Collaborative Development of File Sanitization Solution (FSS) Under CCRP

1	**Problem Statement**	Development of a commercial grade file sanitization solution which will detect and remove the malicious content that can be deployable in a standalone form or as an integrated form in the cloud environment.
2	**Technology Area**	TSEC
3	**Project Introduction**	Ransomware is growing to be the new threat to remote and online cloud infrastructure and systems. Current trends of cyber threats use a combined ransomware approach that both encrypts data and steals data at the same time. C-DOT is associated with multiple secure software projects which contains highly sensitive data. There is a requirement of securing the integrity of this data as well to prevent its compromise to unauthorized access. Viruses, Malwares generally embedded in files stored at file system as a part of meta data which can be added to: • information about the content, such as title, author, publication date, subject, publisher, description. • information about how the digital media's components relate to one another including types, versions, relationships, file format, and size. • information about the file's technical aspects such as technical information about decoding and rendering, preservation information for long-term archiving, and rights information like usage rights. Malicious content in software have embedded in a downloadable asset i.e., cybercriminals hide malicious code that can execute when someone opens the document. This means that any metadata where this code can hide is risky. File content sanitization mitigates malware threats by scanning files, identifying active content using signature based analysis and AI based behavioral analytics, and subsequently removing active code. Finally, the file is recreated without the potentially dangerous code. The system shall have mechanism to upgrade in order to continuously mitigate the cyber threats. The final outcome of the collaborative development project shall be commercially file sanitization solution which can be deployed standalone or in integrated form in cloud environment solution. The project outcomes shall be licensed back to interested participants or third parties, capable of product marketing and deployments for end users, directly or in association with system integrators. Through a process of rigorous technical evaluation, C-DOT shall select participants holding the most promise of delivering commercial grade outcomes as its development partners ("Partner") in the project. In order to achieve a rugged, field deployable solution, C-DOT would prefer to select multiple Partners for the same work item wherever feasible.
4	**Description**	File Sanitization Solution, to scan files and identify if the file contains malware, malicious links and malicious content embedded in it. File

		content should not be modified in the process of file scanning. The proposed solution shall have following features: a) The solution should support pdf, xls, xlsx, doc, docx, jpg, png etc. file formats. b) Solution should contain API interface as well as UI interface for scanning the files and integration with security architectures via REST API. c) Solution should support concurrent requests for file scanning. d) It shall support scanning of 50 concurrent requests of 10MB file size within 15 seconds. e) It should generate different types of the reports of files scanned like time taken to scan each file and types of malicious content discovered, graph representation etc." f) The solution will have multi-scanning capability using signatures, heuristics, and machine learning technology for the highest and earliest detection of known threats. Accuracy: The solution shall have accuracy at least 99% for detecting the malicious content in files and subsequently sanitizing them. It shall have the capability of detecting and mitigating the zero-day attacks. Keeping in mind the technologies available with the industry, C-DOT shall prepare common product requirement specifications (PRS) in consultation with the partners. C-DOT and the project Partners will work collectively in physically realizing the PRS in form of Field deployable commercial product(s).
5	**Roles & Responsibilities of C-DOT**	C-DOT shall lead the integration of the final solution. It will provide technical development assistance, infrastructure and financial support to the project partners selected through a process of evaluation and due diligence conducted by a committee of subject experts. Where ever deemed necessary, C-DOT may arrange equipment resources, testing infrastructure, mandatory clearances, statutory permissions, technical consultancy and provide gap funding to the partners in realizing their respective target deliverables. C-DOT shall license the final solution for mass production and deployment. Royalty proceeds received from licensing shall be distributed amongst all Partners in ratio of the assessed value of each partner's respective contribution determined through mutual discussions while finalizing the product architecture. C-DOT shall engage with Partners on a non-exclusive basis and shall retain its right to develop similar products / through other developmental programs.
6	**Roles & Responsibilities of Participants**	The Partners may build the required solution afresh or by modifying pre-existing background technologies available with them. All concerned Partners shall own the foreground technologies developed by them individually or collectively as the case may be. The Partners may utilize the available test and infrastructure facilities

		offered by C-DOT with no financial implication for its usage. Participation in the project shall be on non-exclusive basis. All partners 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**	Commercial grade file sanitization solution which will be deployable in a standalone form or as an integrated form in the cloud environment and the solution shall be delivered with all the features as described in Section 4 of this document.
8	**Ownership of Background & Foreground IP**	Background technologies used in the project shall continue to remain with their respective owners. New foreground technologies created during the project shall be owned by the respective development partners, individually or collectively as the case may be. Any agreement required for collective ownership shall be settled directly by the concerned partners. The ownership of the final solution shall rest collectively with C-DOT and all its Partners.

Technology Areas (XXXX)

5G6G	5G/6G Technologies
IOTM	IoT and M2M Solutions
AIML	Artificial Intelligence, and Cognitive Sciences
TSEC	Telecom Network and Cyber Security
SRAN	Radio,Wi-Fi, Satellite and Broadcast
OPTL	Optical Access & Transport technologies
NMGT	Network Management System and Framework
APPN	Advanced Telecom Applications
MSOC	SOC/Micro-system level Design
QKDC	Quantum Communication
TSPT	Transport Technologies(Routers, Switches, Aggregators)
OTHR	Other