management

All code changes undergo review and signature processes, with builds and deployments recorded for reproducibility. External audits and bug bounty programs help identify and patch vulnerabilities early. Significant policy changes are communicated in advance to stakeholders.

Thirtieth: Conclusion and Joint Action Request

This proposal presents a multi-layered design ensuring that rescue signals and evidence are not lost even in the absence of communications and public authority. By combining manufacturer pre-

installation, adaptive regional use of satellite message pathways, and hidden storage policies, the reliability required to save lives is achieved. We request review and joint pilots from your esteemed institutions and corporations. Specifically, we propose manufacturer cooperation on pre-installation and security chip integration, telecom and satellite company collaboration on international gateway and satellite pathway activation, and public authority efforts toward standardizing data formats and institutionalizing case initiation procedures.

Appendix A: Functional Integration Summary

Key features include free distribution without advertisements, simple registration, designation of three family contacts, triple power button triggers, voice safety words, power-off and USB detection, 15-second delayed transmissions, 10-minute interval location summaries, hidden offline storage with sequential uploads upon network restoration, proximity anonymous alerts and relays, international SMS and roaming backups, regional satellite messaging pathways, family dashboard and law enforcement packages, stealth UX with cancellation gestures, and hidden modes.

Appendix B: Data Minimization Principles

Account identifiers are pseudonymized, with only phone numbers and email addresses collected as mandatory information. Location and recordings are collected solely within the context of incidents, with automatic expiration policies applied. Logs and audit data are minimized to the extent required by law.

Appendix C: Standard Submission Package

The package includes incident timelines, coordinate continuity summaries, signal path logs, and device state summaries, all verified through hashes and signatures to prove integrity. Submission formats adhere to both court and police standards.

Appendix D: Regional Policy Differentiation

In satellite-friendly countries, satellite message pathways are activated as backups. In restricted countries, terrestrial retries and offline evidence policies are prioritized. In high-risk regions, citizen alert exposure is managed conservatively.

Appendix E: Field Deployment and Training Kits

The kits include offline installation files, QR code guides, multilingual manuals, and training videos. Training modules are designed for completion within thirty minutes. Deployment is prioritized in airports and terminals in cooperation with embassies.

Appendix F: Technical Specifications of Offline Evidence Bundles

Evidence bundles are encrypted and stored within secure device areas, with keys protected by security chips or OS-protected zones. Release is only possible through manufacturer account-based authentication. Uploads begin with summaries, and originals are transmitted sequentially after family approval.

Appendix G: Sample Explanatory Notes for Diplomatic and Security Authorities

A one-page standard brief outlines the application's objectives, data handling principles, incident intake procedures, and international cooperation channels. It includes call response scripts for consular staff and technical validation checklists for investigative agencies.

Appendix H: Pilot Deployment Scenarios in High-Risk Regions

In high-risk regions such as Myanmar, Laos, and Cambodia, deployments proceed discreetly through local NGO partners and embassies. At the initial stage, citizen network alerts remain deactivated, focusing instead on family and operations center responses. Upload windows are aligned with timeframes most likely to see terrestrial network restoration.

Appendix I: Compliance Guide for OS and Manufacturer Policies

Background scanning, automatic transmissions, and location collection comply with operating system policies, requiring explicit user notifications, persistent indicators, and clear opt-in consent. Regular audits are conducted to ensure adaptation to policy changes.

Final Note

This expanded double-volume edition incorporates all key elements of the previous version while significantly strengthening technical design. It also provides ready-to-use operational drafts for diplomatic and security authorities, as well as for manufacturers, telecom providers, and satellite

operators. Based on this document, we propose the sequential drafting of technical specifications, memoranda of understanding, and operational manuals.

AI Review & Refinement Notes

Original:
“Escape from scam compounds is virtually impossible, abduction probability 10%”
Refined:
“Reports consistently indicate that escape from scam compounds is extremely difficult. (Quantitative figures should be cited in footnotes only when official statistics are available.)”

Original:
“Deletion impossible, reset impossible”
Refined:
“When integrated with manufacturer firmware and security chips, deletion is effectively constrained through delay mechanisms, re-authentication, and family notifications. At the standard app level, hidden mode and restoration guidance are applied instead.”

Original:
“Relay via Bluetooth baton-passing over several km”
Refined:
“Detection occurs through a short-range single hop (BLE advertisement), which then relays via the detecting device’s internet/satellite link to expand the coverage radius. In fully offline settings, delay-tolerant mesh networking is assumed.”

Original:
"Cooperation trends with Samsung Electronics and Musk-affiliated companies"
Refined:
"Device–satellite communication interoperability pilots are accelerating worldwide, making this an opportune moment to propose cross-vendor trials. (Specific corporate relationships should be noted via recent press releases in footnotes.)"

Seven Key Areas for Strengthening

1. Moderate quantitative claims (verifiability).

- Instead of "abduction probability 10%," use qualitative terms like "frequent reports of abductions" unless an independent source is available. If numbers are necessary, always provide a citation or methodological note.

2. Adjust language around 'undeletable/unresettable' (realism).

- Claiming that third-party apps cannot be deleted at all will face pushback under OS policies.

- Suggested phrasing: *"When integrated at the firmware/security chip level, hidden evidence remains protected against user deletion or reset (with delay, re-authentication, and family notification features)."*

3. Clarify Bluetooth range mechanics (technical accuracy).

- "Instant multi-km propagation" can mislead. Since your architecture already assumes delay-tolerant messaging plus internet relays, describe consistently as *"short-range hop detection →internet relay."*

4. Flag iOS/Android background restrictions (preempt review risks).

- Triggers like “triple power button press, background voice keyword, or continuous BLE scanning” are highly sensitive under iOS policy.

- Suggested phrasing: *“Operates within OS policy boundaries (subject to manufacturer/operator authorization); in standard app mode, alternative triggers (widgets, shortcuts, wearables) are provided.”*

5. Note legal/regulatory risks (assure authorities).

- Provide a table outlining: satellite restrictions, encryption/localization rules, lawful interception (LEA) requests.

- Current wording (“purpose limitation, minimal retention, family consent”) is strong; add one line on *“emergency disclosure in cases of imminent or severe harm.”*

6. Sharpen collaboration tracks (clear CTAs).

- OEM: *“Pilot for pre-installed app + secure chip key storage.”*

- Telecom/satellite: *“Whitelist for international SMS gateways + satellite message routing.”*

- Diplomatic/security: *“Adoption of standard incident format (timeline, signature, hash) via MOU.”*

- DPA: *“Advance DPIA consultation + audit rights.”*

- Present these one-liners upfront in a “Calls to Action” box.

7. Provide phased timelines & KPIs (credibility).

- The “3 months / 3 developers” claim is ambitious. Instead:

    - Phase 1 (MVP): 3 months
    - Phase 2 (Relay network): 2 months
    - Phase 3 (OEM/gateway integration): 3 months
- Include KPIs such as: delivery success rate, false activation rate, average family response time.

Structural Refinements (reader-friendly)

- **One-page Executive Summary immediately after cover:**
    - Purpose (2 lines)
    - Threat model (3 lines)
    - Triple-axis solution (3 lines)
    - Stakeholder asks (4 lines)
    - Pilot timeline & KPIs (3 lines)
- **Main body:** keep narrative form. Move statistics, policies, and technical constraints into **tables/appendices** for faster review.
- **Appendices:** chain-of-custody sample, DPIA checklist, 1-page MOU template.
- Aim to give reviewers the sense of a *“ready-to-sign draft.”*

Overall Assessment

The strategy is sound and presents a framework that **diplomatic,**

security, manufacturing, and telecom stakeholders can review and align with together.

By refining expression in the **four sensitive areas (numbers, deletion claims, BLE range, OS constraints)**, the proposal will more easily pass policy and legal review.

In conclusion: it is a *strong strategy*, and with just a few phrasing changes plus 2–3 supporting tables, the document will be at submission-ready quality.