This submission refers to items b,e,f and h of the 2016 Census Inquiry terms of reference.

It is my observation that, while the mishandling of capacity planning and incident response reflect badly on the ABS, the far more serious matter is the vast overreach implicit in the changes to data retention and linking that have been adopted.

Longitudinal and inter-database linking of personal data effectively enrols every
resident of Australia into a longitudinal anthropological study, against their will and with no recourse for those who do not wish to participate. I believe that census participants must be offered a choice to withhold identification either in perpetuity or (as previously) for a significant number of years. While a significant body of academic knowledge in the field of anthropology and related fields rests on a few large scale longitudinal studies conducted around the world, one of the reasons such studies are few is that most people are not comfortable disclosing such significant personal information. I think it is well understood that the risk of malicious use of data increases as more people have access to the data. Risks that may be acceptable in an academic study conducted on a small scale become much more severe at nation scale. The deliberate positioning of the ABS census database as a commercial resource for marketing violates the trust of the Australian people.

The notion that names and addresses will be replaced by a de-identified linking-key is not a mitigating factor. Experiments show that re-identification is quite feasible, and the linking key algorithms that have been made public are flawed. The use of a non-cryptographic linking key means that a targeted attack - retrieving the information of one or more known individuals - is not prevented. As a professional who has worked in the area of data security for many years, I believe it is essential that de-identification and key generation procedures be published and subject to rigorous public and academic scrutiny. It is a generally accepted principle in the fields of cryptography and data security that peer review of algorithms is essential, as over time most proprietary schemes invented by non-experts have proven flawed. The cost to individuals should their personal data be leaked or hacked at any time in the future is incalculable, and demands the best possible protection.

It may very well be that scrutiny will show that there is no safe de-identification process, and that the only safe thing to do is abandon the attempt to link census records to other databases and to future censuses. The burden of proof should be on the ABS to show that risks have been identified and mitigated, and the mitigation has been independently reviewed. The ABS has lost the entirely of the great store of trust that it had accumulated from the Australian public, and internal review alone is simply not acceptable.

In regard to item h of the terms of reference I observe
that continuing real decline in funding of the ABS has perhaps been

a factor in the decision by the ABS to re-invent the census as a commercially lucrative marketing data corpus during a period of reduced oversight. This inquiry should establish firm boundaries for the use (if any) of Census data for commercial purposes.