Submission No. 60

28 MAY 2003

NOIE

The National Office for the
INFORMATION ECONOMY

JOINT COMMITTEE OF
30 MAY 2003
PUBLIC ACCOUNTS & AUDIT

Mr Bob Charles MP
Chairman
Joint Committee of Public
Accounts and Audit
Parliament House
Canberra ACT 2600

Dear Mr Charles

PUBLIC KEY INFRASTRUCTURE (ADDITIONAL QUESTIONS)

I refer to your letter dated 29 April 2003 to which was attached a set of additional questions to those questions taken on notice by NOIE officials at the public hearings of your Committee's Inquiry into the Management and Integrity of Electronic Information in the Commonwealth on 1 April 2003.

The questions included:

1. Comment on Microsoft's Trustworthy Computing Environment.
2. What interactions does NOIE have with Government agencies?
3. Comment on how agencies, including NOIE, can prevent the accidental release of confidential information.
4. Comment on suitability of agencies' disaster recovery plans?
5. Comment on the issue of archival integrity.

Please find attached a series of papers prepared by this Agency.

NOIE officials are available to meet with your Committee to discuss any of the matters raised in the attached papers should you require.

Yours sincerely

Keith Besgrove
Chief General Manager
Regulatory & Analysis
26 May 2003

GPO Box 390, CANBERRA ACT 2601, AUSTRALIA
Telephone: (61 2) 6271 1777 Facsimile: (61 2) 6271 1659

www.noie.gov.au

Joint Committee of Public Accounts and Audit Inquiry into the Management and Integrity of Electronic Information Held by the Commonwealth

ADDITIONAL QUESTIONS:

[1]
Trust – The submission from Microsoft Australia mentions Microsoft's Trustworthy Computing Environment. This project aims to build public trust in computers in general, through cooperation between consortia, research communities, Governments and Industry. Do you regard this as a valid and achievable goal? Would you please comment on your reasons?

ANSWER:

The Trusted Computing Platform Alliance (TCPA), was formed by Compaq, HP, IBM, Intel and Microsoft in 1999. The initiative came as a result of these companies concluding that "the level, or 'amount', of trust they were able to deliver to their customers, and upon which a great deal of the information revolution depended, needed to be increased and security solutions for PC's needed to be easy to deploy, use and manage". An open alliance was formed to work on creating a new computing platform for the next century that will provide for improved trust in the PC platform. [1]

In the current security conscious environment NOIE welcomes such initiatives in the private sector that can be applied in both the private and public sectors. NOIE supports research and collaboration efforts undertaken by private sector companies to engender a level of public acceptance of their products which are marketed to meet a perceived need for additional functionality, such as increased security or trust.

NOIE considers that such products and/or applications should be developed to allow for interoperability with other systems and maintain the availability of future choice for customers. In the increasingly networked environment, NOIE would not support collaboration between suppliers that may lead to potential market restrictions in the future. Accordingly products need to be assessed on their individual merits, separate from vendor interests in promoting one form of product or technology. The value and suitability of such initiatives need to be assessed within the government framework for which they are being marketed.

At this stage external commentary on Microsoft's Trusted Computing Platform has been mixed. Concerns around this product include:

- the ability to protect the integrity of a PC through software alone is reaching its limitations;
- there are e-business security and privacy issues that software alone cannot address; and
- use of cryptographic keys in hardware requires escrow of the keys in case of hardware failure with the possible consequence that the escrow service becomes a security liability.

NOIE has not reviewed Microsoft's Trusted Computing Platform; nor does it have the technical expertise to enable it to do so. The technical expertise for carrying out such assessments resides in the Defence Signals Directorate (DSD).

As part of the Government's Gatekeeper Program, government agencies do not utilise any products that have not been endorsed by DSD.

[1] The TCPA website can be accessed at http://www.trustedcomputing.org/tcpaasp4/index.asp

Joint Committee of Public Accounts and Audit Inquiry into the Management and Integrity of Electronic Information Held by the Commonwealth

ADDITIONAL QUESTIONS:

[2]
Interactions with NOIE: several submissions from Government agencies have mentioned their interactions with NOIE. What are the main interactions that NOIE has with Government agencies?

ANSWER

One of NOIE's key roles is to coordinate the application of new technologies to government administration, information and service provision. This requires NOIE to engage with Government agencies across a range of areas. One of the key mechanisms, in this regard, is the Information Management Strategy Committee (IMSC), which was established in late 2002 as part of a new ICT governance and investment framework for Commonwealth agencies.

The IMSC comprises a small group of very senior officials (at Secretary/CEO level) and promotes more strategic approaches to ICT issues across agencies. It is chaired by the Secretary of the Department of Communications, Information Technology and the Arts and oversees the work of a Chief Information Committee (CIOC), which is chaired by the CEO of NOIE, and includes representatives from key ICT user agencies. The committees have identified priority issues for action, including security infrastructure, authentication, strategic sourcing and channel management, and initiated work programs to address these, through a number of working groups. NOIE is actively collaborating with other agencies in progressing both committees' priorities. It provides secretariat support to the committees, and also chairs, and provides secretariat support to, a number of working groups.

A second key role of NOIE's is to provide advice and information to Government and to other sectors of the economy which facilitates the adoption of new technologies and the diffusion of e-commerce. In this second role, NOIE has extensive information, research, policy and regulatory dealings with a very wide range of Commonwealth, state and local government agencies.

Joint Committee of Public Accounts and Audit Inquiry into the Management and Integrity of Electronic Information Held by the Commonwealth

[3]

A recurring theme of reported privacy breaches concerns the accidental release of confidential information. For example, cases where a government officer legitimately releases public information in the form of an electronic file or e-mail, which also contains confidential information that the officer is unaware of. The following cases illustrate the problem:

- The Office of the Federal Privacy Commissioner reported that in November 2001 the Child Support Agency sent an e-mail that accidentally contained 400 client e-mail addresses.
- An ANAO audit into the Health Group IT Outsourcing Tender Process at the Department of Finance and Administration investigated an incident in July 1999, where an Excel spreadsheet was released to IBM GSA containing information about its tender but which also contained information on other tenders.
- The Committee discovered that some of the submissions sent to this Inquiry contained draft versions that could be accessed with the word processing program's reviewing functionality.

How can agencies, including NOIE, prevent this sort of accidental release of confidential information?

ANSWER:

Agencies (including NOIE) are required to comply with the Information Privacy Principles (IPPs) in the Privacy Act. IPP 4 (a) is quoted below.

A record-keeper who has possession or control of a record of personal information shall ensure:

(a) that the record is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure and against other misuse;

In respect to its own records of personal information NOIE endeavours to comply with IPP 4 (a) and the other IPPs.

NOIE manages many extensive e-mailing lists and e-mail discussion groups. To manage these NOIE employs listserves. The advantage of listserves over informal e-mail distribution is that e-mails to the listserve are distributed to the mailing group without the mailing list of e-mail addresses being disclosed.

Joint Committee of Public Accounts and Audit Inquiry into the Management and Integrity of Electronic Information Held by the Commonwealth

ADDITIONAL QUESTIONS:

[4]

Disaster Recovery:
A potential threat to the integrity of the Commonwealth's electronic data is physical disruption caused by an earthquake or fire.

1. How suitable are agencies' disaster recovery plans?
2. How confident are you that data stored by NOIE would survive a disaster such as a fire?

ANSWER:

1. **Agencies' disaster recovery plans**
   An exercise was recently conducted on the Commonwealth's preparedness to effectively handle a disaster situation, which found that all 15 agencies surveyed had Business Continuity Plans in place. These plans are reviewed regularly, at least annually. Some agencies review them quarterly and conduct simulations to ensure effectiveness.

2. **Survival of NOIE data in a disaster**
   NOIE is a member of the Group 5 Agreement for IT&T Services and Industry Development. Telstra Enterprise Services (TES), through the Department of Communications, Information Technology and the Arts (DCITA), provide Group 5 IT&T services to NOIE.

   NOIE data is backed up and a separate copy maintained offsite by TES. This approach would be expected to ensure the survival of data in the event of disaster such as fire.

Joint Committee of Public Accounts and Audit Inquiry into the Management and Integrity of Electronic Information Held by the Commonwealth

ADDITIONAL QUESTIONS:

[5]

Archival Integrity:
Another potential threat is the gradual degradation of data over time.

- Is this issue being addressed by government agencies generally?
- What action is NOIE taking to ensure the long-term archival integrity of the Commonwealth data that it holds?

ANSWER:

NOIE has no information about the extent to which archival integrity of data is addressed by government agencies. NOIE suggests that the Committee ask this question directly of National Archives.

Telstra Enterprise Services (TES) hold backups of NOIE data dating back to the commencement of the Group 5 contract in April 1999.

During the period of the contract, no NOIE systems or data have been archived. Arrangements for any necessary archiving of existing NOIE material will be developed with TES prior to the termination of the current contract arrangements in July 2004. Under the terms of any new IT&T sourcing arrangement from that date, NOIE will make provision for the backup and archival of systems and data.

Where informal e-mail distribution is employed users should use the blind copy function of their e-mail application to prevent the disclosure of the e-mail addresses of others if it is required for these to be confidential. However, there are circumstances in informal e-mail discussions where it is appropriate for the members of the group to be aware of each other's e-mail address, as long as the individuals concerned consent to this.

NOIE, like other agencies, requires its staff to sign a confidentiality agreement on commencement.

In respect to other agencies, NOIE has no statutory regulatory role or powers. The Privacy Commissioner, however, is the regulator in this area and has statutory powers to investigate complaints and to issue Guidelines in respect to breaches of the IPPs.

Despite genuine efforts by agencies to comply with IPP4, it is inevitable that accidental disclosures will occur from time to time.

NOIE liaises regularly with staff of the Office of the Federal Privacy Commissioner (OFPC) and has worked in conjunction with the OFPC on many issues. These include the promulgation of the Privacy Commissioner's *Guidelines for ACT and Federal Government World Wide Websites* as a key enabler in the GovOnline strategy and the development of the *Privacy and Public Key Infrastructure: Guidelines for agencies using PKI to communicate or transact with individuals*. NOIE invited the Privacy Commissioner to develop these privacy guidelines and provided resources and advice.

If the Committee and the Privacy Commissioner consider that this is a systemic problem that requires treatment, NOIE would encourage the OFPC to use NOIE and its networks to examine the matter and to assist in the development of appropriate advice and guidance.

Information Privacy Principles

Principle 1 - Manner and purpose of collection of personal information

1. Personal information shall not be collected by a collector for inclusion in a record or in a generally available publication unless:

   (a) the information is collected for a purpose that is a lawful purpose directly related to a function or activity of the collector; and

   (b) the collection of the information is necessary for or directly related to that purpose.

2. Personal information shall not be collected by a collector by unlawful or unfair means.

Principle 2 - Solicitation of personal information from individual concerned

Where:

(a) a collector collects personal information for inclusion in a record or in a generally available publication; and

(b) the information is solicited by the collector from the individual concerned;

the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, before the information is collected or, if that is not practicable, as soon as practicable after the information is collected, the individual concerned is generally aware of:

(c) the purpose for which the information is being collected;

(d) if the collection of the information is authorised or required by or under law—the fact that the collection of the information is so authorised or required; and

(e) any person to whom, or any body or agency to which, it is the collector's usual practice to disclose personal information of the kind so collected, and (if known by the collector) any person to whom, or any body or agency to which, it is the usual practice of that first-mentioned person, body or agency to pass on that information.

Principle 3 - Solicitation of personal information generally

Where:

(a) a collector collects personal information for inclusion in a record or in a generally available publication; and

(b) the information is solicited by the collector;

the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is collected:

(c) the information collected is relevant to that purpose and is up to date and complete; and

(d) the collection of the information does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.

Principle 4 - Storage and security of personal information

A record-keeper who has possession or control of a record that contains personal information shall ensure:

(a) that the record is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse; and

(b) that if it is necessary for the record to be given to a person in connection with the provision of a service to the record-keeper, everything reasonably within the power of the record-keeper is done to prevent unauthorised use or disclosure of information contained in the record.

Principle 5 - Information relating to records kept by record-keeper

1. A record-keeper who has possession or control of records that contain personal information shall, subject to clause 2 of this Principle, take such steps as are, in the circumstances, reasonable to enable any person to ascertain:

   (a) whether the record-keeper has possession or control of any records that contain personal information; and

   (b) if the record-keeper has possession or control of a record that contains such information:

      (i) the nature of that information;

      (ii) the main purposes for which that information is used; and

      (iii) the steps that the person should take if the person wishes to obtain access to the record.

2. A record-keeper is not required under clause 1 of this Principle to give a person information if the record-keeper is required or authorised to refuse to give that information to the person under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.

3. A record-keeper shall maintain a record setting out:

   (a) the nature of the records of personal information kept by or on behalf of the record-keeper;

   (b) the purpose for which each type of record is kept;

   (c) the classes of individuals about whom records are kept;

   (d) the period for which each type of record is kept;

statement provided by that individual of the correction, deletion or addition sought.

Principle 8 - Record-keeper to check accuracy etc. of personal information before use

A record-keeper who has possession or control of a record that contains personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date and complete.

Principle 9 - Personal information to be used only for relevant purposes

A record-keeper who has possession or control of a record that contains personal information shall not use the information except for a purpose to which the information is relevant.

Principle 10 - Limits on use of personal information

1. A record-keeper who has possession or control of a record that contains personal information that was obtained for a particular purpose shall not use the information for any other purpose unless:

   (a) the individual concerned has consented to use of the information for that other purpose;

   (b) the record-keeper believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person;

   (c) use of the information for that other purpose is required or authorised by or under law;

   (d) use of the information for that other purpose is reasonably necessary for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue; or

   (e) the purpose for which the information is used is directly related to the purpose for which the information was obtained.

2. Where personal information is used for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue, the record-keeper shall include in the record containing that information a note of that use.

Principle 11 - Limits on disclosure of personal information

(e) the persons who are entitled to have access to personal information contained in the records and the conditions under which they are entitled to have that access; and

(f) the steps that should be taken by persons wishing to obtain access to that information.

4. A record-keeper shall:

(a) make the record maintained under clause 3 of this Principle available for inspection by members of the public; and

(b) give the Commissioner, in the month of June in each year, a copy of the record so maintained.

Principle 6 - Access to records containing personal information

Where a record-keeper has possession or control of a record that contains personal information, the individual concerned shall be entitled to have access to that record, except to the extent that the record-keeper is required or authorised to refuse to provide the individual with access to that record under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.

Principle 7 - Alteration of records containing personal information

1. A record-keeper who has possession or control of a record that contains personal information shall take such steps (if any), by way of making appropriate corrections, deletions and additions as are, in the circumstances, reasonable to ensure that the record:

(a) is accurate; and

(b) is, having regard to the purpose for which the information was collected or is to be used and to any purpose that is directly related to that purpose, relevant, up to date, complete and not misleading.

2. The obligation imposed on a record-keeper by clause 1 is subject to any applicable limitation in a law of the Commonwealth that provides a right to require the correction or amendment of documents.

3. Where:

(a) the record-keeper of a record containing personal information is not willing to amend that record, by making a correction, deletion or addition, in accordance with a request by the individual concerned; and

(b) no decision or recommendation to the effect that the record should be amended wholly or partly in accordance with that request has been made under the applicable provisions of a law of the Commonwealth;

the record-keeper shall, if so requested by the individual concerned, take such steps (if any) as are reasonable in the circumstances to attach to the record any

1. A record-keeper who has possession or control of a record that contains personal information shall not disclose the information to a person, body or agency (other than the individual concerned) unless:

   (a) the individual concerned is reasonably likely to have been aware, or made aware under Principle 2, that information of that kind is usually passed to that person, body or agency;

   (b) the individual concerned has consented to the disclosure;

   (c) the record-keeper believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or of another person;

   (d) the disclosure is required or authorised by or under law; or

   (e) the disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.

2. Where personal information is disclosed for the purposes of enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the purpose of the protection of the public revenue, the record-keeper shall include in the record containing that information a note of the disclosure.

3. A person, body or agency to whom personal information is disclosed under clause 1 of this Principle shall not use or disclose the information for a purpose other than the purpose for which the information was given to the person, body or agency.