UNCLASSIFIED

THE HON NICOLA ROXON MP

Attorney-General
Minister for Emergency Management

SPEECH TO THE SECUIRTY IN GOVERNMENT CONFERENCE: PROTECTIVE SECURITY – POLICY IN ACTION

*****CHECK AGAINST DELIVERY*****

TUESDAY 4 SEPTEMBER

Acknowledgements

Thank you Mike (Mike Rothery, First Assistant Secretary, National Security Resilience Policy Division, Attorney-General's Department)

- Roger Wilkins AO, Secretary, Attorney-General's Department
- Security industry leaders and suppliers
- Ladies and gentlemen.

Introduction

It's great to join you for this year's Security in Government Conference, my first as Attorney-General.

SIG is considered to be Australia's premier event on protective security, becoming very well established since its first gathering in 1987.

That was certainly a different era.

I was studying law at the University of Melbourne. And one of the most popular TV shows at the time was *LA Law*. While it wasn't necessarily an accurate portrayal of the law or of legal proceedings, it was entertaining.

I remember in one episode a teenage computer hacker was hired to fix the law firm's phones. I thought the story line was intriguing. Could he really be trusted?

I must admit, I don't recall how the story played out. But I did do a bit of research and was amused to find the episode was written by *Anonymous*. And I think that's enough said about that…

I've also been informed that '87 was the year the first mobile phone call was made in Australia. Today there are more than 29 million mobile phone and internet services in operation in Australia.

Times have certainly changed.

And in terms of national security, we have had a major shift.

We're no longer just dealing with guards and gates, bombs and bullets when we talk about defending our nation and its secrets. We're now fairly and squarely working in an online environment. And this has created a whole new dimension of both opportunity and threat.

What's more, the security issues we faced in '87 are still around – but the tools and techniques are so much more sophisticated. For example, the actions of trusted but covert insiders are still harmful and expensive. But the damage they can now cause in a short space of time is enormous.

Both the private and public sectors have suffered from attacks from insiders and outsiders. And while this conference is focussed on security for government, I believe there are a lot of shared lessons for the private sector.

Identity crime is also an issue that plagues governments and businesses – and worries consumers too. And, nowadays it is one of the fastest growing offenses in Australia. The online environment has not only allowed it to increase – but also to become a key enabler of serious crime.

The threat from within

Just as national security threats have changed, so has the business of government.

We now do more work online. But so do criminals and terrorists.

We hold more information than ever before. This information is not only Government information but it is often personal information of Australian citizens. The responsibility we have to protect that information is immense.

Because the information is now stored online it is also accessible to potentially more people within an agency – increasing the risk of insider threat.

Of course, all organisations – both government and private sector – are susceptible to this risk.

It is interesting though that most people think about national security risks to Government as outsiders hacking in.

And, therefore much of the media and public commentary has focussed on the Government's work to build a strong capacity to protect ourselves from outsiders.

While this is important, the Government recognises that if we do not also prepare for the risk of insider threat we leave ourselves exposed. And so now, we're turning up the heat on our own systems to ensure we're secure from insiders who might have the ability and access to threaten our national security.

One of the ways we're doing this is through the new Protective Security Policy Framework.

The Framework supports the broader definition of national security – enhancing an agency's information, personnel and physical security – and it's been specifically written with an eye on the online environment.

Significantly, the Framework marks an important shift from a compliance based model to a risk management approach, providing guidance on how to identify risks, as well as the controls needed to mitigate them.

People represent the greatest asset of any organisation. And good organisations recognise the value of their people and it's why we see billions of dollars spent every year in training and development.

This is true for both the public and private sectors.

But, we have to accept that one of the greatest risks we face comes from personal error or the behaviour of staff. Criminals know this and they exploit it.

Staff can be confused, exploited or corrupted into providing access to systems. This can be deliberate or accidental.

Combined, human factors and the online environment can create a very serious security threat.

Social engineering is an active tactic used to commit online crimes. Every day, people are lulled into a false sense of security by emails, websites, or identity documents that have been crafted to look familiar and legitimate.

As well as social engineering, unwitting actions or inactions can also lead to a breach of security. This is often reflected in agencies that have a poor security culture.

And it's why the Government is leading the way in protective security policy and action.

To address the risks that could rise from a trusted insider, we need to emphasise the importance of security vetting, contact reporting, and ongoing monitoring of our employees' suitability to access information.

This means continually reinforcing the security awareness message – which is integral to the Protective Security Policy Framework.

Highlights of the protective security policy framework

There are some specific highlights of the framework that I'd like to note. To start, it's in line with key legislation.

It gives effect to the Crimes Act by describing information that should not be divulged to third parties.

The new markings for sensitive but unclassified information also align with categories of sensitive information in the Privacy Act. This provides agencies with a way of distinguishing between business-as-usual information, and sensitive information that needs to be safeguarded – such as citizens' data.

For individual public servants, the message of the Framework is this: You are entrusted with valuable and personal data of Australian citizens and they expect you to treat their information sensitively and with the respect it deserves.

The framework also aligns with the Freedom of Information Act.

Under FOI, information should be made available to the public except where disclosure would be detrimental. The framework provides guidance on assessing whether the release of information is detrimental and if so, how to protect it.

Another highlight is that while the Framework applies to Australian Government agencies, it can also be used by business to manage the security of day-to-day operations.

It's based on international best practice and has smoothed the way for greater information sharing between the public and private sector, where appropriate.

By now, each Australian Government agency has adapted their policies to reflect the new protocols. And as of 1 August, the phasing out of old classifications has begun.

Putting the framework into practice also requires a cultural shift in each agency. Security practitioners, managers and agency heads all play a part in this process.

I know my Secretary Roger Wilkins has been very involved in engaging with his colleagues in this regard, and you've heard from him just now about his priorities to promote a culture of security in government.

As such, I won't go into further detail on this work. Rather, I would like to note other action we're taking to help protect against internal risks.

Protecting against corruption

Earlier this year, the Minister for Home Affairs and Justice, Jason Clare, announced the next stage in reforms to crackdown on organised crime and corruption within Government.

Because of the nature of their work, officers in law enforcement agencies are targeted – and turned – by criminals.

We know this occurs – and we are weeding it out.

That's why the role of the Australian Commission for Law Enforcement Integrity is being boosted.

The resources allocated to ACLEI to oversee the Customs and Border Protection Service have been doubled. Legislation will also be introduced to allow ACLEI to work with the AFP, Australian Crime Commission, and Customs and Border Protection to conduct targeted integrity testing of staff in those agencies. And we will double the number of agencies ACLEI oversights, to include AUSTRAC, CrimTrac, and staff with border compliance responsibilities in the Department of Agriculture, Forestry and Fisheries.

These reforms will not only improve operational efficiency and information management – they will also ensure that corruption risks are mitigated and minimised.

Striking a balance

Another area the Government is working hard in, is the area of privacy.

This Government has taken active measures to provide a robust, predictable and transparent privacy framework that all Australians expect.

Reforms to the Privacy Act will enhance the protections already in place to ensure that, regardless of changing technology, personal information remains secure.

You should also be aware that the proposed national security reforms that have received significant media coverage also propose a strict privacy regime that ensures information is only used when necessary and used according to the law.

But there's more to this story.

To keep pace with the online environment, we also need to make sure our police, security and intelligence professionals are properly equipped to do their work.

That's why I have referred this package of national security reforms to the Parliamentary Joint Committee on Intelligence and Security.

Key areas for consideration include:

- A modern regime for lawful access to telecommunications to ensure that vital investigative tools are not lost as telecommunications providers update their business practices and begin to delete data more regularly and more Australians communicate online in a wider variety of ways
- Whether the Government needs to obligate the Australian telecommunications industry to protect their networks from unauthorised interference because more is being done online than ever before
- An authorised intelligence operations scheme for ASIO officers – so that ASIO officers are afforded the same protection from criminal and civil liability for authorised operations as AFP officers are afforded now.

I want to strike a balance between ensuring we have the investigative tools needed to protect the community and individual privacy. This includes protecting individuals from activities that deeply affect their privacy, including hacking and identity theft.

As you will be aware, there has been a lot of press coverage about one component of the reforms – and that is data retention.

Many investigations require law enforcement to build a picture of criminal activity over a period of time. Without data retention, this capability will be lost.

Many of you will recall the disturbing murder of Cabramatta MP John Newman in Sydney in 1994. Call charge records and cell tower information were instrumental in the investigation and subsequent conviction on Phuong Ngo. These records allowed police to reconstruct the crime scene.

The intention behind the proposed reform is to allow law enforcement agencies to continue investigating crime in light of new technologies. The loss of this capability would be a major blow to our law enforcement agencies and to Australia's national security.

Apart from data retention there are a number of other aspects to the proposed reforms, focussed on modernising our laws.

Gone are the days when we relied on landline phones, the odd fax or two and mail to keep us all connected. Smart phones allow us to engage with people in our workplace and across the world.

Criminals and terrorists have also benefited from this leap in technology. Our police and national security agencies must be backed by solid legislation, to ensure we are all protected and that criminals can be prosecuted.

And it's not only about strangers contacting your kids on the internet.

It's also about protecting the layers of hidden technology driving society like power, water and transport, banks and hospitals.

Another part of the reform focusses on the management of these security risks in the telecommunications sector. Telecommunication networks are critical infrastructure that hold personal data and is an increasingly attractive target to unwanted intrusion.

And, our process is open.

Unlike the Howard Government, I didn't want to blindside the Parliament and the Australian people by introducing national security reforms into Parliament and rush them through without good advice and public scrutiny.

The Government is putting all options on the table so the Australian public, experts and politicians can engage in this important national debate.

That process has already started with more than 170 submissions from people and organisations of all walks of life having their say.

This will ensure the Government has advice from the experts and will be informed by community views, before making final decisions on these important reforms.

I do want to reaffirm the intention of these reforms. We cannot live in a society where criminals and terrorists operate freely on the internet without fear of prosecution. We cannot allow technology to create a 'safe haven' for criminals, or a 'no go' zone for law enforcement.

But, this does not mean unfettered access to private data either.

What it does mean are carefully drafted, tested and oversighted national security laws – and this is what I'm focussed on delivering.

Identity crime

Identity crime is another threat we need to address. This is a challenge for governments, for businesses, and for individuals.

The Government recently commissioned a survey to gauge the community's experience and concern about identity theft and misuse. And the findings are now in.

They actually reinforce what we've known for a while – that identity crime is a real and very serious issue. It appears to be affecting more Australians directly and indirectly.

One in four people reported they had been a victim or had known someone who had been a victim of identity theft.

The effects of these crimes included wrongful impersonation, lodging false tax returns, and falsely claiming benefits.

The findings also showed that nine out of ten people are concerned about identity crime.

So what does this mean for Government?

It tells me there is still more work to be done to prevent identity crime and restore community confidence.

To date, we have established the Document Verification Service. The Service essentially puts out of business those who try and pedal fake identify documents as it confirms details on key identity documents such as passports, driver licenses and birth certificates.

Currently the Document Verification Service is being used by government agencies like Centrelink, the Immigration Department and state agencies like the New South Wales Roads and Traffic Authority.

But, we know that organised criminal groups use false and stolen identities to access prepaid mobiles and banking services anonymously.

So as of next year, the financial and telecommunications sectors will also be able to access the DVS to check Commonwealth identity documents, such as passports and visas.

This is an exciting step forward that the Government is taking to help the private sector better protect the identity of their customers and I look forward to the private sector signing on as the service becomes available.

Conclusion

At this point, it's timely for me to wrap up and say thank you to the many dedicated professionals who also play a part in securing the nation.

Since 1987 when the first of these conferences was opened, the world of security for government, for business and for private citizens has changed remarkably. Importantly, the Government has prioritised constant renewal of our security to protect ourselves against outsiders and insiders who seek to damage us.

As Attorney, my focus is to ensure that Australia is on the front-foot to fight criminals and terrorists who seek to hide their crimes behind new technologies.

The Protective Security Policy Framework, beefing up the responsibilities for ACLEI, our review of national security laws and the Document Verification Service are just some of the examples of the current efforts in this area.

I want to ensure that Australians can use the internet for business or pleasure with confidence and not be afraid of who is lurking behind the bright and glossy veneers of the latest new web craze.

That's what our reforms are about.

And in pursuit of these reforms, I will focus on delivering the right checks and balances to ensure that national security powers are not abused and that the privacy of Australians is respected.

I hope you enjoy the rich program that's on offer today and tomorrow – and I look forward to hearing about the issues discussed. It's now my pleasure to declare SIG 2012 officially open.