CISO Council team appreciates the invitation extended by OTA to review the public draft of IoT Trust Framework. The global adoption of IoT devices and staggering number of devices that are expected to get connected to the internet will demand the need for such a framework. The work on this initiative can be a starting point for creating a recognized IoT Trust Framework.

The overall areas identified and addressed in the frameworks clearly demonstrates the effort and knowledge of the working committee. After a careful review of the draft framework document. We have identified a few areas of improvements for consideration;

5. The term and duration of the data retention policy must be disclosed.

It is an ideal solution to delete all user data upon termination or expiration. However, considering the growing requirement of big data analytics providing more insight into various improvements or a greater good keep customer informed of any such analytics or research will also be a key component.

7. Personally identifiable data must be encrypted or hashed at rest (storage) and in motion using best practices including connectivity to mobile devices, applications and the cloud utilizing Wi-Fi, Bluetooth and other communication methods.

Including some baselines and minimum standards for encryption would add more value

17. For products and services which are designed to be used by multiple family members and collect PII, manufacturers need to incorporate the capability for creating individual profiles and/or have parental or administrative level controls and passwords.

In this case, profile specific data collection should be mandatory and users should have the option to deal with data deletion or other requests upon termination or expiration for a particular profile rather than the account product / complete service.

Additional Area:

As IoT would form part of many government and semi government entities that would consider using cloud service providers. It would be important that the IOT vendors with cloud proposition declare the countries of data centers or other infrastructure where the data resides. As some of the countries demand that the data generated does not reside beyond authorized jurisdiction or cross borders. Eg. Some of the gulf countries have laws related to this.

We thank for your work on the same and would be glad to discuss the recommendations and further participate in the successful development of the final IoT trust framework. Should you have any questions or require any further information. Please contact Ahmed Baig at +971504574361 or ahmed.baig@cisocouncil.com