**Division/Agency:** Australian Bureau of Statistics
**Question No:** 42
**Topic:** 2016 Census – security of data
**Reference:** Written
**Senator:** Ketter, Chris

**Question:**

1) Can the ABS provide details on what legal arrangements have been entered into between the ABS and IBM/Softlayer to ensure the security of the Census data of Australians?
2) Can ABS confirm whether Census-related data of Australians may be sent outside of Australia and/or may otherwise be processed offshore?
3) Is IBM/Softlayer collecting any data relating to Australians who complete the Census online, including (but not limited to) the Internet Protocol (IP) addresses of Australians completing the Census online?
4) Given IBM/Softlayer is a U.S. corporation subject to U.S. law, is there any possibility that Census-related data processed or stored by IBM or Softlayer may be lawfully accessed by U.S. government agencies, such as the National Security Agency, under relevant provisions of U.S. law, such as the USA PATRIOT Act?
5) Has the javascript code used by IBM/Softlayer in its role in processing Census-related data been independently verified by Australian authorities in order to ensure that it complies with international best practice cybersecurity? If it has, who was responsible for verifying the code?"

**Answer:**

1) The Australian Bureau of Statistics (ABS) entered into a formal contract with IBM for the provision of the eCensus solution which included detailed security arrangements for encryption and data location. The contract included formal confidentiality clauses with IBM and with individual staff. Respondent data was encrypted at all times until it was received by the ABS. The ABS held the encryption keys; IBM did not have access to the keys. All respondent data was held on dedicated equipment (non-cloud) in a highly secure and closely managed environment. Softlayer was only used for delivery of static content such as help pages and images.

2) The ABS requires, and the contract states, that all respondent data be managed and stored within Australia only. No respondent data was stored or managed off-shore. Data processing is managed wholly by the ABS within the ABS dedicated, local data centre following receipt of encrypted data from IBM.

3) All respondent data is fully encrypted and IBM has no access to that data. As a component of security protocols, it is standard practice to collect Internet Protocol (IP) addresses during the operation. The ABS also required IBM to collect operational information such as the types of browsers and devices utilised to complete the online Census. All such data is utilised for the purposes of the Census only and decommissioning of the IBM hosted site includes deletion of all such data from the IBM environment.

4) No. All data is held within Australia and remains encrypted until delivery to, and subsequent decryption by the ABS. The ABS supervises the decommissioning (including scrubbing of disks) of the IBM equipment at the conclusion of the operational period. All accesses to the ABS Census environment hosted at IBM are logged for audit purposes.

5) The system has been subjected to significant security assessments and testing. This includes verification of the physical security arrangements at the IBM data centre, verification of encryption algorithms by Australian Signals Directorate (ASD), code review and penetration testing by an independent Australian security company, by IBM and by ABS Information Technology (IT) security experts.