Australian Government
Australian Security Intelligence Organisation

ASIO

DG's Opening Statement

Thank you, Chair.

Australia's threat environment is complex, challenging and changing.

In terms of threat to life, the terrorism threat level remains PROBABLE, and unfortunately it is unlikely to be lowered in the foreseeable future.

Right now, ASIO is aware of multiple religiously motivated violent extremists who want to kill Australians.

Groups such as the ISIL continue to urge attacks, battle hardened foreign fighters could return to Australia, and fourteen Australians convicted of terrorism offences will reach the end of their prison terms over the next five years.

At the same time, our investigations into ideologically motivated violent extremists such as racists and nationalists are approaching 50% of our onshore priority counter-terrorism caseload.

This reflects a growing international trend as well as ASIO's decision to allocate more resources to the threat.

The growth of ideologically motivated violent extremism is concerning and challenging, but it is important to put it into context.

Religiously motivated violent extremism remains our most serious terrorist threat. The two terrorist attacks inflicted in Australia last year were both inspired by ISIL.

ASIO's job is to distinguish between talk and intent, belief and capability, ideology and action.

In terms of threats to our way of life… attempts at espionage and foreign interference remain unacceptably high.

Australia's adversaries are trying to steal our secrets, undermine our sovereignty and interfere in our democratic institutions.

We continue to see multiple espionage and foreign interference attempts from multiple countries.

This is the context to the recent and welcome investment in ASIO's sensitive capabilities.

To secure Australia and protect its people, ASIO needs to be able to do things our adversaries think are impossible.

We must out-imagine and out-maneuver sophisticated foreign adversaries that are effectively unconstrained by law, ethics and resources.

We must detect and defeat extremists who are acutely security aware and tech-savvy.

Once an adversary knows what we can do, we need to do new things they consider impossible. There is no set and forget in security intelligence.

That is why ASIO will sometimes ask for investment for new capabilities, or legislative change. We don't do it lightly, we do it because we need to keep technology on our side, not on the side of our opponents

The challenge for ASIO is that our adversaries are using technology to our nation's disadvantage.

We are seeing an exponential uptake of encrypted and secure communication platforms by spies and violent extremists. Even supposedly unsophisticated targets are routinely using secure messaging apps, virtual private networks, fake emails and number generators to avoid detection.

Encryption is fundamentally a force for good. As a society, we need to be able to shop, bank and communicate online with confidence.

But even a force for good can be hijacked, exploited and abused. In the case of encryption, we need to recognise how it is being used by terrorists and spies.

End-to-end encryption is degrading our ability to protect Australia and Australians from the gravest of threats.

My counterpart at MI5 was recently quoted saying that end-to-end default encryption will effectively give some of the worst people in our society a “free pass” by allowing them to plan their crimes in secret.

He is right.

Through their use of encryption, social media and tech companies are, in effect, creating and maintaining a ‘safe space’ for terrorists and spies.

It’s extraordinary how corporations that suck up and sell vast amounts of personal data without warrant or meaningful oversight can cite a “right to privacy” to impede a counter-terrorism investigation by an agency operating *with* a warrant and rigorous oversight.

I should stress that ASIO enjoys valuable relationships with the overwhelming majority of companies.

Our partnerships are crucial enablers of our operations.

Encryption is just one of the technical challenges we are dealing with. It is well known that ASIO can "collect the dots". The new investment will allow us to better *connect* the dots.

More data was created in the last 2 years than the rest of human history. We need to be able to sift through it to find patterns and linkages of security concern. Given the volume and complexity of data, we are not searching for a needle in a haystack, we are searching for a needle in a hayfield.

This is *not* mass surveillance. Quite the opposite. It allows us to be more targeted and proportionate.

The security threats facing Australia are significant, enduring and evolving. But so is ASIO's ability to deal with them. Agility and ingenuity are at the core of our business. Our clever, curious people are constantly honing their abilities and capabilities to ensure we continue to keep Australia and Australians safe.

I look forward to your questions.