Chris Drake
CryptoPhoto.com Pty Ltd.
PO Box 988,
Noosa Heads, QLD, 4567

22nd August 2017

Submission to the 2017 Senate Inquiry:-

Circumstances in which Australians' personal Medicare information has been compromised and made available for sale illegally on the 'dark web'.

My name is Chris Drake. I am a computer security professional and expert with 35 years' experience, I have won numerous international cyber security and innovation awards, spoken at many international conferences on the subject of cyber security, run multiple security-related businesses, and I own several security patents, including the world's #1 most-cited cyber security patent of all time.

I respond to each term of reference in order:

a. any failures in security and data protection which allowed this breach to occur;

My understanding of the nature of the Medicare cyber incident and my long experience in programming secure software lead me to conclude that this was a simple mistake caused by a programmer not considering security implications while authoring software. Secure programming is vastly different from regular programming, and requires the author to "think like a hacker" at all times, considering exploitable conditions in every line of code written. Such an author would ideally hold excellent results from an "Ethical Hacking" course, to ensure they most fully understand the nature of the exploits their work will be subject to. This appears not to have happened.

Code should be reviewed, to ensure it is not exploitable, by an appropriately skilled person ("Ethical Hacker" at a minimum) – this too appears not to have happened.

Some form of professional system testing should be performed; assuming this was done, a blacklist needs to be established to prevent the persons who overlooked this oversight from being allowed to continue to participate in future security testing. This was an obvious and elementary mistake – there is no excuse for the person or firm reviewing security to have missed it.

b. any systemic security concerns with the Department of Human Services' (DHS) Health Professional Online Services (HPOS) system;

As I said in the previous section, failure to engage appropriately skilled programmers and reviewers, and failure to engage a reputable penetration systems testing team reveal systematic security failures within DHS/HPOS.

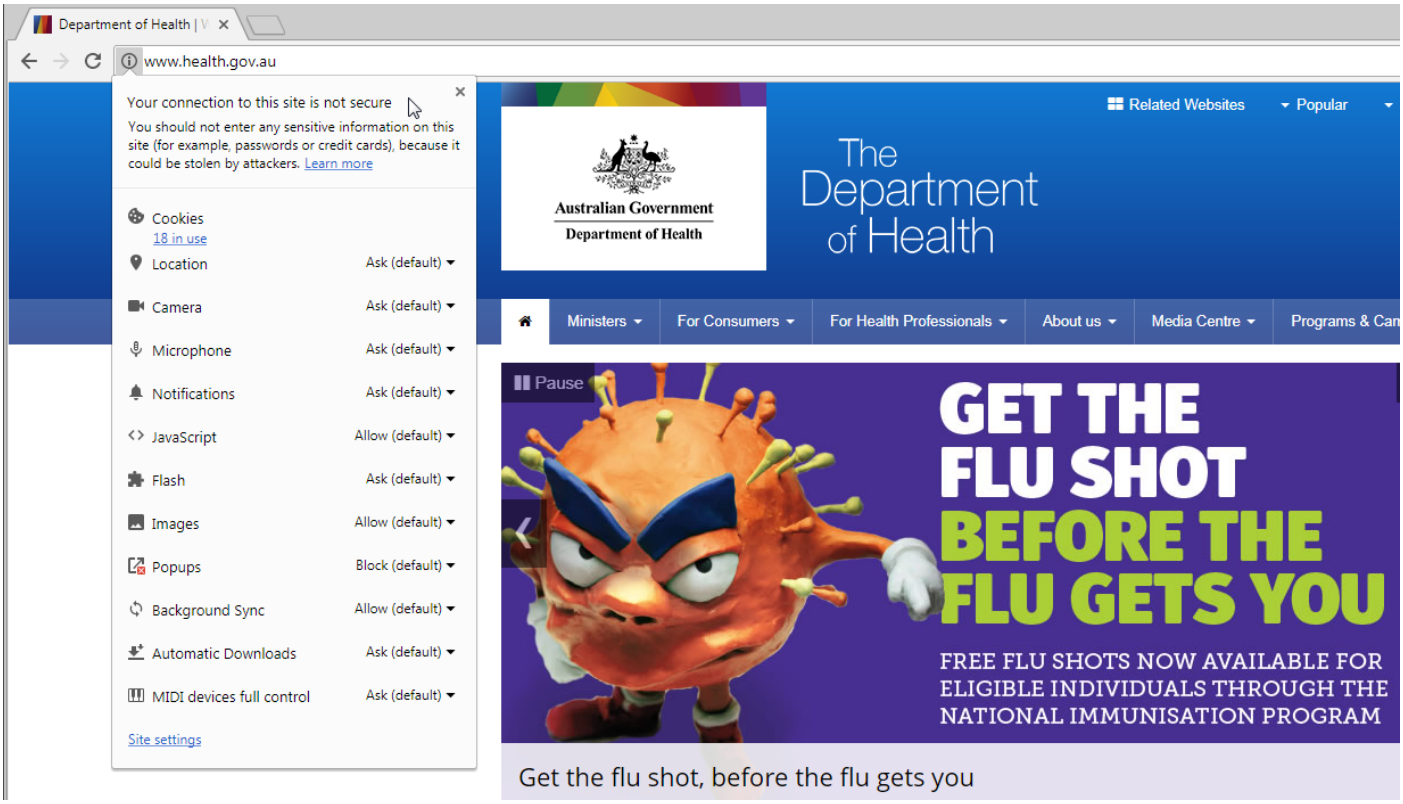
During a closed session with the ASD last year a private group of professional security engineers including myself were treated to a candid presentation on the state of cyber security within Australian Government. We were told that the ASD does not have power to compel government departments to deploy adequate security, and departments regularly choose not to take ASD advice regarding cyber-security. As a result, the ASD is extremely overworked, dealing with large numbers of cyber intrusions. The ASD told us that they do not have the time or

patience to encourage recalcitrant departments to take security seriously. The way the ASD deals with these departments, is to "let them get hacked", so they learn their lesson. This, in my opinion, is an unmistakably clear indication of systemic cyber security breakdown within government in general, and within DHS and HPOS in particular.

In my experience and observation, the vast majority of Australian Government online providers put "Security" as one of their lowest priorities in practice, and generally choose not to comply with security best practice or guidelines. When challenged on this, my experience is that the departments involved reply with untrue allegations of security compliance and other related PR material which does not reflect their true security practices. I have encountered a mixture of false representations from Government regarding security – some are probably innocent mistakes, while others have been knowing and deliberate deception along with refusal to acknowledge or repair serious security problems. There appears to be a culture of denial and cover-up with respect to cyber-security incidents in Australian Government.

There are 34 government websites relating to health or DHS listed on the A-Z directory. Only 10 of them use TLS (https://) security, and only 1 uses "hsts", an acknowledged best-practice mitigation against downgrade attacks.

Here is an example screenshot (taken today). Note the browser security warning that this site triggers:-



Somehow, nobody in government seems to notice or care that there is no security on the homepage. This, in my opinion, reveals a multitude of failures and lack of serious concern right across all government departments relating to Australian health care data.

c. the implications of this breach for the roll out of the opt-out My Health Record system;

In my opinion, this incident probably exacerbated public distrust of government competence, and gave fuel to future opponents of change. Opinion and fact usually differ: the **actual** public implication is probably nothing.

Besides the public however, this incident will have had an effect on staff. The media hype, and this inquiry are all serving to dramatically educate staff that they need to stop putting security issues last!

d. Australian government data protection practices as compared to international best practice;

International best practice is irrelevant. Australia needs adequate, if not outstanding, data protection practices, regardless of what the rest of the world might be doing.

As I mentioned earlier regarding the ASD – Australian Government departments rarely adhere to guidelines or follow best practices. Extrapolating from two ASD reports, one published last year, one the year before, there are, on average, 4 acknowledged successful cyber-intrusions into Australian Government computer systems every day of the year. The ASD also report that the average time to discovery of these intrusions exceeds 6 months, and in my experience (and also found in a UK report), the number of actual intrusions versus acknowledged ones is typically double.

Perhaps the best indication of just how badly policy does not match practice is here:-

The A-Z directory of government services currently lists 992 different web sites. Zero of them use best-practice security (TLS + HSTS + HPKP), only 51 of them (5%) use HSTS security, and 678 of those websites (68%) use no security whatsoever. This, incidentally, includes the AEC, which are currently running a TV campaign to encourage voters to enrol. At the time of writing, https://aec.gov.au/ has no secure server even available – only the insecure version works, also showing the same browser-insecurity warning (see screenshot previous page) to every user who loads this page. The Census was the same.

How is it possible, that in a cyber-aware country in the year 2017, we have our Government accepting citizen voter enrolments through a website with no working security? The sheer scale of failures right across the board that had to happen to allow this to be true is staggering. Every programmer, every designer, every reviewer, every tester, every pentesting company, all the PR and advertising people, and every single person who ever loaded the website and chose to ignore the browser security warning.

e. the response to this incident from government – both ministerial and departmental;

This inquiry is excellent, providing it causes someone to actually start taking security seriously, instead of just saying that they take it seriously.

f. the practices, procedures, and systems involved in collection, use, disclosure, storage, destruction, and de-identification of personal Medicare information;

I'm aware of several recent scholarly articles relating to re-identification of de-identified data. This is a very difficult problem which is probably not well (if at all) solved.

Timely and friction-free use and information disclosure to those who need it are very important to ensure best possible health outcomes; this is not well addressed in Australia. Security is nice, but not at the expense of our lives please. This is not a hard problem to solve – I encourage the department to seek industry solutions; the best quality and lowest-risk ICT solutions are the ones already in the marketplace – not the ones that freshly hired government employees design and build themselves.

g. the practices, procedures, and systems used for protecting personal Medicare information from misuse, interference, and loss from unauthorised access, modification, or disclosure; and

I addressed this in answer a. and b.

h. any related matters.

Data breach reporting, and breach event handling are totally dysfunctional in Australian Government. Broken systems rarely get fixed. Reports get ignored. Submissions to Inquiries sometime also never appear, and recommendations in them ignored too (e.g. my Census Inquiry submission) from last year, which covered much of the same ground as this submission again.

Yours sincerely
Chris Drake