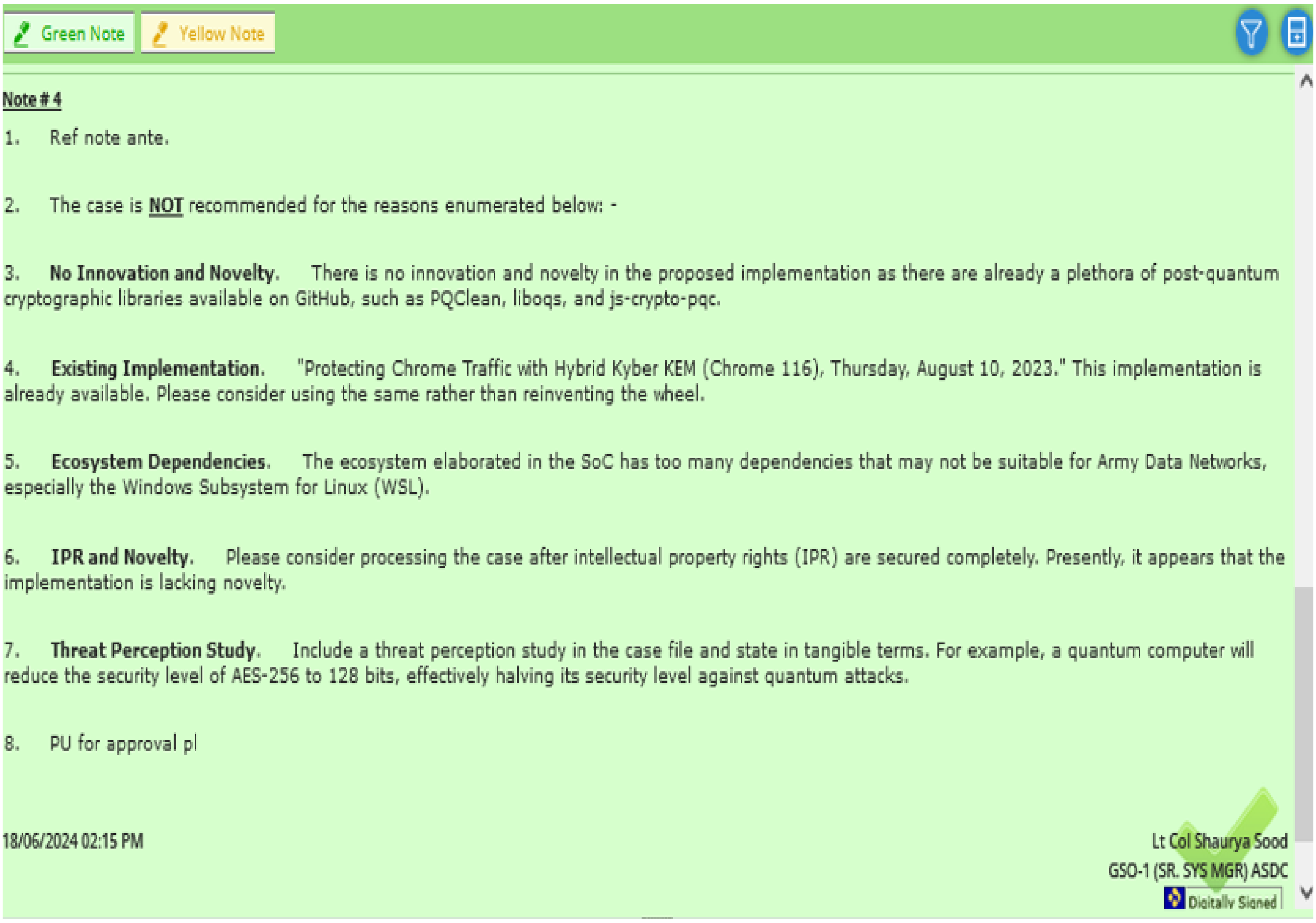

Note # 4

1. Ref note ante.

2. The case is **NOT** recommended for the reasons enumerated below: -

3. **No Innovation and Novelty.** There is no innovation and novelty in the proposed implementation as there are already a plethora of post-quantum cryptographic libraries available on GitHub, such as PQClean, liboqs, and js-crypto-pqc.

4. **Existing Implementation.** "Protecting Chrome Traffic with Hybrid Kyber KEM (Chrome 116), Thursday, August 10, 2023." This implementation is already available. Please consider using the same rather than reinventing the wheel.

5. **Ecosystem Dependencies.** The ecosystem elaborated in the SoC has too many dependencies that may not be suitable for Army Data Networks, especially the Windows Subsystem for Linux (WSL).

6. **IPR and Novelty.** Please consider processing the case after intellectual property rights (IPR) are secured completely. Presently, it appears that the implementation is lacking novelty.

7. **Threat Perception Study.** Include a threat perception study in the case file and state in tangible terms. For example, a quantum computer will reduce the security level of AES-256 to 128 bits, effectively halving its security level against quantum attacks.

8. PU for approval pl

18/06/2024 02:15 PM

Lt Col Shaurya Sood
GSO-1 (SR. SYS MGR) ASDC
Digitally Signed