Ms Margot Kerley
The Committee Secretary
Joint Committee of Public Accounts and Audit
Parliament House
CANBERRA ACT 2600

Dear Ms Kerley

INQUIRY INTO THE MANAGEMENT AND INTEGRITY OF ELECTRONIC INFORMATION IN THE COMMONWEALTH

Please find attached the Australian Bureau of Statistics (ABS) submission to the Joint Committee of Public Accounts and Audit inquiry into the management and integrity of electronic information in the Commonwealth.

An electronic version of this document will be sent to your office for placement on the Committee's website.

If you have any further questions regarding this submission please contact Ms Marion McEwin, Assistant Statistician, Policy Secretariat Branch on (02) 6252 5533 or email marion.mcewin@abs.gov.au.

Thank you for providing the ABS with the opportunity to comment on this inquiry.

Yours sincerely

Dennis Trewin

December 2002

Submission to the JCPAA Inquiry into Management and Integrity of Electronic Information in the Commonwealth

The preservation and protection of the confidentiality of information entrusted to the ABS by its respondents are matters of fundamental importance to the ABS and are central to the continued success of its operations. As the national statistical agency, the ABS collects information from businesses and individuals and disseminates the statistics it compiles from these sources. Although the ABS does have the power to direct businesses and individuals to provide data, ABS experience is that high quality statistics can only be achieved with the willing cooperation of the Australian community. Central to that cooperation is public confidence in the ABS's ability and commitment to maintain the confidentiality of the information that is provided.

2. Furthermore, the ABS does use administrative data for statistical purposes (eg customs, births and deaths). This data is accorded exactly the same protection as data collected directly collected from businesses and individuals.

3. The ABS has an enviable reputation for the preservation of the confidentiality of reported data, and for the protection of its statistical data holdings from unauthorised release or illegal access. Set out below are the various elements which help the ABS to achieve this:

Census and Statistics Act 1905

4. The fundamental concern for the protection of the confidentiality of information provided by respondents is reflected in the secrecy provision of the *Census and Statistics Act 1905* (CSA) which prohibits the disclosure of information collected under the Act, whether collected directly or from administrative sources, other than by the confidential means the Act allows.

5. The secrecy provisions of the CSA are reinforced by Section 7 of that Act which requires all ABS officers to sign an undertaking of fidelity and secrecy before they can commence duties. Apart from being a requirement under the Act, the purpose of the undertaking is to ensure that every officer is aware of the secrecy provisions imposed on them by the CSA before they obtain access to information and also to provide documentary evidence that these obligations have been brought to their attention.

6. The CSA provides an indictable offence punishable on conviction by a fine not exceeding $5,000 or imprisonment for a period not exceeding 2 years, or both, for a breach of the Secrecy provision.

The physical security of ABS data holdings

7. The facilities and procedures in place to protect the security of ABS data are too comprehensive to attempt to detail here, and for obvious reasons we would not wish to do so even if it were possible. However, in simple terms, access to all ABS offices is strictly controlled by a combination of security pass identification, electronic surveillance and electronic identification.

8. The ABS Firewall infrastructure, which provides secure connections to the internet, has been continuously Defence Signals Directorate (DSD) certified since 1996. The ABS was the first agency to acquire certification. The ABS considers the certification process a valuable and useful discipline and appreciates the advice and assistance received from DSD.

9. The ABS's computer systems are secured. Access by ABS officers to the ABS network is well controlled with access to applications and databases provided on a "need to use" basis. Access to confidential data collected under the provisions of the CSA is strictly limited to specific ABS staff on a "need to know" basis. Access controls are enforced by a variety of means including passwords, one time passwords, certificates, program path control and encryption. Systems access is logged and monitored and staff are held accountable for appropriate use. The IT Security Section is staffed by competent and professional staff who are dedicated to maintaining and improving the security of the ABS IT environment.

ABS policies and practices

10. The ABS Corporate Plan identifies the protection of data provided to the ABS as a "key principle" and essential to ensure the trust of respondents to its surveys. The Corporate Plan states that "*every ABS officer is required by law to give an undertaking of fidelity and secrecy, and the ABS maintains a highly secure physical and computing environment. We make sure that in publishing data, identifiable information is not released.*".

11. Procedures and policies within the ABS are designed to ensure that access to information is strictly restricted to officers on a "need to know" basis. The ABS Policy and Legislation Manual includes policy on IT security (refer Attachment A). The policy requires managed change to the IT environment and compliance with Security standards.

ABS culture

12. The ABS culture is one which strongly values information security. This culture is supported through the undertaking which all staff sign on joining, appropriate training, work practices which place an emphasis on information security, and an IT environment and systems which support good security and management of information.

13. Additionally, all ABS officers are subject to the APS Code of Conduct which requires that APS employees must not make improper use of information they obtain in undertaking their duties, and the Commonwealth *Crimes Act 1914* which provides criminal penalties for the improper disclosure of confidential information.

Internal and external scrutiny

14. The ABS was one of 10 agencies which participated in the ANAO "Audit of Internet Security within Commonwealth Government Agencies". The ANAO found that "security levels across the audited agencies varied significantly from very good to very poor". The ABS was advised at the exit interview that it was regarded as "very good". The "ANAO Issues Paper" made 7 recommendations and all of these have been implemented by the ABS.

15. The ABS internal audit program includes regular audits of IT and Physical Security.

16. The Protective Security Management Committee, chaired by a Deputy Australian Statistician, meets regularly to review IT security plans and issues.

Conclusion

17. The ABS has every confidence that the stringent secrecy provisions provided under the CSA, combined with a corporate culture which is strongly supportive of the protection of personal information, ensures, to the maximum extent possible, that the confidentiality of the information entrusted to the ABS is securely protected. The strong commitment of ABS staff to the protection of respondent confidentiality is evidenced by the ABS's history, which has never recorded a deliberate breach of the Secrecy provisions of the Act by an ABS officer. It is well known that ABS management would act immediately on any alleged breaches.

18. In essence, the security and integrity of electronic information is enabled by a combination of:

- supporting legislation;
- knowledge that this legislation will be enforced if necessary;
- a corporate culture which emphasises the importance of the secrecy of information provided to us by businesses and households;
- great care in ensuring that our IT environment remains secure even with changing threats; and
- a dedicated team of security specialists to monitor the situation and ensure our arrangements remain "state of the art".

Attachment A

ABS Information Technology Security Policy

1 It is ABS Policy that:

(a) The ABS Information Technology Environment (the 'IT Environment') is to support the ABS mission.

(b) Access to the various hardware and software components of the environment and to the various data stores residing within the environment is granted on a 'needed to do the job' basis, and staff must only be granted access to those components or data stores on that basis.

(c) The operation of the IT Environment will conform with Australian Government requirements covering IT security. Of particular importance is the Australian Government Protective Security Manual. Staff using or otherwise working within the IT Environment must comply with the rules, standards and procedures published in the Protective Security Manual and the Defence Signals Directorate publication, ASCI 33. Where possible and practicable the rules, standards and procedures are to be supported by system documentation and controls within the IT Environment.

(d) Changes may only be introduced into the IT Environment in accordance with appropriate procedures, authorisations and licence arrangements and only by staff authorised to introduce and install such changes.

(e) The ABS respects the copyright of software owners and aims to ensure that at all times it operates within licence or other legal requirements in all areas.

(f) The ABS claims copyright over all software products developed using the facilities of the IT Environment or by ABS staff in the course of their work except in specifically identified and agreed circumstances where different arrangements may apply.

(g) Each individual staff member must guard and protect the access authorities granted to him or her, and must exercise those authorities in a responsible fashion consistent with work requirements and ensure that those access authorities are not disclosed to or used by any other person. Additionally, individuals must take all reasonable precautions to guard against accidental misuse of particular authorities, must immediately relinquish any authorities that are no longer appropriate following a change in duties or in the environment, and must not obtain or use authorities outside those properly granted in relation to his or her duties.

(h) All use of the IT Environment must be in accord with ABS personnel policy guidelines and guidelines on the use of Commonwealth equipment, in particular those pertaining to the APS Values and the APS Code of Conduct specified in the Public Service Regulations, OHAS, Workplace Diversity and Privacy.

(i) ABS staff must not use the IT Environment for non work related purposes, other than for purposes which are acceptable according to the document headed "Guidelines for Acceptable Non Work Related Use of the ABS IT Environment"

(j) Privately owned equipment and storage media are not to be used to process and / or store information owned, collected or under the custody of the ABS unless that information has been published or disclosed in accordance with the provisions of the *Census and Statistics Act 1905*.

(k) External connections to the IT Environment may be established only with the approval of the First Assistant Statistician, Technology Services Division and must include stringent precautions to prevent unauthorised access to ABS data.

(l) Respondent data may only be communicated via the Internet by approved secure means. The approval process will include a risk assessment which is used by Security to determine the security model.

(m) The ABS will monitor the operation of its IT Environment at a level sufficient to protect the integrity of that Environment, to detect and identify breaches of the standards and guidelines, to manage performance and plan for and control changes, and to account and charge for use of all facilities provided.

(n) Generic IDs may only be introduced and used in the IT production Environment in accordance with appropriate procedures and authorisations as stated in the "Creation and use of Generic IDs" guidelines document.

(o) The Security Section is the authoritative source of advice on matters relating to the security of the IT Environment.