Proposal No. 09

(Proposal details for the R&D scheme of USOF)

Subject: Security & Encryption platform

Problem Statement / Challenge title	Development of Proprietary Post-Quantum-Cryptography (PQC) Algorithm based on Lattice-based cryptography
Challenge brief / definition	With the rapid advancement in quantum computers, classical key exchange algorithms shall no longer be safe as the mathematic hard problems on which these algorithms are based shall be quickly solved by these new types of computers. The strength of classical key exchange mechanisms gets reduced to zero in this new quantum computing paradigm. Although, standardization of PQC algorithms is already in process at NIST (USA) but there is a need to design & develop proprietary asymmetric algorithms (based on similar/same hard problems as of PQC algorithms) for high level of security.

Format of Response

Companies / organizations / institutions / individuals developing enabling technologies / modules / components / subsystems / products are required to respond in the format provided in Annexure-A, on the DOT website (link address provided- refer “format of response”)