
The business opportunities in supporting the **Australian Intelligence Community**

July 2005



Report by Athol Yates



About the Centre

The Australian Homeland Security Research Centre undertakes independent, evidence-based analysis of domestic security issues. Its research is funded by publications and professional development courses.

The Centre's research priorities include:

- The homeland security market in Australia
- The appropriate sharing of security costs and benefits between businesses and society
- A national security and industry policy
- Security expectations of corporate Australia
- The appropriate balance between:
 - different threats including biological, explosive, chemical, radiological, incendiary, kidnapping, extortion, and electronic
 - protection of critical infrastructure and the built environment
 - a terrorism and all-hazards focus
- Performance measures for domestic security policy
- Trends in science, engineering and technology for homeland security
- Sectorial stocktakes

Australian Homeland Security Research Centre
Tel 02 6161 5143, Fax 02 6161 5144
PO Box 295, Curtin ACT 2605
info@HomelandSecurity.org.au
www.HomelandSecurity.org.au

ISBN 0-9757873-0-6

© 2005, Australian Homeland Security Research Centre.

All rights reserved. Other than brief extracts, no part of this publication may be produced in any form without the written consent of the publisher. This report can be purchased at www.homelandsecurity.org.au.

About the author

Athol Yates is the Executive Director of the Australia Homeland Security Research Centre.

He specialises in analysing national security policy and the role played by the private sector in enhancing national security.

He has written extensively on the subject as well as giving a large number of invited presentations.

Athol's qualifications include a Bachelor of Engineering, GradDip Soviet Studies, and Masters of Public Policy.

He is the editor of the *Australian Homeland Security Market Insight* and the *National Security Practice Notes*.

His work as the Associate Director at Engineers Australia resulted in him publishing the following reports: *Engineering a Safer Australia: Protecting Critical Infrastructure and the Built Environment*, and *Queensland Infrastructure in the Age of Terrorism*.

Author's introduction

This report draws on information from interviews and publicly available from Australian Government reports, AIC agency documents and websites. Due to the sensitivity of the subject matter, discussion of specific projects and examples is limited.

Although the report highlights many challenges facing companies that are seeking to partner with the AIC, the intention was not to indicate that the AIC is difficult to work with.

Rather it is to highlight areas where the AIC is different from other parts of government and why this is so. Only with this understanding can an informed business relation be built.

I would like to thank David Beveridge and many others for their significant contributions to this report.

Athol Yates

Executive Summary

More than \$500 million is spent each year by the Australian Intelligence Community (AIC). On the surface, this expenditure would appear to offer a significant opportunity for Australian business.

However, a detailed examination of the expenditure reveals that the potential for the private sector is rather modest and winning a portion of the work that results from this expenditure is challenging. But this reserved assessment does not mean that work in the AIC is not worth pursuing.

This report details the business opportunities in supporting the AIC, and the costs and benefits of winning work.

The AIC comprises six Australian Government intelligence and security agencies which are:

- Office of National Assessments (ONA)
- Australian Secret Intelligence Service (ASIS)
- Defence Signals Directorate (DSD)
- Defence Intelligence Organisation (DIO)
- Defence Imagery and Geospatial Organisation (DIGO)
- Australian Security Intelligence Organisation (ASIO)

Each AIC agency is quite different from the others as each has a unique culture and modus operandi due to their history, the type of work they undertake and staff background. This means that companies selling to the AIC should treat each agency as a unique client. Applying the tools and techniques used in winning work in other AIC agencies, let alone in Defence or the AFP, will not generate success unless they are substantially tailored for each agency.

In evaluating whether to enter the intelligence market, companies obviously need to weigh up the costs and benefits, and the opportunities elsewhere.

The costs of entering the AIC market include the price of building relationships and trust, obtaining information on opportunities, meeting product standards that can exceed commercial standards and meeting personnel security requirements that include vetting of staff.

The benefit of winning work with the AIC is generally restricted to the profitability of each project. This is because while completing a project allows you to get your foot in the door of an agency, it does not make it much easier to win work from another areas or different agency. The marketing value of the work is also limited as agencies invariably do not wish for their projects to be publicly discussed. Consequently the practice of loss leading does not make sense.

Selling products to the AIC is generally substantially easier than selling services. This is because products often do not require intimate access to the agency's work and there is no need to have a detailed understanding of how and where the products will be employed. Examples of this are storage systems, IT analyst tools and interception equipment. A challenge for the supply of products is ongoing support and maintenance. The broken equipment often cannot be readily inspected unless service technicians have security clearances and the details necessary to replicate a fault might never be forthcoming.

Two types of services can be of interest to AIC agencies – commercial support services and professional service provision.

Commercial support services, such as recruitment and training, are easier to supply than professional support services, such as project management, engineering and analytical services, which require intimate knowledge of the agency's operations.

It is important to remember that some work is unavailable to Australian organisations, for all intents and purposes, because of system sensitivities, such as cryptographic systems, or the technical level of competence required. However, in general, there is a preference at the senior levels to use Australian product suppliers for routine COTS products and maintenance as a way of reducing dependence on other countries as well as lowering costs and reducing response times.

Size is not really a determinate in a company's chances of entering the AIC market. In many ways, smaller companies have an advantage as the size of typical AIC projects is often smaller than the viability threshold for large companies.

Opportunities for the supply of goods and services are directly related to the challenges which are facing the AIC agencies. There are a number of cross-agency challenges and these include:

- recruiting and training
- managing the volume of intelligence being distributed, notably snapshot assessments
- ensuring the AIC is sustainable during extended crises or when multiple operations are underway
- preventing mistakes as the agency expands
- meeting increasing demand
- the need to demonstrate to Government that the additional funding given has delivered measurable benefits
- data quality control

There are also a range of potential opportunities with individual agencies. These include DSD's four major projects which have capital expenditure timelines out more than a decade, and the work arising from DIGO's capability development work.

Over the next few years, it appears there will be increased opportunity for industry to contribute expertise and solutions to the AIC. This assessment is based on the twin trends of increased intelligence production requirements and too few resources. These trends mean that efficiencies must be found to ensure that the intelligence output is timely, relevant and of appropriate quality. Working with the private sector is one effective way of achieving this.

Due to the ingrained attitudes of secrecy and caution, the increased use of the private sector will be neither rapid nor constant across the AIC agencies. Another factor slowing it down will be the isolated pockets of resistance in dealing with the private sector. Their concern, once common in the ADF, is that the private sector only cares about profit and meeting contractual requirements, rather than about the capability being delivered. Others are cautious about engaging consultants and contractors, particularly for IT work, because they worry that it will highlight the pay rates and employment options within the private sector, leading to AIC staff separating.

However, with the promotion of AIC leaders who are more comfortable with technology and are focused on outcomes, engagement with the private sector will inevitably increase as it has across all government agencies.

Table of contents

Executive Summary	3
The opportunities and the risks	
1 Introduction	6
2 AIC characteristics	6
2.1 Implications for the private sector	10
2.2 Breaking into the market	10
2.3 Making the decision	11
2.4 Market size	13
3 Cross-agency challenges	13
4 Agency business opportunities	14
5 Conclusion	15
Annex 1: The AIC Agencies	
A Foreign intelligence Agencies	16
A1 Office of National Assessments	16
A2 Australian Secret Intelligence Service	17
A3 Defence Intelligence Group	18
Defence Imagery and Geospatial Organisation	19
Defence Signals Directorate	20
Defence Intelligence Organisation	20
B Security intelligence Agency	
B1 Australian Security Intelligence Organisation	21
Annex 2: Contracts and consultants	
C List of ONA contracts	23
D List of DISG consultancies	24
Annex 3: Acronyms and endnotes	
E Acronyms	26
F Endnotes	26