Custom Hardened Mobile OS development for PriMe Project

1	**Problem Statement**	Development of securely hardened mobile OS and flashing of the same on UE handset. It should be easy to plug it into C-DOT PriMe Solution.
2	**Technology Area**	4G/5G Networks, Audio/Video codecs, VoIP Communication Systems, Instant Messaging solutions, Software development tools and frameworks
3	**Project Introduction**	The solution should be a highly secure mobile operating system, preferably in lines with AOSP, and should be capable of running applications build for Android Platform without depending upon Google Play Services or any other similar service. The solution should include the highest levels of security measures and should plug any kind of known vulnerabilities in the base OS/ Kernel. It should also prevent the system from the upcoming Zero Day Attacks through regular patching. The solution should support the existing PriMe Product Suite developed by C-DOT for Android OS. The solution should be customisable as per the security requirements shared by C-DOT based upon the feedback of user agencies. The solution aims to deliver high-quality, real-time audio/video communication tailored for 4G and 5G mobile networks. The solution will enhance the existing PriMe solution developed by CDOT, ensuring seamless integration and interoperability with it. Leveraging the multimedia communication framework developed by C-DOT, this solution should support multi-stream capabilities along with file/ image/ video sharing for enhanced collaboration between the users and should be optimised in terms of battery usage and maximum duration of service after full charge. It should be able to accommodate multiple network conditions and device types. System should have robust quality of service (QoS) mechanisms to ensure a seamless user experience, strong security protocols to protect sensitive information, and interoperability with diverse systems, facilitating effective communication across platforms. The solution should be compatible with the 3GPP standards for 4G/ 5G networks. This solution is ideal for a wide range of use cases, including enhancing connectivity and collaboration in critical scenarios. By utilizing the advanced capabilities of 4G and 5G networks, the project seeks to empower Government Officials with reliable, efficient, and secure text/audio/video communication tools while maintaining low latency, low bandwidth and storage requirements.
4	**Description**	**Key Features**:

		1. Hardened Kernel ● Solution should support runtime kernel protection and detect/ mitigate memory-based exploits dynamically. Combined with proactive patching for zero-day vulnerabilities. **2. Hardened OS Components** ● Solution should apply rigorous hardening to system libraries and OS components, incorporating fuzz testing and secure coding practices. Its hardened components should reduce the attack surface and defend against sophisticated exploitation techniques. **3. Built-in VPN** ● Solution should harden the VPN system APIs while the VPN client app and VPN backend service is provided by C-DOT **4. Built-in MDM** ● Solution should make necessary changes in OS to support MDM at OS level. Solution should harden MDM system APIs. While the MDM client app and server will be provided by C-DOT. **5. VPN Always On** ● VPN disconnection prevention mechanisms ensure all traffic is secured without interruptions, enforced at the kernel level for reliability. **6. All Data Routed Through VPN** ● Solution should offer enhanced traffic routing through C-DOT VPN, ensuring no data bypasses the encrypted tunnel. **7. MDM Always On** ● Solution should ensure MDM services cannot be disabled without explicit authorization, enforced through secure hardware-backed policies. **8. Improved Biometric Authentication (Stored in TEE, TPM)** ● Biometric data is isolated in a Trusted Execution Environment (TEE) ensuring secure and accurate authentication.

		9. Update VPN OTA Without OS Update ● Solution should allow independent updates to VPN components, ensuring clients can quickly adapt to emerging threats without OS-level changes. Solution should make necessary OS changes to support this. **10. Update MDM OTA Without OS Update** ● Solution should enable OTA updates to MDM features via a secure, cryptographically signed channel, ensuring uninterrupted service. Solution should make necessary OS changes to support this. **11. Update OS OTA** ● Solution should ensure seamless OTA updates with verified cryptographic signatures and ensures compatibility. Solution should harden the OS update system. **12. PIN and Password Brute-Force Protections** ● Solution should implement exponential delay mechanisms and forensic-grade wipe options after failed attempts, ensuring data security against brute-force attacks. **13. Forensic-Grade Secure Data Deletion on Brute-Force Login Attempts** ● Solution should implement Proprietary deletion algorithms ensure irrecoverable data wiping, exceeding forensic-grade standards. **14. Removal of Default Apps of OS** ● A fully modular OS allowing removal or replacement of default apps, minimizing attack vectors and enhancing customization. **15. Removal of Default App Store Reliance** ● Solution should add whatever app store app is provided by C-DOT and remove any dependency on the default App Store. **16. Ephemeral Sessions for Sensitive Apps**

		● Sessions leave no trace, leveraging in-memory storage and automatic purging mechanisms. **17. Frequent, Automatic Security Updates** ● Our proactive approach ensures updates should be pushed immediately when vulnerabilities are identified, with minimal user intervention. **18. Verified Update Channels with Cryptographic Signatures** ● End-to-end signing validation prevents tampering, ensuring updates originate only from trusted sources. **19. Randomized MAC Addresses for Wi-Fi Connections** ● Enhanced randomization protects against tracking while ensuring seamless connectivity. **20. Location Spoofing for GPS Tracking Control** ● Solution should make the client Location Spoofing APIs in the OS. It should interface with the C-DOT control server. **21. Restricted Access to Unique Device Identifiers** ● Solution should implement strict access controls over identifiers like IMEI and serial numbers, ensuring they're accessible only to authorized entities. **22. Administrative Control Over Debugging and ADB Access** ● Centralized control mechanisms allow fine-grained access management, ensuring only authorized debugging. **23. Secure Data Wipe on Factory Reset** ● Solution should implement secure wiping mechanism exceeding international standards, ensuring no data recovery is possible. **24. Removal of Default OS Launcher and Configure Custom Launcher** ● Solution should offer a fully customizable launcher with granular control over functionality and interface design. **25. Secure WebView Implementation**

		• Solution should offer WebView implementation that incorporates sandboxing and advanced security mitigations to prevent injection and other common web attacks. **26. Support for multiple isolated user profiles**
5	**Roles & Responsibilities of C-DOT**	C-DOT will provide technical development assistance, and financial support to the project partner(s) selected through a process of evaluation and due diligence conducted by a committee of subject experts. Wherever deemed necessary and depending upon the project type (i.e. co-development or fully outsourced), C-DOT may arrange resources, equipment, training, testing infrastructure, mandatory clearances, statutory permissions, and provide gap funding to the partner(s) in realizing the respective target deliverables. Development costs of the module, whether developed from scratch or derived from existing background technology of partner(s), shall be borne by C-DOT. C-DOT shall use the final solution for integration with production grade software. C-DOT reserves the right to modify and enhance the solution and provide it to C-DOT customers or another Partner(s). C-DOT shall engage with Partner(s) on a non-exclusive basis and shall retain its right to develop similar projects/products through other developmental programs.
6	**Roles & Responsibilities of Partner(s)**	The Partner(s) may build the required module afresh or by modifying pre-existing background technologies available with them. As per the project demand or project type, the Partner(s) may utilize the available test and infrastructure facilities offered by C-DOT with no/some financial implication for its usage. Specialised equipment required for system specific testing and demonstration of solution capabilities, will have to be arranged by the partner(s). All commercial proposals shall include necessary cloud infrastructure cost as per requirements, manpower and cost breakup (Capital, Consumables, Travel, DA, Training, Contingency, Overhead, GST etc.). The proposal should include minimum of one year support for enhancements and capacity building for future enhancements in the product. Participation in the project shall be on a non-exclusive basis. All partner(s) shall be required to demonstrate commitment to the project by entering into a formal agreement with C-DOT as per the CCRP policy.

7	**Expected Deliverables**	**System Architecture Document & Design**: Overview of the solution's architecture, components, interfaces, and interactions with other network elements. **Functional Requirements Specification**: Detailed specifications of system functionalities, working and tuning **Solution Source code**: Implementation of server and client interfaces and steps to scale the system, along with the entire working source code of the solution. **Security Protocols Report**: Overview of implemented security measures and compliance. **Testing Reports**: Results from functional, performance, and security testing. **User Manual and Training Materials**: Guides for users and administrators on system usage. **Deployment Plan**: Strategy for deploying the solution and setup procedures. **Maintenance and Support Plan**: Guidelines for ongoing maintenance and support.
8	**Ownership of Background & Foreground IP**	All technologies created during the project shall be owned by the C-DOT. Any agreement required for collective ownership shall be subsequently settled directly with the concerned partners, but the ownership/IPR of the final solution shall rest with C-DOT only with all the deliverables including complete source code etc.
9 10	**Timeline for Project** **Eligibility Criteria of Partner(s)**	3 Months from date of approval Desirable Vendor Requirements for ensuring expertise in Secure and Custom AOSP Development: 1. Proven Android Security Expertise Requirement: The vendor must have formally reported at least 200 security vulnerabilities in the Android OS within the past 5 years. The reports should be supported by references from public acknowledgment sources such as Google's Android Security Bulletin, Google Security Blogs, or other verifiable channels. 2. Top Industry Recognition and VRP Rankings Requirement: The vendor must be associated with or acknowledged by leading mobile OEMs or companies in the Android OS domain, such as Google. 3. Experience in Secure AOSP Builds Requirement: The vendor must have a proven track record of developing security solutions, including at least one custom AOSP-based OS project completed within the past three years.

		4. Security Red Teaming Expertise Requirement: The vendor must have conducted red team assessments for at least five Android-based applications or SDKs within the past three years. 5. Proprietary Security Products Requirement: The vendor must have a strong portfolio of proprietary security solutions, with proven capabilities in designing and implementing secure systems for mobile platforms.