Submission No. 99

JOINT COMMITTEE OF
2 1 OCT 2003
PUBLIC ACCOUNTS & AUDIT

SAKER **SECURITY CONSULTING**

ABN 26 650 675 863

P.O. Box 1602
CANBERRA ACT 2601

Tel: (02) 6295 9750

19th October, 2003

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

Dear Sir or Madam,

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

I am concerned that there is no effective program in Australia for the education and training of System Security Technologists. I believe that consideration of this matter is within the Terms of Reference of your Inquiry, hence my submission.

I have considerable experience in this aspect of security as I worked for 22 years as a civilian in the Defence Security Branch (now the Defence Security Authority), 13 years of which were as the Director of Technical Security. During this time I was responsible for recruiting and training technical security specialists.

Since separating from the Department of Defence in 2002, I have been trying to obtain sponsorship to conduct research to determine the specific education and training requirements for System Security Technologists. One person contacted was Senator Kate Lundy, who recommended I put a submission to the Committee.

Should the Committee agree with my proposal their support would be invaluable.

My submission and a copy of my proposal are attached.

I would be happy to provide any further information you may need. If detailed information is required it may be more effective if I present it verbally to the Committee.

Yours faithfully

William A. MacCallum
Principal Consultant

THE JOINT COMMITTEE OF PUBLIC ACCOUNTS AND AUDIT

INQUIRY INTO MANAGEMENT AND INTEGRITY OF ELECTRONIC INFORMATION IN THE COMMONWEALTH

A SUBMISSION BY SAKER SECURITY CONSULTING

SUMMARY

1. Security is an essential element in the management of information. The application of security policy and standards for the protection of the Commonwealth's electronic information needs to be undertaken by highly skilled personnel who are qualified and certified to analyse system security complexity, recommend appropriate counter-measures and, where applicable, oversight the implementation of such measures. There is a current shortage of such people. This submission to the Committee addresses system security requirements for the protection of information and the need for a high level security education and training program to produce System Security Technologists.

INTRODUCTION

2. The Terms of Reference for the Inquiry indicate the Committee will consider:

a. the privacy, confidentiality and integrity of the Commonwealth's electronic data;
b. the management and security of electronic information transmitted by Commonwealth agencies;
c. the management and security of the Commonwealth's electronic information stored on centralised computer architecture and in distributed networks; and
d. the adequacy of the current legislative and guidance framework.

3. It is essential however, that information is not considered in isolation from people and the environment in which those people live and/or work, and in which information is stored, transmitted and accessed. This is vital when considering system security requirements. Thus, before specifically addressing information management and security, there is a prime requirement to consider the interface/interaction of three core elements of a Commonwealth, or business, 'operation':

a. people;
b. environment; and
c. information.

Consideration of these three elements as a system is reflected below in the use of the phrase 'total system security'.

4. The point must also be made that Commonwealth information is accessed physically and/or electronically by elements of the Private Sector, who should therefore comply, as a minimum, with Commonwealth policy and standards for information management and security.

CURRENT SITUATION

5. In general, there is a need for an improved security status in the Commonwealth and the Private Sector. This has resulted from:

a. an increased threat;
b. increasing system complexity arising from the application of technology and the size and spatial distribution of systems;
c. the need for total system security assessment;
d. the need for top down security architecture development; and
e. the need for correct implementation, verification and validation of security measures.

Policy and Guidance

6. The two main areas of the Commonwealth that provide essential core security policy and guidance are the Attorney General's Department and the Defence Signals Directorate. This is reflected in the:

a. Commonwealth Protective Security Manual (PSM); and
b. Security Guidelines for Australian Government IT Systems (ACSI 33).

The basic policy and guidance given in these manuals may need to be enhanced where there is information requiring a high level of protection e.g. the Department of Defence produces the Defence Security Manual.

7. Guidance on the application of policy and standards is provided by the respective agencies. Although this area is vital to any security program it is only a small element of the total security workload. The bulk of security work is in determining the security architecture and specifications for each application of security policy and standards, ensuring the subsequent implementation of the security features and ongoing operational security management.

8. **Timely Implementation of Security Measures**. Implementation of security measures based on guidance provided by the Attorney General's Department and the Defence Signals Directorate can be delayed, as there is a limit to the number of security personnel from these areas that can provide such guidance and assist with implementation.

FUTURE

9. The implementation of total system security should be carried out by system security personnel who can:

a. conduct a risk analysis;
b. determine the security architecture;
c. specify the security requirements; and
d. oversight the development, commissioning, accreditation and ongoing support.

These system security personnel need to have relevant academic qualifications and security experience. There is a current shortage of such people. This shortage and the lack of a formal education and training program will reflect on the ability of the Commonwealth and Private Sector to effectively implement security programs. An enhanced national security program to counter an increased threat would need a concomitant increase in system security personnel and a commitment to their education and training. The aim would be to ensure that there are sufficient personnel in both the Commonwealth and the Private Sector, to effectively apply security policy and standards derived from a consideration of total system security requirements. Establishing a base of system security technologists across Commonwealth Departments and the Private Sector would ease the security workload on the Attorney General's Department and the Defence Signals Directorate and provide a valuable source of skilled security personnel in an emergency.

EDUCATION AND TRAINING

10. It takes about three years to train a technical person in the application of security policy and standards such that they can work with minimum supervision. A further two to five years are required to gain experience that would enable security technologists to work in positions such as a Security Manager in a large corporation or government department, or a Project Manager on large security tasks. There is also the need for experienced people to be involved in an ongoing education and training program both as participants and lecturers/instructors.

11. To date there has been no formal security education and training program for the level of system security personnel proposed. There is therefore a need for the Commonwealth, the Private Sector and Academia, to co-operate in a formal program of recruiting, educating and training high quality, first degree qualified, engineering and science graduates, to produce system security technologists of the calibre needed. Participants would gain experience in the application of security policy and standards, and undertake a masters degree in security technology.

12. The education and training program needs to be supported by the Commonwealth Government as a national requirement, to ensure the development of an appropriate security education policy and training standards, applicable throughout Australia.

13. **Exchange Program**. In view of the need for a global response to system security requirements, arising from the terrorist threat and computer hacking, it would be prudent to involve at least Australia's major allies in the proposed education and training program. A specific item could be the exchange and/or attachment of personnel to broaden experience.

CONCLUSION

14. There is a need for System Security Technologists in an overall Australian security program. To be effective and to ensure wide recognition of the capabilities of these technologists Commonwealth support is essential. Research needs to be undertaken to identify the education, training and experience required to enable a person to be qualified to work in the field of system security.

POSSIBLE COMMITTEE ACTION

15. The Committee might:

a. Agree that determination of the security requirements for the protection of information has to be done as part of the determination of the security requirements for total system security.

b. Agree that there is a need for an increase in the number of system security personnel.

c. Support a research project to determine specific education and training requirements for such personnel, as outlined in the attached unsolicited proposal.

William A. MacCallum
Principal Consultant
Saker Security Consulting