INTELLIGENCE AND SECURITY COMMITTEE FINANCIAL REVIEW - INTRODUCTORY NOTES

3 December 2013

Opening Statement by Director, Government Communications Security Bureau

I would like to start by taking a few minutes to set out for the Committee the 2012/13 year, and look at the way ahead from the Bureau's perspective, and then I'm happy to take questions.

Firstly, as noted by the chair and by Dr Tucker, this is the first Financial Review of the intelligence agencies to be heard in public. We see this as a positive step toward providing greater transparency and understanding of how our organisations are managed.

Having the hearing in public forces us to think hard about how much we can talk about. That is a healthy exercise as we are trying to explain more about what we do and why, and hopefully provide greater understanding about the value we deliver for New Zealand.

As the Annual Report makes clear, the 2012/13 year was dominated by the recognition in September last year that support for a police operation the previous December and January was unlawful. We are still dealing with the consequences of that breach, and will continue to for some time yet.

Internally within the Bureau, Rebecca Kitteridge's review has led to a significant internal change programme to strengthen legal and procedural compliance.

Externally, the same events led Government to conclude, as the Kitteridge review did, that the Government Communications Security Bureau (GCSB) Act 2003 as it then stood was fundamentally not fit for purpose.

Government amendments to the legislation took effect on 27 September 2013.

The Bureau's management team and structure have been strengthened. Our top and middle management layers are now substantially stronger and more diverse in talent and experience than was previously the case. This investment is already beginning to pay dividends as the legislative and review implementation processes unfold; the Bureau is also now beginning to turn its mind to its operational strategies and priorities for the coming period.

After the past 15 months or so, a lot of the changes that we are making are addressing issues raised by staff in a climate survey.

One of the recommendations from the Compliance Review is that we ensure compliance with all relevant legislation, not just the GCSB and Oversight Acts. We

have been reassured by the advice we have received about compliance with the Equal Employment Opportunities Act and the Public Finance Act. We have reviewed our Privacy Policy and a draft is out for consultation.

It's clear that, having put strengthened compliance, oversight and policy processes in place, the Department needs to look afresh at its delivery of both information assurance/cyber and intelligence products to government. This reflects the changing environment within New Zealand and externally, and the resource pressures faced by all government departments.

Our thinking about this is being informed by the first Performance Improvement Framework (PIF) review for the core New Zealand Intelligence Community. We have also undertaken a survey of our customers, as we identify ways to improve our service delivery. Looking forward, we are working on a series of product and service improvements which will reflect the feedback that this survey and the PIF review will provide for us.

The combination of the customer survey and the PIF review is a valuable foundation for improvements. Taken together with the compliance, policy and legislative reform, the result is an opportunity for the Department's products and service to reflect the security and intelligence environment which New Zealand faces now and into the future.

I am pleased to have started this work that has a more outward focus, with a view to better meeting government priorities and customer needs within the robust compliance framework I have set out.

The environment continues to present a number of challenges, including:

- The rapid take up of advanced digital services using Internet protocol-based networks has led to an explosion in economically valuable services offered and delivered over the Internet. It has also led to an explosion of opportunity for cyber borne espionage, crime and, increasingly, aggression.

- New Zealand's open economy, and growing economic engagement with emerging markets in the Asia Pacific region mean that New Zealand's security interests and its economic interests are not automatically the same; this puts a premium on providing government with strong information assurance and cyber defence, and on the development and deployment of effective security and intelligence capabilities to enable New Zealand to identify, advance and defend its interests in a more complex and less stable global, political and economic environment.

- These challenges extend increasingly across New Zealand's economy and society, as these issues apply almost as significantly to major economic actors as they do to the mechanisms and information requirements of government itself.

Against these challenges, the Bureau needs to continue to work hard to develop a combination of compliance, customer focus and delivery, and constant adaptation to a rapidly evolving operating environment.

The Bureau now has a good understanding of these issues, a strong team in place, and a growing sense of how to tackle these challenges in the years ahead.

I would like to conclude by making some observations about the value of intelligence.

Here, it's important to start by making clear what we're not and what we don't do.

We're not executive. We protect New Zealand's information as best we can and we uncover information that is intended to help foreign policy and defence.

That means the value of what we do lies in the information protected, and in our foreign policy and the safety and effectiveness of our armed forces. Intelligence and information protection is an input, but not itself an end product.

Against that, it is genuinely hard to point to a simple arithmetic calculation of value. But equally New Zealand governments have understood the value of intelligence for decades.

And there is daily evidence of foreign interest in wanting access to our information clandestinely. If we have secrets which are worth stealing, they're worth protecting.