CABINET MINUTE

Security Committee

Canberra, 13 December 1993

No. 2412 (SEC)

Memorandum 1361 - The Threat to Australian Government Communications

The Committee noted the Memorandum.

Michael Keating
Secretary to Cabinet

[27]

MEMORANDUM No. 1361

COPY No. 15 of 30

FOR CABINET

Title	**THE THREAT TO AUSTRALIAN GOVERMENT COMMUNICATIONS**
Date	7 October 1993
Originating Department(s)	Secretaries Committee on Intelligence and Security (SCIS)
Cabinet or Ministerial Authority for Memorandum	Decision 6193 (SEC) of 25 June 1985 asked SCIS to report regularly to Security Committee on all relevant intelligence and security matters
Purpose of Memorandum	To provide the Security Committee with a report on the threat to Australian Government communications and the state of communications security based on advice provided by the Defence Signals Directorate in consultation with ASIO.
Legislation	Not Applicable
Consultation: . Departments consulted	SCIS (comprising Secretaries of the Departments of the Prime Minister & Cabinet, Defence, Foreign Affairs & Trade, Finance and Attorney-General's, the Chief of the Defence Force and the Directors-General of ASIO and ONA). The Director DSD was also consulted.
. Is there agreement?	Yes
Cost: . This fiscal year . year 2 . year 3	Not Applicable
Evaluation Strategy Agreed?	Not Applicable

THE THREAT TO AUSTRALIAN GOVERNMENT COMMUNICATIONS

This memorandum reviews the threat to Australian Government communications and the state of communications security. It draws primarily on the annual report to SCIS prepared by the Defence Signals Directorate (DSD), in consultation with ASIO, for the period 1992-93.

FOREIGN SIGNALS INTELLIGENCE ACTIVITY AGAINST AUSTRALIA

Russia

2. [redacted] ASIO assessed in the reporting period that the Russian Embassy in Canberra [redacted] This is based on a number of factors:

[redacted]

[redacted]

(c) An ASIO assessment in 1992 indicated that [redacted] but a subsequent investigation led to a re-appraisal [redacted]

[redacted]

3. ASIO assesses that personnel from the Russian foreign intelligence service (the SVR - the KGB's successor) in Australia [redacted]

[redacted] ASIO presently assesses [redacted] This notwithstanding, [redacted]

Other countries

4. [redacted] In considering the likely risk involved:

(a) In the case of [redacted] (which are the subject of security intelligence study), ASIO's understanding of [redacted]

(b) Several other Asia-Pacific countries [redacted] However, these countries [redacted] has been the subject of [redacted] ASIO is unable to comment on whether [redacted]

5. DSD is unable to determine to what extent Australian communications may be targeted by these countries. But it seems likely that their Sigint assets are used primarily to monitor military communications in areas of greatest strategic interest to those countries, or communications within their own territorial boundaries.

6. [redacted]

The General Threat

7. [redacted] In the absence of information as to [redacted] are at greatest risk. [redacted]

8. Based on [redacted] DSD continues to assess that there is a high level of threat to the Government's communications when they are not properly enciphered. This applies not only to international communications carried via satellite, but also landline and microwave circuits provided to Australian government agencies by the communications authorities of foreign countries and to unprotected Government communications within Australia.

9. DSD considers that the use of DSD approved cipher equipment and the ADCNET secure network for government communications overseas should be encouraged to eliminate the risk of interception and exploitation.

THE STATE OF COMMUNICATIONS SECURITY

Telephone, Facsimile and Data

10. Many crisis situations in recent years (eg. Bougainville, the Gulf War, Somalia and Bosnia) have demonstrated the need for the availability of secure telephone, facsimile and data facilities within Government departments. DSD is developing the *SPEAKEASY* project as a means of providing an affordable, secure terminal for widespread government use.

11. DSD advises that the *SPEAKEASY* project has made significant progress over the past year. Current results are very positive and the technical risk in proceeding to a production version is assessed as slight. Full scale production is planned to commence in mid 1994.

Telegraphy and Data

12. Government telegraphy and data services processing national security classified information are protected by high-grade crypto equipment which has been upgraded progressively over the past years. Provided the

equipment continues to be used correctly and in accordance with prescribed doctrine, DSD considers that classified government information transmitted by this means is safe from exploitation. [redacted]

Sensitive Classified Data

13. The publication of the new Protective Security Manual and the introduction of new classifications (Highly Protected, Protected, In-Confidence) has served to focus attention on the need to secure government data communications in the interests of privacy. Much of this data, although not classified for national security reasons, has potential intelligence value for its economic, trade and financial content. The use of DSD approved commercial standard cryptographic equipment has spread and has increased the resources a foreign intelligence service would need to devote to any attempt to exploit these communications.

14. Both the Privacy Commissioner and Australian National Audit Office have been instrumental in directing government agencies to seek DSD's advice on data protection and on the security of information processing systems generally. In that regard the relocation of DSD's information security branch to Canberra continues to provide a more responsive service to the various customer agencies.

15. When combined with a robust DSD/Attorney-General's Department computer security educational program, the result has been a much greater awareness across government agencies of the value of the information they process and the need to take measures to protect its confidentiality, availability and integrity. But there is a continuing threat from 'hackers' to Government information processing systems of all types, and DSD assesses that this threat will continue to grow.

CONCLUSIONS

[redacted]

[redacted]

(d) unenciphered telegraphy, telephone, facsimile and data links to and from Canberra, and the mobile telephone network, are particularly at risk of exploitation;

(e) the risk to Australian Government communications carried on international circuits and not protected by DSD-approved cryptographic equipment remains high;

(f) the secure system operated by the Department of Foreign Affairs and Trade on behalf of the Australian Government minimises the risk of hostile electronic exploitation;

(g) the *SPEAKEASY* Government Secure Communications Terminal project should continue to be progressed by DSD and AOTC and brought into service as quickly as possible in order to meet the need for an affordable secure telephone for widespread government use;

(h) there is a continuing risk to government information processing systems from unauthorised access; and

(i) there continues to be a heightened awareness in agencies beyond the traditional intelligence and security community of the requirement to improve the security of their information processing systems.

SML NO. 1361

SECURITY

SEE FILE KCA 1535/P1