TERMS OF REFERENCE FOR THE R&D PROJECT
LITD 17 "Information System Security and Privacy, Sectional Committee"

1. **Title of the Project**: Study for Management of Mobile Applications' Permissions

Duration of project: 3 Months

2. **Background:**

a) Bureau of Indian Standards (BIS) committee, LITD 17 "Information System Security and Privacy, Sectional Committee" is the committee for standardization in security and privacy aspects of Information systems.
b) According to a joint study by Associated Chambers of Commerce and Industry of India and PwC, the number of smartphone users in India were expected to rise by 84% to 859 million by 2022 from 468 million in 2017. Mobile phones have different mobile applications (app) being used for various purposes. These mobile applications seek various kinds of permissions and gather data. Data being collected may or may not be required by the app for performing actual intended function. This results in privacy concerns for users.
c) A detailed study is proposed to be carried out for mobile applications being developed and used for all operating systems (like Android and ioS systems). Outcome of study shall provide best practices, recommendations that should be followed by mobile applications developers and mobile phone manufacturers to address data privacy concerns related to mobile applications.
d) Based on the outcome of R&D project, an Indian standard would be formulated. This standard "Guidance for seeking mobile phone applications' permissions" would be useful to mobile application developers/mobile manufacturers to provide data privacy assurance to their customers.

3. **Scope**:

a) To carry out comprehensive study of permissions sought by mobile applications (for all mobile phone operating systems like Android and iOS);
b) To analyze practices, standards, guidelines being followed by mobile applications developers while developing mobile applications as well as by mobile phone manufacturers;
c) To analyze best practices, guidelines, documents being used and referred by being used by app stores (like google play store, ioS store, mSeva app store) related to privacy concerns of mobile applications;
d) To analyze standards developed, referred by other countries related to mobile applications' permissions;
e) To provide recommendations to be followed by mobile applications developers and mobile phone manufacturers to address data privacy concerns related to mobile

applications. Following are some of the examples of expected recommendations, best practices:

i) some of the mobile applications mention whether the permission being sought is mandatory or optional. Based on this finding there could be a recommendation that all mobile applications shall mention whether the permission is mandatory or optional.

ii) some phones have a functionality called permissions manager which provides various options like it automatically removes the permission for apps which have not been used for a certain period of time. This could also be a recommendation.

iii) recommendations related to the common language of text (for seeking permissions) for similar types of permissions and functionality of application.

4. Deliverables:

a) Study report covering all the aspects mentioned in the scope, including following:
   i. Compilation, comparative analysis and summary of all points;
   ii. Response to questionnaires of discussions;
   iii. Specific recommendations to be followed by mobile applications developers and mobile phone manufacturers to address the data privacy concerns associated with mobile applications.

5. Research Methodology:

a) Literature survey:
   i. research papers, existing studies carried out in this area.
   ii. standards developed, referred by other countries related to mobile applications' permissions
b) Discussions with ten (10) mobile applications developers, ten (10) mobile phone manufacturers and collect feedback, information through structured questionnaires.
c) Focus group discussions with users of mobile applications and collect feedback, information through structured questionnaires.
d) Analysis of mobile applications and permission sought by them:
   i. Categorize mobile applications into various categories based on their primary function (like financial services, gaming etc.). Common categories used by Google play store and iOS app store may be used as reference.
   ii. At least a total of 100 mobile applications and 10-20 mobile applications for each category should be analysed.
   iii. To identify and record the purpose/reason provided by mobile application for seeking a specific permission.
   iv. To identify and record the common permissions sought by each category of mobile applications.
   v. To identify and record the commonalities & variety of purposes for each category of mobile application against each type of permission.

vi. Recommendations based on study, including language for reason/justification for seeking permission etc.

6. Requirement for the CVs:

The individuals, organizations engaged in this project should have working knowledge, experience related to operating systems and mobile applications, specifically in security and privacy domain.

7. Timeline and Method of Progress Review:

Timeline starts from the day of award of R&D project.

Project initiation (Month 1): The project officially begins with a detailed review of mobile applications, initiation of analysis of mobile phone applications and study of research papers, existing studies, standards.

Data Collection and Mid Term review (Month 2): Discussion with mobile phone manufacturers, mobile application developers and users. Draft report is submitted for mid-term review to assess progress and adjust methodologies as necessary.

Report Submission (Month 3): Final project report is submitted.

8. Support BIS will Provide:

Guidance and access to existing Indian and ISO/IEC standards relevant to data privacy. Additionally, BIS may facilitate exchange with mobile phone manufacturers.

Contact Details:
Sh. Kshitij Bathla, Sc-C, LITD (litd17@bis.gov.in)