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

1. Title of the Project: Study of criteria for symmetric-key ciphers for possible inclusion in IS/ISO/IEC 18033 series

Duration of project: 6 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) Cryptographic algorithms aim at securing data in storage or transit by broadly providing for the following.

i. Confidentiality
ii. Integrity
iii. Authenticity

Cryptographic algorithms are employed in the various products and services, such as:

i. Digital banking
ii. Mobile applications
iii. Online shopping
iv. Electronic mail
v. Online social networks
vi. Digital signature tokens
vii. Digital television
viii. Smart cards
ix. Radio frequency identification (RFID) tags
x. Wireless sensor nodes

Symmetric-key ciphers and cryptographic hash functions (which are often built around symmetric-key ciphers) are important classes of cryptographic algorithms used in civilian and military applications. Major civilian sectors using these algorithms include the following:

i. Finance / banking
ii. Telecommunications
iii. E-commerce
iv. Automotives
v. E-governance

Since the late 1990s, several standardization bodies / Governments have successfully implemented open initiatives aimed at standardisation or recommendation of symmetric-key cryptographic algorithms for widespread adoption. These initiatives specify stringent criteria for the algorithms for possible adoption or continuation as standards. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) also specifies similar criteria for symmetric-key ciphers in Annexures A & B of ISO/IEC 18033-1. ISO/IEC 18033-1 has been adopted as Indian standard IS/ISO/IEC 18033-1.

The proposed project seeks to lay down the basic criteria for symmetric-key ciphers (stream ciphers and block ciphers) to be considered for possible inclusion in, as well as removal from IS/ISO/IEC 18033-1.

3. Objective:

a) Examination of existing criteria for adoption / deletion of symmetric-key cryptographic algorithms as / from standards.

b) To lay down the basic criteria for symmetric-key ciphers (stream ciphers and block ciphers) to be considered for possible inclusion in, as well as removal from IS/ISO/IEC 18033-1.

4. Scope:

a) To review the criteria for adoption / deletion of symmetric-key cryptographic algorithms as / from standards. At present there is one such set of criteria in IS/ISO/IEC 18033-1. To particularly find out and analyse this and other such criteria.

b) To suggest any changes that may be required in the criteria of IS/ISO/IEC 18033-1, along with the rationale for such changes.

5. Expected Deliverables:

a) Study report covering all the aspects mentioned in the scope, including following:

i) detailed and specific recommendations for the changes in the criteria as specified in Annex A and B of IS/ISO/IEC 18033-1.

ii) List of all such other criteria and comparative analysis of all such initiatives/criteria.

6. Research Methodology:

a) Detailed study of the eligibility criteria for encryption systems under IS/ISO/IEC 18033-1, and other such initiatives/criteria.

b) Identifying lacunae in the criteria and suggesting any changes that may be required along with the rationale for the changes.

7. Requirement for the CVs:

The individuals, organizations engaged in this project should have knowledge and experience in the analysis of symmetric-key ciphers.

8. Timeline and Method of Progress Review:

Project initiation (Month 1): Detailed study of IS/ISO/IEC 18033-1 and identification of other initiatives/criteria for adoption / deletion of symmetric-key cryptographic algorithms as / from standards.

Data Collection (Months 2-3): Detailed study of international standardization initiatives in the area of symmetric-key cryptography.

Mid Term review (Month 4): Draft report is submitted for mid-term review to assess progress and adjust methodologies as necessary.

Report Submission (Months 5-6): Collecting and processing expert review comments on the draft report and submission of the final project report.

8. Support BIS will Provide:

BIS will offer guidance and access to relevant existing Indian and ISO/IEC standards.

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