4

Agreement between Australia and the USA concerning Security Measures for the Reciprocal Protection of Classified Information

4.1 The proposed Agreement between Australia and the USA concerning Security Measures for the Reciprocal Protection of Classified Information sets out procedures and practices for the exchange and protection of classified information and for visits between Australia and the United States of America. Upon entry into force, the proposed Agreement will supersede three existing non-legally binding instruments with the USA regulating classified information:

- the 'Security Agreement' between the Department of Defense of the United States of America and the Department of Defence of Australia which came into effect on 29 August 1950, as amended;
- the United States-Australian Arrangements for facilitating Disclosure of Classified Military Information to Commonwealth Nations which came into effect on 29 August 1950; and
- the 'General Security of Information Agreement' between the Government of Australia and the Government of the United States of America concluded by an exchange of notes dated 2 May 1962, as amended.[1]

---

1 Information about the proposed treaty action is taken from the National Interest Analysis, tabled in conjunction with the treaty text on 27 August 2002, and a public hearing held in Canberra on 16 September 2002.

Background

4.2 While there is no suggestion that either party has, or would, fail to comply with its commitments under the existing instruments, the US requested in February 2000 that the arrangement be formalised by treaty and has indicated that it requires a legally binding agreement. Australia agreed to this request and agreement was reached on all the relevant parts of the documents in March 2001. Ministerial approval was granted in August 2001. The agreement was signed on 25 June 2002.[2]

4.3 Similar Agreements recently reviewed by the Committee and recommended for ratification were the Agreement between the Government of Australia and the Government of the Republic of South Africa for the Reciprocal Protection of Classified Information of Defence Interest, done at Canberra on 11 May 2002, and the Agreement between the Government of Australia and the Government of Kingdom of Denmark for the Reciprocal Protection of Classified Information of Defence Interests, done at Copenhagen on 27 September 1999.

The Agreement

4.4 The Committee has been advised that the proposed Agreement with the United States will set uniform standards and procedures for exchanging classified information between all government departments and agencies in both countries.[3] It will also enable companies in both countries to tender for, and participate in, contracts which involve access to security classified information. Following termination of the existing instruments, any information previously exchanged shall continue to be protected in accordance with the proposed Agreement.

4.5 Under the proposed Agreement, classified information which the Government of Australia passes to the Government of the United States of America will be afforded protection similar to United States information of corresponding security classification, will not be used for a purpose other than that for which it was provided and will not be passed to any third party without the written consent of the Australian Government. Access to Australian classified information will be limited to those United States Government officers whose official duties require such access. Equally, information passed under the proposed Agreement from the

2 M. McCarthy, *Transcript of Evidence*, p.32.

3 NIA; evidence from the Attorney-General's Department, public hearing 16 September 2002.

United States Government to the Australian Government must be protected in the same manner. Supplementary Implementing Arrangements can be separately negotiated to cover particular departmental or agency issues.

4.6 The Committee was advised that the Australian Government currently exchanges a large amount of classified information with the United States. These exchanges include government to government information, details of defence acquisition projects (permitting the other country's industry to tender for, or participate in, classified contracts), and information related to cooperation between the two countries' armed forces. The proposed Agreement provides the necessary protocols and security assurances to facilitate the exchange of classified information by ensuring that the information is protected by legally binding obligations.

4.7 The Committee understands that the delay between the granting of ministerial approval and the actual signing was in part due to the events of 11 September 2001. The arrangements in the proposed Agreement provide all the necessary safeguards for the exchange of classified information even given that change in world circumstances; there has not been a need to revisit the terms or the negotiated terms as a result of 11 September and the reassessment that many countries, including Australia, have made of their security arrangements.

Provisions of the Agreement

4.8 The provisions of the Agreement include the following matters:[4]

Marking of classified information (Article 3)

4.9 The name of the originating government must appear on all classified information received by both parties. National security classifications to all classified information must be assigned on transmission and on receipt.

Protection of classified information (Article 4)

4.10 Each Party must accord classified information, or anything containing classified information, received from the other Party a standard of physical and legal protection no less stringent than that which it provides to its own classified information of corresponding classification.

4 Extracted from the National Interest Analysis.

4.11 The recipient Party shall only disclose, release or provide access to classified information received from the other Party to individuals who require access in order to perform their official duties and hold an appropriate personnel security clearance.

4.12 The recipient Party must ensure that each facility or establishment that handles classified information maintains a registry of the clearance of individuals at the facility or establishment who are authorised to have access to the information.

Personnel Security Clearances (Article 5)

4.13 Article 5 sets out the criteria for granting personnel security clearances, requires the Parties to investigate adherence to the criteria and obliges them to provide assurances to the other Party about the classifications of persons receiving information.

Release of Classified Information to Contractors (Article 6)

4.14 Prior to any release of classified information to contractors or prospective contractors, personnel and facilities must be checked to ensure that the information is going to be protected in accordance with national laws.

Responsibility for Classified Information (Article 7)

4.15 Each Party is responsible for all classified information it receives from the other Party while the information is under its jurisdiction and control. During the transmission of information the transiting Party retains responsibility until the custody of the information is formally transferred to the other Party.

Responsibility for Facilities (Article 8)

4.16 Each Party is responsible for ensuring that all facilities, where the classified information of the other Party is kept, are secure.

Transmission of classified information (Article 10)

4.17 Classified information shall be transmitted between the Parties through government-to-government channels or channels mutually approved in advance in writing by both Parties. The minimum standards for packaging the classified information are detailed in the proposed Agreement.

Visits (Article 11)

4.18 Visits by representatives of one Party to facilities and establishments of the other Party, that require access to classified information, or where a security clearance is required to permit such access, shall be limited to those necessary for official purposes and to representatives who hold a valid security clearance. All requests, with details of the visit, will be forwarded through each Party's embassy prior to such visit.

Security standards (Article 13)

4.19 On request, each Party must provide to the other Party information concerning its security standards, practices and procedures for the safeguarding of classified information, including those relating to industrial operations. Each Party must inform the other Party of any changes to its laws and regulations that would affect the manner in which classified information is protected under the proposed Agreement.

Reproduction of Classified Information (Article 14)

4.20 Each Party must ensure that any reproductions made of classified information are marked with all original security markings, placed under the same control as the originals and are limited to the numbers required for official purposes.

Destruction of Classified Information (Article 15)

4.21 The destruction of classified information must be done by means that will prevent the reconstruction of the classified information.

Downgrading and Declassification (Article 16)

4.22 Each Party must not downgrade the security classification of the classified information received from the other Party without prior written consent of the originating Party.

Loss or compromise (Article 17)

4.23 To minimize any risk of damage through the loss or compromise of exchanged classified information the receiving Party shall immediately inform the originating Party of any loss of, or known or suspected compromise of, such information. The receiving Party shall then investigate the circumstances of such loss or compromise and inform the

originating Party of the finding of the investigation and corrective action taken or to be taken.

Disputes (Article 18)

4.24 Any disputes shall be resolved by the Parties through consultation and shall not be referred to any national court, international tribunal or third party for settlement.

Termination of Agreement

4.25 The proposed Agreement may be terminated at any time by mutual agreement in writing, ninety days after the giving of such notice. If the proposed Agreement is terminated, the responsibilities and obligations of the Parties in relation to the protection, disclosure and use of classified information already exchanged shall continue to apply, irrespective of the termination. This provision ensures the ongoing protection of classified material including its destruction or return to the originator when no longer required for the purpose for which it was exchanged.

Consultation

4.26 The Minister for Foreign Affairs provided approval for the Department of Defence to be the coordinating authority for the Commonwealth in the implementation of this proposed Agreement. The Department of Defence consulted with Department of Prime Minister and Cabinet, the Attorney-General's Department and Department of Foreign Affairs and Trade throughout the negotiation process and they have confirmed that the proposed Agreement meets the requirements of all Australian Government departments and agencies that deal with national security classified information.

4.27 The States and Territories were advised about the proposed Agreement through the Commonwealth-States-Territories Standing Committee on Treaties' Schedule of Treaty Action. No State or Territory comment has been received to date.

Implementation

4.28 The Committee has been advised that no changes to domestic laws or policy are required to implement the proposed Agreement. The proposed

Agreement can be implemented through the Commonwealth Protective Security Manual, which sets out the procedures covered by the Agreement. The Agreement will not effect any change to the existing roles of the Commonwealth Government or the State and Territory Governments.

4.29 The Security Authorities responsible for implementing the proposed Agreement are the Head Defence Security Authority, Australian Department of Defence, and the Director International Security Programs, USA Department of Defense.

Issues arising

Classifying information

4.30 In response to the Committee's concerns about the different national security classifications between Australia and the United States of America, officials from the Department of Defence stated that it was a matter of different bureaucracies giving different names to substantially the same information. The Department also suggested this is based on different definitions of the harm that will come to national security if the information is compromised and advised that there is 'always an element of subjectivity in those judgments.'[5] The Committee was advised, subsequent to the public hearing, that there are four levels of national security protective markings, which are assigned to reflect the consequences of the compromise of the information:

- RESTRICTED – when the compromise of the information could **cause limited** damage to national security;
- CONFIDENTIAL – when the compromise of the information could **cause damage** to national security;
- SECRET – when the compromise of the information could cause **serious damage** to national security; and
- TOP SECRET – when the compromise of the information could cause **exceptionally grave damage** to national security.[6]

5 McCarthy, *Transcript of Evidence*, p.34.

6 Supplementary information provided by the Department of Defence, 10 October 2002.

4.31 Where there is a difference in levels of classification, or a discrepancy in terms used for classified material, the Department stated that the United States will treat Australian restricted information in the same way that it treats its own (American) confidential information.[7]

Access

4.32 The Committee was advised that access to Australian classified information will be limited to those United States Government officers whose official duties require such access. Equally, information passed under the proposed agreement from the United States Government to the Australian Government must be protected in the same manner. Supplementary implementing arrangements can be separately negotiated to cover particular departmental or agency issues. The agreement will not in any way prejudice the existing procedures for access to classified information by elected representatives. The agreement will not change domestic law or policy.

4.33 The Department confirmed, as per the Exchange of Notes which were included with the tabling documentation, that Members of Parliament have access to classified information with no requirement for a security clearance:

> In respect of the requirements for security clearances in the Agreement, the Parties acknowledge the special status of elected representatives at the federal level, and confirm their intention to continue to apply their current practices to them.[8]

Transmission of information

4.34 The Department advised that shared information is transmitted both electronically and in hard copy, and as is the case with the majority of government information which needs to be transmitted and stored, it is encrypted.

4.35 The Committee was advised that the Defence Signals Directorate, in its role as the national information security authority, actually provides advice to the whole of government about levels of encryption; a higher level of encryption will obviously be needed to encrypt, for example, highly sensitive information flowing between departments. The Defence

7 M. McCarthy, *Transcript of Evidence*, p.34.

8 Exchange of Notes, paragraph 5.

Security Authority advises the Department of Defence on policy in relation to matters such as encryption.

4.36 The Department referred to the cost of levels of encryption and the risk assessments which are carried out to judge the appropriate standard of encryption:

> It is not that the Defence Signals Directorate would or would not attempt to limit levels of encryption; it is that it would advise on appropriate levels of encryption for different types of information, recognising that there are high costs involved as you increase the level of encryption.[9]

Visits to facilities

4.37 In the context of Article 11 of the Treaty, the Committee expressed concern about the ability of Australian Members of Parliament to visit joint (US-Australia) facilities in Australia, and the arrangements for visits of American elected representatives to those sites. Some Committee members expressed a belief that members of the American Congress have greater access to some Australian-based facilities than Members of Australian Parliaments. The Committee requested further information from the Defence Security Authority on how visit requests are made, how many requests have been received and whether they have all been undertaken.

4.38 The Committee was advised subsequently that the sole joint facility in Australia is the Joint Defence Facility Pine Gap (JDFPG), which operates under the Pine Gap Treaty (Australian Treaty Series 1966 No. 17, amended by Australian Treaty Series 1988 No. 36). Access to this facility must be approved by the Minister for Defence. Records dating from 1996 show that 14 visits were made by Members of the Australian Parliament and eight visits by Members of the Northern Territory Assembly. From March 1996 to August 2002 there have been 17 visits by US congressional staff to the JDFPG. The information about the number of requests made is still to be provided.[10]

4.39 While the Committee was advised during the hearing that there are specific national areas within joint facilities, the Committee understands that this evidence is to be amended. The Committee also requested information from officials from the Department of Defence about the

9 McCarthy, *Transcript of Evidence*, p.40.

10 Department of Defence, *Correspondence*, 10 October 2002.

briefings that are able to be obtained in those circumstances. At the time of printing this report, the Committee is still awaiting clarification of these issues.

Loss or compromise - penalties for disclosure

4.40 The Committee was advised that if there is a breach of the conditions of this treaty, the parties will initially advise one another that there has been a possible compromise of their information. The two organisations concerned would need to consult about the level of compromise. The Committee understands that it then becomes a matter for the government concerned. Defence officials stated that:

> For example, in the defence context the penalties might range from a minor breach due to oversight rather than malice where the penalty might be that the person receives further training in awareness through to, at the most extreme end, possible criminal sanctions for the unauthorised disclosure of classified information. The government concerned would sanction the person concerned and would keep the other government apprised of what action it was taking. Obviously it would want to reassure the other government that appropriate steps had been taken and that any systemic problems, for example, that might be identified are addressed.[11]

Monitoring

4.41 The Committee was advised that there is not a formal monitoring regime in place for this Agreement, but that the Defence Security Authority and its counterpart agencies in the United States are in regular contact, which may also include visits to discuss issues under the treaty.[12]

4.42 The Committee notes that Australian companies which are handling US classified information will also be internally monitored and evaluated to ensure compliance with the terms of the Agreement. It was the view of Defence Department officials that the United States has similar audit arrangements in place for its own facilities.[13]

11 McCarthy, *Transcript of Evidence,* p.41.

12 McCarthy and Wishart, *Transcript of Evidence,* p.41.

13 McCarthy, *Transcript of Evidence,* p.42.

Concluding remarks

4.43 The Committee notes that there were several areas, particularly in relation to the procedures relating to visits referred to under Article 11, on which departmental officials were unable to provide an adequate briefing. Further, the Committee was advised that certain evidence given at the hearing required amendment. The Committee is still to receive formal notification of where inaccuracies occurred in evidence provided by the Departmental officials. The Committee expresses its concern at the quality of evidence that was provided at the time of the hearing, and the delay in any subsequent correction.

4.44 The Committee is of the view that this treaty is, overall, in the national interest. Conscious of the timeframe imposed upon the Committee for the tabling of reports, the Committee recommends ratification. However the Committee remains concerned that the Department of Defence and the Defence Security Authority have yet to provide specific answers to requests from Committee members on issues arising under Article 11 of the Treaty. Accordingly, the Committee will seek further briefings from the Department of Defence and the Defence Security Authority about the procedural issues that have led to this situation, and proposals to ensure that it does not recur.

Recommendation 4

The Committee, concurring with the views expressed in the National Interest Analysis, recommends that the Agreement be ratified.

Recommendation 5

The Committee recognises that responses to questions on notice and requests to amend the Hansard record must receive security clearance and Ministerial approval prior to their release.

The Committee recommends that the Department of Defence ensures that these measures do not inhibit its ability to provide requested information to the Committee within an acceptable timeframe.