Appx C
(Ref para 11 of DDG IT letter No B/04001/Policy/Sw/DDG IT (T&P) Dt as in Digital Sign)

CHECKLIST FOR SECURE SYNC VIDEO CONFERENCING SOFTWARE

S No	Mandatory Details	Remarks
1.	Name of proj.	Secure Sync Video Conferencing Software.
2.	Name of Sponsor.	Nil.
3.	Type of Sw.	Customized.
4.	Brief justification/ endorsement on reqmt for devp of Sw appl.	(a) The current video conferencing setup is done by a third-party application and purchase of licenses. The same can be vulnerable to security breaches and attacks, risking the confidentiality of sensitive discussions and data. (b) A need was felt to design an indigenous video conferencing software for the same which can be tailored to specific military needs, ensuring the confidentiality and seamless communication and to reduce the dependence on foreign technologies, enhancing strategic autonomy, and the expenditure on the third-party VC software.
5.	Aim, Scope and Purpose incl utility, beneficiaries and tgt users.	(a) The current video conferencing system relies on third-party applications and licensed software, which introduces potential security vulnerabilities. These external platforms pose risks to the confidentiality of sensitive discussions and critical data, leaving them susceptible to breaches and cyberattacks. Recognizing these challenges, there is an urgent need to develop an indigenous video conferencing solution tailored specifically to military requirements. Such a platform would prioritize robust security protocols, ensuring seamless and secure communication across various operational levels while safeguarding classified information. (b) In addition to addressing security concerns, a domestically developed system would reduce dependency on foreign technologies, thereby enhancing strategic autonomy. This shift aligns with broader national security objectives, as it mitigates risks associated with external control or influence over critical communication systems. Furthermore, the implementation of an in-house solution would lead to substantial cost savings by eliminating

S No	Mandatory Details	Remarks
		recurring expenses tied to third-party licensing and maintenance fees. (c) Overall, the creation of a customized video conferencing platform would not only strengthen operational security but also foster self-reliance in technological capabilities. By addressing both security and financial challenges, this initiative represents a critical step toward achieving a more secure, cost-efficient, and strategically independent communication infrastructure for military operations.
6.	To be hosted on internet/ ADN with brief justification.	(a) Secure Sync is a cutting-edge real-time audio and video communication system designed to operate over a Local Area Network (LAN), ensuring high-speed, secure connectivity without requiring internet access. (b) By leveraging advanced technology, it minimizes latency while optimizing video quality and data security, providing a seamless and reliable communication experience. The secure Sync software is encrypted, built in India and easy to use. The entire communication between participants will be end to end encrypted with server hosted in defence premises. (c) With a focus on safeguarding data integrity and confidentiality, Secure Sync offers a secure, efficient, and dependable solution for real-time collaboration, reinforcing operational resilience and independence from external networks.
7.	Being devp in house or through IT funds.	In-house devp
8.	Hw and IT infrastructure reqd in the form of Virtual Machines at Data centre.	01 x Ubuntu machine for server
9.	Usability of proposed appls by other arms/ services/ org/ est.	(a) Use of software for audio and video conferencing at any level. The use of video conferencing software in other arms/ services/ org has become an integral part of modern defence operations, enabling secure, real-time communication across geographically dispersed units. This technology supports a wide

S No	Mandatory Details	Remarks
		range of applications, including strategic planning, operational coordination, intelligence sharing, and training programs. (b) By providing high-definition video and audio capabilities, it facilitates seamless interaction among personnel, regardless of location, enhancing decision-making and situational awareness in critical scenarios. (c) This video conferencing software empowers the armed forces with secure, efficient, and flexible communication tools, strengthening coordination, streamlining operations, and enhancing the overall readiness and effectiveness of military missions.
10.	Brief details of content of proposed Sw appl.	The external connections can be categorized into two main groups. Firstly, the connections between clients that request a video or audio connection are performed through remote requests and data streams. The second category of external connections is those to external services that help store recordings, stream recordings, stream videos, or help with creating meetings. The salient features of the software includes : (a) Custom algorithm. (b) End to end encryption. (c) Screen sharing, Chats, Polls, File transfer. (d) Audio sharing and screen recording. (e) White board and presentations. (f) Password protected rooms with LAN configuration. (g) Compatibility with windows OS, Linux, Mac OS, BOSS OS. (h) Bandwidth toggle mode.
11.	Endorsement by Head of Br/ Svc/ Fmn.	NA

S No	Mandatory Details	Remarks
12.	Details of user base.	(a) The Secure Sync server architecture is designed for deployment at each formation headquarters, with client distribution tailored to operational requirements. Each formation headquarters will host a dedicated server, ensuring localized control and enhanced communication efficiency. The number of clients supported per formation is aligned with the authorized strength of Active Directory (ADN) users within the formation. (b) The application is optimized to accommodate up to 100 concurrent clients per meeting, providing scalable functionality for diverse operational scenarios. The individual initiating the meeting is automatically granted moderator privileges, enabling them to manage participant interactions and maintain meeting order effectively. This architecture ensures robust, secure, and seamless communication within formations while adhering to established user management protocols. It is designed to support mission-critical operations, with scalability and administrative control embedded as core features to meet the strategic and operational needs of the organization. **<u>Role of the Users</u>.** (a) In the **Secure Sync** system, the individual initiating a meeting will automatically hold moderator rights for standard meetings. Participants can join these meetings through any browser using the designated meeting URL. During breakout sessions, all participants are granted moderator rights, enabling collaborative control and functionality within these smaller groups. For password-protected or encrypted meetings, moderator privileges remain exclusively with the initiator, ensuring centralized control over the session. (b) Participants in both standard and secure meetings have access to a suite of features, including bandwidth adjustment, screen sharing, audio recording, presentation tools, and virtual whiteboards. This ensures operational flexibility and enhances collaboration during sessions.

S No	Mandatory Details	Remarks
		(c) The moderator is granted additional privileges to manage the meeting environment effectively. These include the ability to mute reaction sounds, initiate hidden mode, mute all participants, or configure the session such that all attendees or the recording system follow the moderator's actions. These controls are designed to maintain order and ensure focus during high-priority discussions, particularly in operational contexts requiring strict communication protocols. This design provides a secure, efficient, and flexible communication platform that aligns with military standards for collaboration and information sharing. By offering granular control for moderators and robust functionality for participants, Secure Sync supports mission-critical communications while ensuring security, operational efficiency, and ease of use across diverse operational scenarios.
13.	Envisaged cost of entire proj incl license fees and maint.	NIL.
14.	Projected dt of completion incl maj timelines.	Project is prepared and ready for implementation.
15.	Brief details of Sw platform and tech stack proposed for devp of appl incl op sys dependencies (if any).	WebRTC compatible JavaScript application is used and code was built upon React and React Native. XMPP server used for signalling. The application makes use of React Redux as well, this is used as a general state store to keep track of important parameters that are used throughout the application. Server is hosted on Ubuntu and Clients can be hosted in any machine and operating system with Google chrome or Mozilla Firefox.
16.	Brief details of proposed network and bandwidth requirements.	The main design pattern employed in the architecture of Secure Sync is the *bridge pattern*, which modularizes each component to enable isolated modifications without affecting the rest of the application. A prime example of this is the I frame API, which is developed independently of the main application. Any updates to the API can be implemented solely within its scope, without requiring changes to the surrounding codebase. For instance, if a new version of the API is required, it can be developed alongside the existing one and swapped out by simply updating the import references. This modular approach minimizes disruption and reduces development

S No	Mandatory Details	Remarks
		complexity when changes or upgrades are necessary. The bridge pattern not only simplifies modifications but also provides developers with a clear understanding of the system's structure and the location of specific code. This method prevents the codebase from becoming a monolithic block, instead fostering a clean and scalable architecture. Such a design paradigm aligns well with the objectives of Secure Sync, ensuring that its components remain intuitive, adaptable, and easy to maintain over time. WebRTC compatible JavaScript application that uses Video bridge to provide high-quality, scalable video conferences. Build upon React and React Native. The external connections can be categorized into two main groups. Firstly, the connections between clients that request a video or audio connection are performed through remote requests and data streams. The second category of external connections is those to external services that help store recordings, stream recordings, stream videos, or help with creating meetings.
17.	Brief details of OS and Sys software reqmts.	Server to be hosted on Ubuntu and Clients can be hosted in any machine and operating system with browser limitation of Google chrome or Mozilla Firefox.
18.	Brief details of proposed data security measures incl backup of data.	(a) The secure Sync software is encrypted, built in India and easy to use. The entire communication between participants will be end to end encrypted with server hosted in defence premises. It uses 256-bit encryption alongwith second layer of custom encryption which includes xor and a random number algorithm. (b) With a focus on safeguarding data integrity and confidentiality, Secure Sync offers a secure, efficient, and dependable solution for real-time collaboration, reinforcing operational resilience and independence from external networks.
19.	Brief details of Proposed database Engine to be used in the appl.	NIL.
20.	Detls of Sw architecture and COTS Sw proposed to be utilised.	ADN PCs, Ubuntu based server machine.
21.	Detls of proposed architecture – Centralised/ Federated/ Hybrid.	Centralised – PAN Indian Army

S No	Mandatory Details	Remarks
22.	Brief details of proposed utilisation of Public Key Infra (PKI) and Iden and Access Mgt (IAM).	NIL.
23.	Technology dependencies (if any).	(a) Ubuntu based server. (b) Browser based clients.
24.	Database reqmts.	NIL.
25.	Enhancement/ Upgradation (incl Patch mgt/ Sw updt procedure and mechanism).	The identification of vulnerabilities and loopholes in the system should be managed centrally to maintain a unified and efficient security framework. A centralized approach ensures that potential risks across the ADN are consistently detected, analysed, and addressed. By consolidating this process, organizations can streamline the management of vulnerabilities, reduce redundancies, and establish a coordinated response to security threats. Once vulnerabilities are identified, timely patch updates should be developed and implemented across the ADN to mitigate risks and fortify system defences. Centralized patch management allows for efficient deployment, ensuring that all nodes in the network are updated simultaneously to maintain uniform security standards. This reduces the risk of exploitation due to delayed or inconsistent updates. In addition to patching, proactive monitoring and regular vulnerability assessments are critical to adapting to evolving threats. A centralized system also facilitates better tracking, reporting, and accountability for security measures, ensuring that the network remains resilient against potential breaches.
26.	Details of licensing (if any).	NIL.