2 May 2017

Committee Secretary
Joint Committee of Public Accounts and Audit
PO Box 6021
Parliament House
Canberra ACT 2600

E-mail: jcpaa@aph.gov.au

Dear Madam/Sir,

Cybersecurity Compliance – Inquiry into Auditor General's Report 42 (2016-17)

Chartered Accountants Australia and New Zealand (Chartered Accountants) welcomes the opportunity to provide a brief submission regarding the Auditor General's Report 42 concerning cyber security compliance.

The Auditor General's report encompasses the Department of Human Services, the Australian Taxation Office (ATO) and the Department of Immigration and Border Protection.

Our submission focuses exclusively on the ATO and cyber security.

Who we are

Chartered Accountants Australia and New Zealand is a professional body comprised of over 120,000 diverse, talented and financially astute members who utilise their skills every day to make a difference for businesses the world over.

Members are known for their professional integrity, principled judgment, financial discipline and a forward-looking approach to business which contributes to the prosperity of our nations.

We focus on the education and lifelong learning of our members, and engage in advocacy and thought leadership in areas of public interest that impact the economy and domestic and international markets.

We are a member of the International Federation of Accountants, and are connected globally through the 800,000-strong Global Accounting Alliance and Chartered Accountants Worldwide which brings together leading Institutes in Australia, England and Wales, Ireland, New Zealand, Scotland and South Africa to support and promote over 320,000 Chartered Accountants in more than 180 countries.

Chartered Accountants Australia and New Zealand
33 Erskine Street, Sydney NSW 2000
GPO Box 9985, Sydney NSW 2001, Australia
T +61 2 9290 1344 **F** +61 2 9262 4841

charteredaccountantsanz.com

We also have a strategic alliance with the Association of Chartered Certified Accountants. The alliance represents 788,000 current and next generation accounting professionals across 181 countries and is one of the largest accounting alliances in the world providing the full range of accounting qualifications to students and business.

Digitalisation

The digitalisation of the ATO is a major part of its Reinvention strategy. The 2015-16 Federal Budget provided the ATO with additional funding to reduce red tape and to simplify compliance by making digital interaction the main mechanism for taxpayer engagement with the ATO. The Government rightly expects a good return on its investment.

Greater digitalisation has the ability to generate efficiencies for taxpayers, tax agents and the ATO and allow tax policy-makers access better data analysis. However, these benefits could be eroded if privacy and security are compromised. The community's confidence needs to be maintained in the way our tax system works.

This means cybersecurity is not just an internal ATO issue: it is also an issue for everyone who interacts with the ATO. Such interaction goes well beyond dealings with taxpayers and their agents.

The ATO is obtaining electronic data from an ever increasing range of sources. This data allows the ATO to pre-fill income tax returns and undertake data matching. Increasingly, tax data is being shared not just with other domestic agencies, but also across borders between tax regulators.

Much of this data is obtained directly from taxpayers, but much also comes from financial institutions under the Commissioner's extremely broad information gathering powers.

The ATO also deals electronically with tax agents.

Soon, additional data streams will come online, such as Single Touch Payroll and through the greater adoption of E-invoicing.

This wide variety of sources of data provided to the ATO increase substantially its vulnerability to cyber-attacks, particularly where the data triggers entitlements to tax refunds.

There is also a growing incidence of criminal behaviour which seeks to trick Australian citizens into thinking they are dealing with the ATO, particularly ATO debt collectors.

Cyber-security working group

The Auditor General's report mentions several times that the ATO has insufficient protection against cyber-attacks from external sources.

We cannot speak for the internal workings of the ATO, other than to note that there exists a Security Committee within the organisation and we understand that the ATO regularly identifies and defeats cyber-attacks.

Our interaction with the ATO on this topic arises mainly via the Cyber Security Working Group[1], which Chartered Accountants ANZ Co-Chairs.

[1] CSWG. Its first meeting was on 16 March 2016

One of the aims in establishing the CSWG was to address the future role of tax agents and software developers in reducing the threat of cyber incidents (both for the ATO and users of ATO online services).

The group was established partly as a result of a SWAT analysis prepared by Chartered Accountants ANZ which highlighted the common cause that all participants in the tax industry had in addressing this issue. This SWAT analysis can be provided to the Committee on request.

As a result of the efforts of the CSWG, the ATO has recently released the following documents:

- Top cyber security tips for businesses - Tips on how to keep your business and client data safe from hackers and identity thieves.
- Top cyber security tips for individuals - Tips on how to keep your information secure and how to protect your identity details from being stolen and used to commit fraud and other crimes.

The CSWG is well aware that more can be done. Our next projects include:

- Guidance for tax professionals on how to seek assistance from the ATO (and other agencies such as IDCare) if a cyber incident occurs
- A response plan for the commencement of the Privacy Amendment (Notifiable Data Breaches) Act 2016

Cyber security strategy

At a broader level, we note that the government has recently released its first annual update of its cybersecurity strategy and the Australian Stock Exchange has also released a cyber health check for ASX 100 companies.

The annual update of Australia's cyber security strategy notes that "it has become clear since the launch of the Cyber Security Strategy that more needs to be done to support the cyber security capacity of Australia's small and medium businesses."[2]

That is particularly true for tax agents, many of whom themselves are small-medium businesses.

Chartered Accountants already provides our members with some training on cyber security.[3] However, at a broader level, we think it is time to consider incorporating basic cyber security requirements and health checks into the tax agent accreditation process that is administered by the Tax Practitioners Board to assist the ATO in its endeavours to adequately protect privacy and data. We appreciate that this may be regarded by some tax agents as additional red tape, but if implemented well, this measure could protect the tax agent's business as much as it protects ATO systems from attack.

The ATO may raise the bar on cyber security

Whilst the ATO is actively encouraging taxpayers to deal with it online, and requiring tax agents to do so, there is nonetheless a fear that data transmitted to the ATO may somehow circumvent ATO safeguards and allow the entry of malware which threatens the security of ATO systems.

[2] Page15 https://cybersecuritystrategy.dpmc.gov.au/cyber-security-strategy-first-annual-update-2017.pdf
[3] See http://www.cpdlive.com/charteredaccountants/seminars4/6583/8168/IntroductiontoCyberSecurity.html?Display__this=Y

These fears have led to some initial discussions within the CSWG about whether the licence to operate as a user of ATO online services should be accompanied by new conditions for users involving cyber security standards. This licence to operate would be separate and distinct from any new requirements which might be imposed by the Tax Practitioners Board on tax agents.

We stress that these discussions are at an early stage and it is hoped that the tax-related software used by businesses and tax agents will meet the minimum standards which may be specified by the ATO. In this regard, the Committee may wish to explore with organisations such as the Australian Business Software Industry Association how its members met and maintain compliance with Australian standards for relevant safeguards.

But even if the software meets minimum standards, the ATO may still require tax agents to agree to policies and procedures which help combat "humanware" issues. These policies and procedures would also presumably be required of businesses which deal directly online with the ATO.

The role of intermediaries in helping to protect regulators such as the ATO and consumers

Another "glass half-full" way of looking at the issue is for the Committee to examine the role which intermediaries such as tax agents can play in protecting the integrity of ATO systems and consumers.

Regrettably, we are all too familiar with reports of cyber-crime perpetrated against Australians by criminals pretending to be acting on behalf of the ATO. Both the ATO and the Australian Federal Police tell us that the sophistication of the technology used by these criminals (most of whom operate offshore) makes it almost impossible to stamp out the problem.

We think that the ATO has yet to fully explore with the tax profession the role that intermediaries can play in protecting consumers, and helping to ensure that "clean" data is transmitted to the ATO.

For example, an easy response to a fake ATO debt collector is for a consumer to say: "You should be talking to my tax agent. Go away".

And noting our comments earlier about minimum security standards for tax agents, a tax agent's systems for dealing with the ATO should be more secure than, say, a citizen's home based computer whose security safeguards are rarely updated.

There is also the opportunity for members of the accounting profession to adapt by gaining new skills which help keep business technology systems secure, perhaps as part of an accreditation system approved by regulators such as the ATO.

Accordingly, we think that this is an important discussion for the ATO and the tax professional bodies to have as, together, we explore what the future of Australia's tax system will look like.

***

Chartered Accountants Australia and New Zealand consents to this submission being made public.

I would be happy to discuss any aspect of our submission with you. I can be contacted on [redacted] or by e-mail at [redacted].

Yours faithfully

[redacted]

Michael Croker
Tax Leader Australia
Chartered Accountants Australia and New Zealand