Submission No 116

Inquiry into potential reforms of National Security Legislation

Organisation: Unisys Australia Pty Limited

Parliamentary Joint Committee on Intelligence and Security

Unisys

Unisys Australia Pty Limited
ABN 31 105 642 902

Unisys Campus
Rhodes Corporate Park
1G Homebush Bay Drive
Rhodes NSW 2138
PO Box 288
Concord West NSW 2138

Telephone
61 2 9647 7777
Facsimile
61 2 9647 7000

20 August 2012

The Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
CANBERRA ACT 2600
pjcis@aph.gov.au

Submission in response to potential reforms of national security legislation

Unisys welcomes the invitation to submit our views in relation to the public discussion paper "Equipping Australia against emerging and evolving threats". In so doing, we hope to assist you in your deliberations, bring another perspective to the table and further inform discussion on some of the issues raised.

Background

Unisys is a global information technology services provider that designs, builds and manages mission-critical environments for businesses and governments where there is no room for error.

Our public sector practice in Asia Pacific specialises in the domain areas of national security and law enforcement, alongside other industry practice focus areas of aviation and financial services. This is underpinned by four capability areas of focus: security, data centre transformation and outsourcing, end user outsourcing and support services, and application modernisation and outsourcing. In sum, we specialise in those areas of the market where the cyber-security risk and potential impacts are wide-reaching, highly significant and very complex.

In Australia we provide, or have provided, security solutions and services to several national and state agencies including the Department of Defence, Department of Immigration and Citizenship, Australian Federal Police, Department of Foreign Affairs and Trade (Australian Passports), the Independent Commission Against Corruption, NSW Police, and Qld Department of Transport and Main Roads (biometric drivers licence).

In this context, we help governments maintain national security in a world characterised by new classes of threats and opportunities, accelerating information overload, and constrained funding. Based on this experience we believe that effective national security fundamentally requires the ability for national security and law enforcement agencies to efficiently share, protect and exploit of information.

Market insight

Unisys also brings to this submission a depth of insight based on market research conducted in Australia and other countries around the world. The Unisys Security Index™ was launched in Australia in 2006 and is conducted at regular intervals in 11 countries[1] to monitor public attitudes on security-related issues. Conducted in Australia by Newspoll, the Unisys Security Index enables us to monitor overall levels of concern over time and levels of concern on specific topics or questions such as national security.

The annual Unisys Consumerisation of IT research is conducted in Australia and eight other countries.[2] It explores issues related to large public and private organisations and their employees using technologies developed for the consumer market, specifically social media and mobile devices, as business productivity and customer engagement tools. A central focus of the research is the increased cyber-security threats these technologies create. Relevant results from both research studies are highlighted in our submission.

Response

In the public discussion paper we see three consistent, inter-related topics emerging from the comments and questions posed:

1. The fundamental need for agencies to be able to share information securely to strengthen national security capabilities and resources
2. The impact of mobility and consumerisation on the traditional definition of “computer”
3. The need to expand the definition of what constitutes “national infrastructure” and how this creates a shared responsibility for the government and private sector to protect national security

In our submission we will address these topics and outline steps that all parties should take to protect the security and safety of Australia, its citizens and businesses.

1) Obtaining and sharing information for national security

Looking at the requirement of a modern intelligence and security agency legislative framework to support enhanced corporation between agencies we need to consider the collection, interpretation, securing and sharing of data and how the importance of that data may change when combined with other sources.

[1] www.unisyssecurityindex.com.au

[2] http://www.unisys.com/unisys/ri/topic/researchtopicdetail.jsp?id=700004

- **Collection**

  This is not limited to data collected via covert intelligence gathering. Open Source Intelligence, the collating and analysing of unclassified, publically available information can enable governments to identify patterns and hot spots of public sentiment, conversation or activity, transforming disparate information into intelligence. However, it provides both challenge and opportunity in the national security context.

  In today's online world the detail and sheer amount of data available from public information sources has exploded. From online media, web-based communities, social networking sites, wikis and blogs through to official reports, to academic papers - it involves massive amounts of data, constantly being published.

  Given the requirement for budget cuts, much of this analysis can be automated using advanced tools such as neural-network technology that is based on our growing understanding of how brains store information as patterns and use those patterns to solve problems.

- **Interpretation**

  But not all public information should be treated with the same respect. It is critical that the context be taken into account when determining what weight to give a particular piece of open source information.

  For example, is the source of the information considered to be highly reliable or typically unreliable? Does the source have "an agenda"? What was the timeframe and location in which the information was published and what other events or activities might bias the source? Are there corroborating alternative sources, and if so how reliable are they? We need to consider that counter intelligence may be disseminated through open source channels with the aim of providing misinformation and distraction.

  Access to privately held data, such as described in the amendments to the *Telecommunications (Interception and Access) Act 1979* may help validate/discount information obtained from a public source and is an example of the shared responsibility of government and the public sector.

  Of course, the privacy of the individual and the organisation that holds their personal data must be respected. However, it is our observation that public attitudes towards security and privacy are evolving and we have regularly tested assumptions about the level of public support for certain types of security measures via the Unisys Security Index – Australia's only regular barometer of the public's sense of security. We have observed that people are much more demanding of security in many dimensions of their lives (to enable them to do their banking online, to travel easily, to receive better government service, etc.) and with this comes a willingness to participate in security measures by doing or allowing some things they might not once have done, including the provision of sensitive personal information if it enables greater security.

For instance, according to the May 2012 Unisys Security Index 95% of Australians supported airport customs or immigration staff using facial recognition to identify passengers on police watch lists and 92% supported police using facial recognition technology to identify people from security camera footage or video obtained from the public. However, only 66% said it was acceptable for employers to use the technology to identify what parts of a building staff had accessed and with whom (29% opposed the idea) and just 38% said it was acceptable for Facebook to use it to make it easier for users to identify friends in photographs (50% opposed). In summary, there is high public support to use what may be considered an invasive technology for policing or protecting borders, but not in other circumstances.

- **Securing**

  Another challenge in government circles is the classification of the intelligence gained by aggregating and analysing that data as with analysis its value and potential sensitivity increases.

  This raises questions about what the threshold is to go from “open” to “secret”. Who makes the decision about how to classify data obtained from open sources? And with whom can that data be shared? Being able to share intelligence across departments, between the public and private sector, and across international borders may be advantageous, but such information may need to be secured if it could reveal sensitive information to adversaries.

  This comes back to the need to find a balance between protecting sensitive data while being able to securely share that data between trusted parties. Sensitive data in the wrong hands can pose real danger. But valuable intelligence that is unavailable to key decision makers is worthless.

  Post 9/11 there was a public call for greater cooperation between governments globally to share information against common threats. However, in the last few years there has been debate regarding the degree to which data should be shared – particularly if doing so would remove a competitive edge or “decision advantage”. There has also been some public backlash fuelled by fears of privacy being breached by governments that create digital dossiers on their citizens.

- **Sharing**

  Once it is determined who should have access to the intelligence, the issue comes down to how to share that data securely. Today's constrained IT budgets, remote workers, cloud computing and mobility bring new challenges on this front. And quite frankly, you must assume that even the internal network is a hostile environment.

  Not all data is the same – the level of sensitivity varies with security classification levels typically defined by the harm that would be incurred should a particular piece of information be disclosed to an unauthorised individual or organisation.

  Ultimately, access to sensitive information should be guided by need-to-know as well as clearance level. Historically this has been very cumbersome and expensive to implement and manage, but the latest generation of encryption technologies allow multiple "communities of interest" to share the same IT infrastructure without fear of data leakage outside their community of authorised individuals. In this way only those roles that have a valid need to have access the data can do so. This puts the focus on securing the data itself, rather than your ability to gain access to a machine.

2) Mobility and the new definition of a "computer"

The use of consumer-style technology, such as smartphones, tablets and social media, by information workers (iWorkers) in Australian workplaces continues to accelerate necessitating the need to change the definition of 'computer' as referenced in section 25A of the *Australian Security Intelligence Organisation Act 1979*.

In the soon–to-be-released 2012 Unisys Consumerisation of IT research, 69% of Australian information workers say they use a laptop for work purposes, 55% use a smartphone and 24% use a tablet – all higher than the global average. In addition, 42% of workers downloaded mobile apps for work use with 63% saying that they did so because they needed it but their employer did not provide an alternative.

Many IT departments are delaying rolling out formal or comprehensive mobility or bring-your-own technology programs because they are concerned about the security implications. However, the trend is being led by employees and will continue regardless.

As a result, the reclassification of security levels of access to data must also be considered when applied to mobile devices and social media as classification-based and need-to-know-based access control may be insufficient when protecting sensitive data.

Yet why give employees these powerful devices if they can't take advantage of their features? By recognising that not all information has the same level of sensitivity, appropriate information can be opened up to take advantage of the productivity benefits provided by mobile devices without jeopardising truly secure information. For this to work, there needs to be more interaction between the IT teams and those who make the decision about who/what is "need to know".

Attribute-based access control is also an emerging technology that grants access based not only on the nature of the data and the individual requesting access, but also on the location from which access is being requested, the method used to authenticate your identity and whether there is anything about the access request that is outside your normal pattern.

3) Redefining critical national infrastructure and the resulting shared responsibility for the government and private sector to protect national security

Our increasing reliance on IT systems—from the Internet, mobile phone networks and banking systems through to the systems used to run physical infrastructure such as water and power supply or train timetables—requires an expanded definition of what constitutes "critical national infrastructure".

The May 2011 Unisys Security Index found that 45% of the Australian public considered the Internet to be extremely or very vulnerable to a malicious or terrorist attack, ranking only airports and airlines as being more vulnerable (48%). Interestingly, this question was fielded in 11 countries and Australia and New Zealand were the only two countries where perceived vulnerability of the Internet was so high. Perhaps this is because of our remote location where we are aware of how reliant we are on the Internet for both our business and personal lives.

The idea of knocking out or blocking access to critical infrastructure to weaken an opponent is nothing new. In ancient times attackers would surround cities and cut off access to food, water and other supplies. Such blockading is common military offensive strategy.

But with our increased dependence on our technology networks in both our work and personal lives, it is no surprise that today's attackers seek to exploit security vulnerabilities in the cyber world with the aim of disrupting the physical world. This applies regardless of whether the cyber attack is designed to take down the IT system itself or is used to damage other critical infrastructure such as water or energy supply.

For this reason, the amendments proposed in the *Telecommunications Act 1997* to institute obligations on the Australian telecommunications industry to protect their networks from unauthorised interference reflects the critical nature of telecommunication services and recognises that certain critical national infrastructure sits within the private sector.

Concluding remarks

In conclusion, I would like to reinforce our support of the Australian Government's intention to ensure our ability to respond to national security keeps pace with rapid developments in technology. We would be very happy to elaborate further on any of the issues raised in this submission and to share the results of our Unisys Security Index and Unisys Consumerisation of IT research in more detail.

We also invite you to visit the Unisys Security Innovation Centre in Canberra. The Centre is a working demonstration centre and test lab that brings together the best minds from the private, public and education sectors in the interests of better cyber-security solutions for Australia and our community.

Yours sincerely,

John Kendall
Security Program Director, Asia Pacific
Unisys