Major Government Agencies Cyber Resilience Audit

To the Committee Secretary,

Cyber-Security is here to stay.

DHS genuinely took one step in the right direction – however bureaucracy is stopping it from being a world-class leader in the cyber-security domain.

Please allow us tell you why.

Firstly, QILA is a Canberra based cyber-security firm specializing in ethical cyber practices and cyber education. We have a track record of having worked with The Department of Human Services (DHS) in our previous incarnation in the arena of software security. In addition we have experience within DIBP, with some staff currently working there full-time.

We approached DHS to educate them on the need to build great software above and beyond the standard software development lifecycle (SDLC). We wanted to work with them to eventually reach a state where they are truly building great products and services that are fundamentally built upon the Secure Software Development Lifecycle (SSDLC).

We understood that within DHS there is a very large gap in terms of technical capability in the creation of cyber-secure software and associated systems. This is a non-trivial area of expertise. Having worked and built software inside the Department for over 4 years, we had amazing insights into their current practices and processes. We knew that every single member of staff needed a cyber-education to create a benchmark of awareness and facilitation.

To DHS's credit, we were able to educate approximately 50 staff members, in the first phase of software security. Our interaction was through the DHS learning center, which unfortunately is NOT staffed with decision makers, nor with any managers of sufficient technical expertise or desire to change or improve anything at all. QILA had no direct access to any of the people involved in security and it turned into a very frustrating exercise and so we have given up as we need to chase work we can actually win. The gulf was too wide to cross. We knew we could add immense value and yet as a local, Australia business we had no access mechanisms of any merit.

Australia has so much talent and expertise in cyber security, yet the bureaucracy of these large federal agencies will continue to result in sub-standard outcomes until the very best Australia has to offer can be brought into the fold. We happen to believe, that even with a small amount of tuning, that this is possible.

By way of summary, and to crystalize direct benefits and gains to DHS, ATO and DIBP, we state the following for the perusal of the committee:

Key Issues:

- Cyber security is seen as an ex-post facto exercise. This is completely the wrong philosophy
- Organization's like QILA cannot get a seat at the negotiating table. Australia has deep, world-class experts that are not being utitlized with organisations such as DHS due to the bureaucracy and lack initiative by these large Federal Departments.
- Secure software is a journey and not a destination. DHS severely lacks the skills to build world-class, secure software systems from the ground-up. This is not an opinion, and is true for the majority of the developers currently employed by both DIBP and DHS. Our agency has worked in both and we know their processes better than probably even the committee members themselves.
- The culture of learning – to be frank – in the public service – is dead.

Key Recommendations:

1. Federal Government Agencies need to re-ignite the passion for learning and self-improvement. Cyber awareness and knowledge will result as a secondary benefit
2. For highly technical areas of cyber security, we recommend an innovation hub be created that is NOT directly run by the Federal Government Agency. Rather it is formed from the commercial sector as an interest group. DHS, DIBP etc can be represented and therefore both sides of the equation are represented and allows for private enterprises to join the discussion and be partners in innovation. This needs to have genuine stakeholders and funding allocated to it to make sure it works
3. Bring in secure software experts, such as QILA, to provide training and an ongoing journey in the technical field of software security as well as build an on-going cyber security culture.

QILA would love the opportunity to future advance the discussion. We are ready to provide the basis for many of the recommendations above, as well as provide direct testimony and briefing to the ANAO committee on cyber resilience.