

20th September 2017

Submission to the 2017 Senate Inquiry: **Digital delivery of government services.**

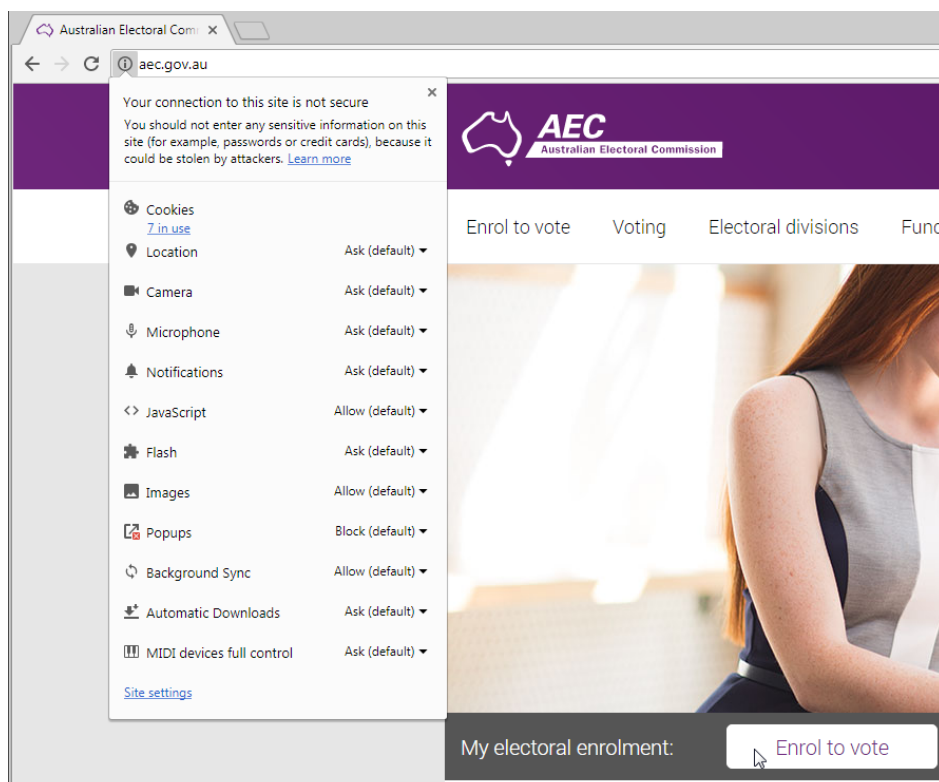
My name is Chris Drake. I am a computer security professional and expert with 35 years cyber experience, I have won numerous international cyber security and innovation awards, spoken at many international conferences on the subject of cyber security, I run multiple security-related businesses, and I own several security patents, including the world's #1 most-cited cyber security patent of all time. I have been closely involved with numerous recent government digital delivery services, in at least the following roles: tenderer, participant, user, observer, and reporter of security oversights. I travel regularly to government events relating to digital delivery and cyber security both within and outside Australia, and I am member and active participant in several working groups relating to security and digital service delivery.

I respond to each term of reference (shown below in blue) in order:

- a. whether planned and existing programs are able to digitally deliver services with due regard for:
 - i. privacy,

There is a marked difference between rhetoric and reality with respect to the claimed versus actual privacy practices of Australian digital government services. For example:-

The A-Z directory of government services currently lists 992 different web sites. Zero of these use best-practice security (TLS + HSTS + HPKP), only 51 of them (5%) use HSTS security, and 678 of those websites (68%) use no encryption 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 available – only the insecure version works, which shows the following browser-insecurity warning to every user who loads this page:



Without working encryption (e.g. TLS, aka SSL, aka “https://”) and some attempt to prevent it’s downgrade (e.g. HSTS/HPKP) little or no privacy protection at all is afforded to users. It is not sufficient to encrypt just some website pages (on account of downgrade attacks).

To be clear: 68% of government websites, including critical voter enrolment, as well as our recent Census (as I reported in my Census inquiry submission which was never published) offer no working privacy protection, while displaying an unmistakable “this site is not secure” warning to all users.

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 all those website and chose to ignore the browser security warnings – all of these people failed us.

The problem is far deeper than just mere privacy and security failures: our government also has no working mechanism to correct oversights, and no useful mechanism for reporting them – and certainly none that takes action. For example, I reported the Census security oversight soon as I noticed (12th August), and on approximately 50 occasions since then I repeated my report – I made contact via numerous public online feedback mechanisms, in public government forums, in response to the majority of newspaper reports on their web sites, in blogs, in security groups I am a member of, in person to the Australian Privacy Foundation, directly to The Australian Newspaper, and directly by email to at least 3 different government ministers, the Census themselves, Data61, Alastair MacGibbon, and Sen C. Ketter. No corrective action was ever taken.

Another example: I reported the lack of AEC security and received written acknowledgement of the problem more than a month ago. I also included in my report that I will be including the outcome of their action in this inquiry submission, to illustrate how reports are never acted on, and how privacy and security oversights are never corrected. As of this writing, my prophesy was accurate: no corrective action has been taken, and the AEC website is still insecure.

The former Digital Transformation Office (DTO) requested tenders (RFI DTO-197) from businesses to assist in the creation of a privacy-respectful digital identity service, after holding many meetings with industry affirming their support for both us and the principals of privacy. My company filed a comprehensive bid to strongly protect both the privacy and security of Australian citizens. We followed up with numerous oral, written, and electronic requests to meet and demonstrate our technology, and we built a working alpha demonstration to showcase our solution. As is well documented, the DTO, which then became the DTA, chose to reject all industry participation and refused to communicate with us, and to the best of our knowledge, all other tenderers. We made every feasible attempt to engage the DTO and DTA to show how to protect citizen privacy and security on the modern internet for their project, but we were completely ignored. I filed a FoI request after no tender submitters heard anything subsequent to the tender, and discovered that the report due to be written was never done. The Alpha identity project that the DTO wrote turned out to me a near complete failure. A second re-write, their “Beta” project, also turned out to be a complete failure, and as of time of writing, a new team has recently been hired to re-do this project (to discard all previous work and begin anew). These identity projects are notable for the fact that a very strong emphasis has been placed on the collection of biometric data from citizens, which has far-reaching and potentially catastrophic privacy consequences for all citizens. It is possible to offer privacy-respectful identity services with no biometric risks using appropriate technologies, however, this has never appeared on a their agenda.

By way of example: the DTO rhetoric clearly stated in early meetings that biometrics would NOT be used because they pose too great a privacy risk. In later reality, it became part of all the (private) projects they worked on, and all their work was carried out in great secrecy.

I also draw your attention to the discrepancy behind the rhetoric published by the DTA website (<https://www.dta.gov.au/blog/govpass-privacy-by-design/>), and the reality of their recent Privacy-Impact-Assessment (PIA https://www.dta.gov.au/files/DTA_TDIF_Alpha_Initial_PIA.pdf)

The DTA, under the heading "**How Govpass ensures privacy**" links to the above PIA which reports that their system **failed every single assessment criteria that they tested**, and inexplicably grants them a "compliant" mark on PIA provisions that the DTA somehow manage to convince the assessor **not** to test.

TDIF Component	Status	Notes
1. Mandatory policies and standards	Requires further review / action	
2. The Identity Exchange	Requires further review / action	
3. Identity Providers (IdPs)	Requires further review / action	
Is the data 'personal information'?	Requires further review / action	
APP 1 – Openness and Transparency	Requires further review / action	
APP 2 – Anonymity and Pseudonymity	"Compliant"	Declared out-of-scope (not tested)
APP 3 – Collection of solicited personal information	Requires further review / action	
APP 4 – Dealing with unsolicited personal information	"Compliant"	Declared out-of-scope (not tested)
APP 5 – Notification	Requires further review / action	
APP 6 – Use or Disclosure	Requires further review / action	
APP 7 – Direct Marketing	Requires further review / action	
APP 8 – Cross Border Disclosure	Requires further review / action	
APP 9 – Government Related Identifiers	Further action required	
APP 10 – Quality of Personal Information	"Compliant"	Incompleted section not assessed
APP 11 – Security	Further action required	
APP 12 – Access	Further action required	
APP 13 – Correction	Further action required	

It is clearly highly unreasonable and **deliberately deceptive and misleading** to label an internet web link that points to an assessment outlining absolute and complete privacy failure, with "How Govpass ensures privacy". This is just one of a great many examples I have observed of government saying one thing, **but doing the opposite**, when it comes to privacy and/or security online.

In conclusion: my considerable experience with government systems and programs shows that they typically choose to ignore privacy, they fail to adequately ensure protection of private data, they actively reject offers of outside help to improve privacy, and they never correct reported privacy issues, not even on critical systems. The foregoing are a mere fraction of the examples I can cite.

ii. security,

Many of my comments regarding privacy apply equally to security (security is, after all, a pre-requisite for privacy).

The following is an extract of my response to the Medicare inquiry:

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.

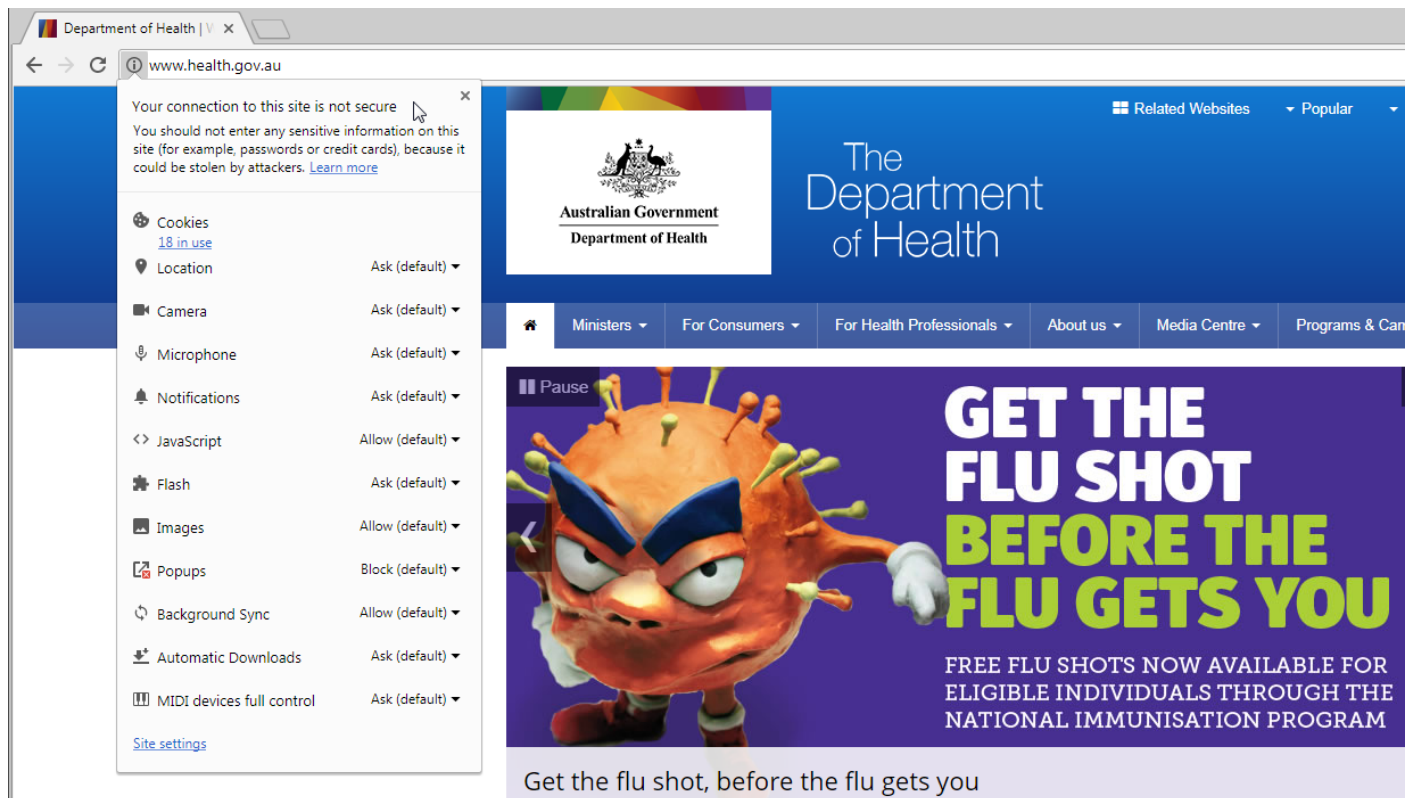
As I said in the previous section, failure to engage appropriately skilled programmers and reviewers, and failure to engage a reputable penetration systems testing team reveal systematic security failures within DHS/HPOS.

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 recent screenshot. 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.

I have been invited to participate in the Prime Minister's Advisory Council on Cyber Security Industry Working Group "Threat Blocking at the Network level", for which I am grateful and I believe I can provide great positive input, however, although I offered my services, I was excluded from the "Security Roundtable" from which this group evolved. We are now in the unfortunate position that an ineffective cyber-direction (network level) has become the scope, which (if not corrected, and in my experience, these never are) will put Australians at great future risk with practically no security benefits. Better effort needs to be expended to engage high-quality security professionals when seeking advice, and to vet their advice for (at least) common sense. The ASD has many extremely proficient experts; they would make an excellent adjudicator, if not participant, to ensure that advice provided to government is useful and sensible.

Vendors are typically considered "the enemy" in government threat-intelligence sharing. This insulting attitude needs to be corrected: we are the ones providing the solutions to these threats, and we are typically the foremost experts in our fields, and we typically understand the efficacy of our own, and competing, security products far greater than any other individuals. There is no point sharing intelligence, if there is an exclusion of solution providers to those problems! Yes, we make money fixing your problems, but this costs **at least** an order of magnitude less than the hacks that come when the problems are not fixed!

Our ASD produces many excellent security advice documents, however, in my opinion, much advice is heavily dated, and is not sufficiently ranked in order of threat importance.

Assorted government departments also produce security advice and run security programs like "Stay Safe Online Week". These are typically plain wrong (for reasons that take considerable time to explain; suffice it to say, many reputable studies exist showing that advice given is ineffective, if not outright dangerous and misleading). Typically, such advice appears to me as if written by a "junior" who perhaps spent an hour in google finding someone else's

(aged) advice to paraphrase. There appears to be no consideration to the efficacy of written government security advice provided, or any measurement of the results from giving it.

Some Government Privacy and Security statistics that I have collected include:

- Personally Identifiable Information (PII) has dominated the cybercriminals “most wanted asset” list for at least the last year.¹
- 62% of Australian cyber break-ins are to Government servers.² That’s 4 new ones every day.³
- The average time Australian Government takes to detect a break-in exceeds 6 months⁴.
- Break-ins at *other* web sites (non-government ones) facilitate government frauds too.⁵
- Getting it wrong is disastrous, especially when biometric data is stolen.⁶
- Phishing has been for years, and still remains, the top cause of break-ins.⁷ 15,000 Australians every day become infected with known malware.⁶ 40% of malware remains unknown and undetected for 2+ weeks, and 10% lives on for > 1 year. Phishing hits 1,000,000 Australians daily; 500 get hooked.⁸
- 68% of federal government web sites use no SSL⁹, and less than 5% use HSTS or HPKP.
 - There are 5.8 million public Wi-Fi hotspots in the world. This means that it is impossible even to start trying to secure the majority of government web sites (free Wi-Fi, among other things, lets attackers easily do anything they want on a non-SSL connection - including downgrade every attempt it might make to try and get secure).
 - HSTS and HPKP exist for a very good reason - but you can't use either without SSL to start with! That makes 678 federal, and thousands of other government sites where Australian users are totally exposed, and one-click away from completely undetectable identity theft.
- 66% of adults worry more about identity theft than anything else; theft, burglary, murder included.¹⁰

In conclusion: again, my considerable experience finds that government typically choose to ignore security, they fail to adequately deploy it, they actively reject offers of outside help, and they never correct reported issues, not even on critical systems. The foregoing are also a mere fraction of examples I can cite.

iii. quality and reliability,

My expertise lies in the domain of cyber-security and digital identity. In my opinion and considerable experience, there is a near-total lack of quality and reliability exhibited in public-facing government services in at least these two critical areas. Most of my foregoing examples demonstrate this.

There is also a near-complete lack of ability to cure poor-quality and unreliable services, with no action being taken when problems are reported.

¹ Source: Cytegit Intelligence Reports, Marc 2015 through March 2016: <http://cytegit.com/cytegit-intelligence-reports/>

² Australian Signals Directorate: www.asd.gov.au/publications/protect/cyber-security-picture-2013.htm

³ DPM&C page 16: <https://cybersecuritystrategy.dpmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf> (+37%) plus ref #2 above

⁴ From ASD presentation, and also <http://www.zdnet.com/article/businesses-take-over-six-months-to-detect-data-breaches/>

⁵ <http://www.smh.com.au/it-pro/security-it/five-hundred-tax-file-numbers-hacked-every-day-20151028-gklcx7.html>

⁶ U.S. Office of Personnel Management (OPM), Philippines Commission on Elections, US Voter Database, Turkish citizenship database, and similar hacks <http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

⁷ Australian Cyber Security Threat Report: https://www.acsc.gov.au/publications/ACSC_Threat_Report_2015.pdf

⁸ Adjusted to Australia-only: <http://www.getcybersafe.gc.ca/cnt/rsrscs/nfgrphcs/nfgrphcs-2012-10-11-en.aspx>

⁹ 87 of the 781 here: <http://www.australia.gov.au/about-government/departments-and-agencies/a-z-of-government-sites>

¹⁰ Source: <http://www.sileo.com/identity-theft-statistics-gallup-poll/>

Here are just a few of the government mega-failures that I'm aware of relating to just one topic: digital identity:

- Business Authentication Framework (2002): FAILED¹¹
- ATO Digital Certificates (2005): FAILED¹²
- AUSkey (2013-2016): FAILED^{12,13,14,15} "inflexible and cumbersome" - *ATO commissioner*.¹⁶
- ATO Authenticator 2016 (Auskey 4.0?). ATO's most recent security revelations are not encouraging¹⁷. Plaintext password databases, fake lock-out mechanisms, client-side-only checking, text email recovery...
- MyGov: here's their advice about what to do (disable it) when you need their security most (when you're travelling and in cyber-hostile territory)²⁶ :-



- DTO Digital Identity "Alpha" (2016) – total failure¹⁸.
- DTA Digital Identity "Beta" (2017) – total failure again¹⁹.
- DTA TDIF (2018) – to be seen: will Government learn their lesson? Perhaps it is time to dust off the TDIF tender responses, and let the industry experts with already-working solutions put them in place, instead of hiring yet another team of inexperienced amateurs to attempt to build such a complex solution?

In my experience, neither quality nor reliability is demonstrated in the majority of government services I'm involved with.

iv. value for money;

Again from my experience, there is extremely poor value for the money spent of the projects I watch. They are typically very expensive (tens of millions of dollars), and more often than not they are totally scrapped (never used – e.g. the TDIF).

Monetary value is not such a simple concept. Not only are the projects I refer to above still not operational after numerous total rewrites, they are more than a decade late, and their lack of delivery has caused vast direct losses from fraud (hundreds of millions of dollars), incalculable loss to citizens in the form of wasted time and effort, and massive cost escalations in government call centres. Their lack of existence has also created massive development duplication through local, state, and federal governments, and created serious barriers for future solutions to overcome, including loss of trust and vastly expensive retooling to replace the duplicitous interim systems built while waiting (decades) for the original (still not even started) delivery.

¹¹ Source: <http://www.itnews.com.au/news/third-time-lucky-for-atos-digital-authentication-176444>

¹² Mac: 2013: <http://www.smh.com.au/it-pro/security-it/apples-java-block-creates-a-tax-headache-20130211-2e7xe.html>

¹³ Windows IE: 2014: <http://news.softpedia.com/news/Internet-Explorer-Starts-Blocking-Old-Java-Versions-458303.shtml>

¹⁴ Chrome: 2015: <http://www.ghacks.net/2015/04/15/chrome-42-blocks-java-silverlight-other-plugins-by-default-now/>

¹⁵ Everywhere: 2016: <http://www.lifehacker.com.au/2016/01/oracle-finally-decides-to-kill-java-plugin-once-and-for-all/>

¹⁶ Source: <http://blog.cebit.com.au/john-dardo-ato-moving-toward-digitalisation-at-a-fast-pace>

¹⁷ Ghastly security record: <http://www.zdnet.com/article/the-taxpayer-funded-plain-text-password-store/>

¹⁸ In-confidence assessment from state government agency, plus <http://www.afr.com/brand/boss/promise-of-digital-government-diverted-by-tech-screwups-20170220-gupjw>

¹⁹ Phone call I had with interim DTA staff planning a complete restart

The DTA operates a “Marketplace” which makes it “easy” for government departments to bypass the tendering process and quickly hire staff for projects. The rates that professionals are paid for these projects is often listed on this site, and is typically 5 to 10 times higher than the expected industry pay rate (for example: \$500,000 p.a. equivalent salary for web designers – the national average for this role is \$54,000).

Much more serious than the egregious overpayment of contractors through this website, is the heavily one-sided service nature that it encourages. It is supposed to be the role of ministers to ensure that public money is spent responsibly, however, when there is no easy working mechanism to buy solutions from industry, but there is an easy way to spend vast sums of public money to hire contractors to create duplicate implementations of industry solutions, it’s clear how this is turning out: enormous wastage of public monies on failed and low-quality projects while Australian-Industry suppliers of high-quality, low-risk, working solutions are forced to move to the USA to find customers because Australian Government cannot (and/or will not) hire them.

b. strategies for whole of government digital transformation;

My recommendations are as follows:

1. Put security first. Immediately issue the cessation of all non-TLS websites on the .gov.au TLD. There is no excuse for zero security on any website; it’s completely free to set up.
2. Make it mandatory that every project considered, and contractor hired by government, is only commenced or engaged after a genuine attempt is made to source a working solution from Australian Industry for the solution that the project or contractor is to create. Working industry-built solutions are typically vastly superior in quality, much lower risk, and significantly less costly than anything built by contractors and government workers.
3. Seek advice from Industry and experts, and use the ASD to vet the advice, and discontinue engaging individuals found (by reputable experts like ASD) to be providing unsound advice.
4. Source Australian First. Many of the world’s best cyber solutions are built right here. Government should be using these, not least because they’re indisputably the best in their respective fields!

c. digital project delivery, including:

i. project governance,

Most of the projects I follow (DTO/DTA, TDIF, Marketplace) have been complete failures in my experience, and much of the work I observe (Census, Medicare) exhibits major flaws all attributable to total or near-total project governance breakdown.

ii. design and build of platforms,

Like above. Refer the TDIF PIA total assessment failure for example. It takes a very special form of complete design and build messup to manage to **fail every single assessed area** of a privacy impact statement!

The Marketplace is another excellent example: it was a year overdue, despite simply being “copied” from the UK, it never fulfilled the original design intent (it supplied only services, no products or solutions), and the promised “ideation platform” simply never arrived. The architects of the marketplace all recently resigned, suggesting that it will not ever deliver its intended outcome. The side-effect of this half-delivered failure is that agencies are now using this for the only thing it’s good for (hiring staff), which is costing up to 1000% more than accepted pay rates and causing government to compete against (if not destroy) local industry in their quest to re-invent the wheel and “build instead of buy”, with the majority of outcomes that I observe being total failures (entire projects scrapped and never used).

iii. the adequacy of available capabilities both within the public sector and externally, and

The ASD has outstanding capabilities, however, to the best of my knowledge, they are generally unavailable for government use, and are typically vastly over-worked and under appreciated. Advice they provide is routinely ignored, and any adherence to advice is typical minimal (e.g. only the “top 4” (out of 35) cyber-security recommendations get more than passing consideration).

From my observation, there is a serious lack of quality capability within the public sector to design, build, or deliver secure or reliable digital outcomes.

From my participation in numerous industry working and special-interest groups, there is a vast available pool of quality solutions and commercial service providers in Australia, adept at delivering quality, tested, working digital outcomes, however, there is no working mechanism for government to easily engage this talent, and at least within the DTA, DTO, and NSW and QLD state governments (in my experience), there appears to be no motivation to seek solutions, or to accept them when offered. As best I can tell, the public sector appears to operate a culture of “build it ourselves at all cost” and a near-total refusal to defer to industry experts on projects.

iv. procurement of digital services and equipment; and

The very topic of this item supports my earlier point. Government should NOT be procuring “digital services” at all, it should be procuring “digital outcomes”. Australian industry experts with working solutions should be used in preference to all other methods for attaining an outcome. At present, this appears to be extremely difficult for public servants: it appears to be far too easy to hire an overpriced contractor to build a dubious-quality solution, and far too difficult to buy a solution.

While I am aware of at least one world-leading Australian equipment vendor in my industry, I am not aware of any vendor achieving commercial success in Australia (100% of them move overseas to succeed). This suggests that Government’s equipment procurement procedures are deeply inadequate.

d. any other related matters.

There is no list of Australian cyber-security suppliers. There is the “ACSGN” – Australian Cyber-Security Growth Network, who are tasked with growing this industry, but have inexplicably refused on repeated occasions to seek out or survey who is in it. This problem needs to be solved – it makes no sense to try and grow this sector when you don’t accurately know who is in it!

It is too hard for smaller and niche-expert suppliers to do any kind of work with government. We are the innovation experts with the most up-to-date solutions, but are routinely excluded, overlooked, or ignored when it comes to assisting with delivery of digital outcomes for government.

QLD Government runs a program called “TWiG” – “Testing Within Government” – all governments should run something similar: I recommend that government and industry each submit proposals, and that equal numbers of each are regularly selected. This will deliver immediate business-building opportunities and job growth across all regions in Australia, while delivering high-quality low-cost rapid and innovative digital outcomes across many agencies.

To the best of my knowledge, my submission to the Census Inquiry was never read. I include it in its entirety on the following pages, in the hope that someone will take action before the next census, and we don’t have to endure a repeat of these security oversights again. It falls within the scope “a” (item “i” and “ii” at least) of this inquiry.

Yours sincerely
Chris Drake

Senator Chris Ketter
Chair, Senate Standing Committee on Economics
P.O. Box 6100
Parliament House
Canberra ACT 2600
economics.sen@aph.gov.au

Submission to the Senate Inquiry into the 2016 Census

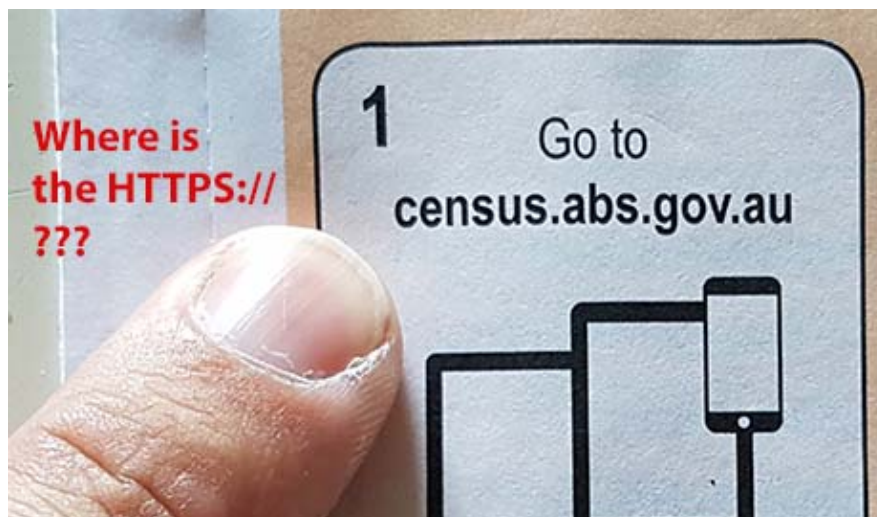
This submission covers technical security matters not present in existing submissions 1 through 90. It also covers procedural security failures again not mentioned in previous submissions. I address terms a, c, f, i and j in respect of the census web site security, and the wide ranging failure of every mechanism that should have prevented, mitigated, and repaired a glaringly obvious, critical security mistake thereon.

I am a computer security professional and expert with 35 years' experience, and volunteer firefighter.

The 2016 Census was insecure, and unsecurable:

1. Failure to implement TLS properly.

The acknowledged minimum-security standard for protecting web information is TLS (Transport Layer Security, formerly called SSL or Secure Socket Layer).¹ This is familiar to almost everyone – it is the “https://” in front of a URL; it is what almost all security advice (e.g. internet banking etc) tells end users to watch out for. The Census entry page had **no security**:-



Census forms (like the above), all links and references and publications that I observed and can find (physical and online) all failed to include TLS.

¹ E.g. Mitigation number 4, Information Security Advice for All levels of Government; Australian Signals Directorate, 2015
<http://www.asd.gov.au/publications/protect/cloud-security-tenants.htm>

It is widely known to all competent security professionals that “bootstrapping TLS” is an important security problem:² if you do not start from the beginning with security turned on, you cannot guarantee that security can be turned on thereafter, because the lack of initial security allows imposters/attackers/etc to downgrade all attempts to enable security.

There are mitigating technologies that exist to help overcome this problem (for the event where a careless user has accidentally entered a web URL and forgotten to type the “https://” prefix, or in this case, not been told to do that at the start).² HTTP Strict-Transport-Security response header (HSTS) and Certificate Pinning are two such examples.

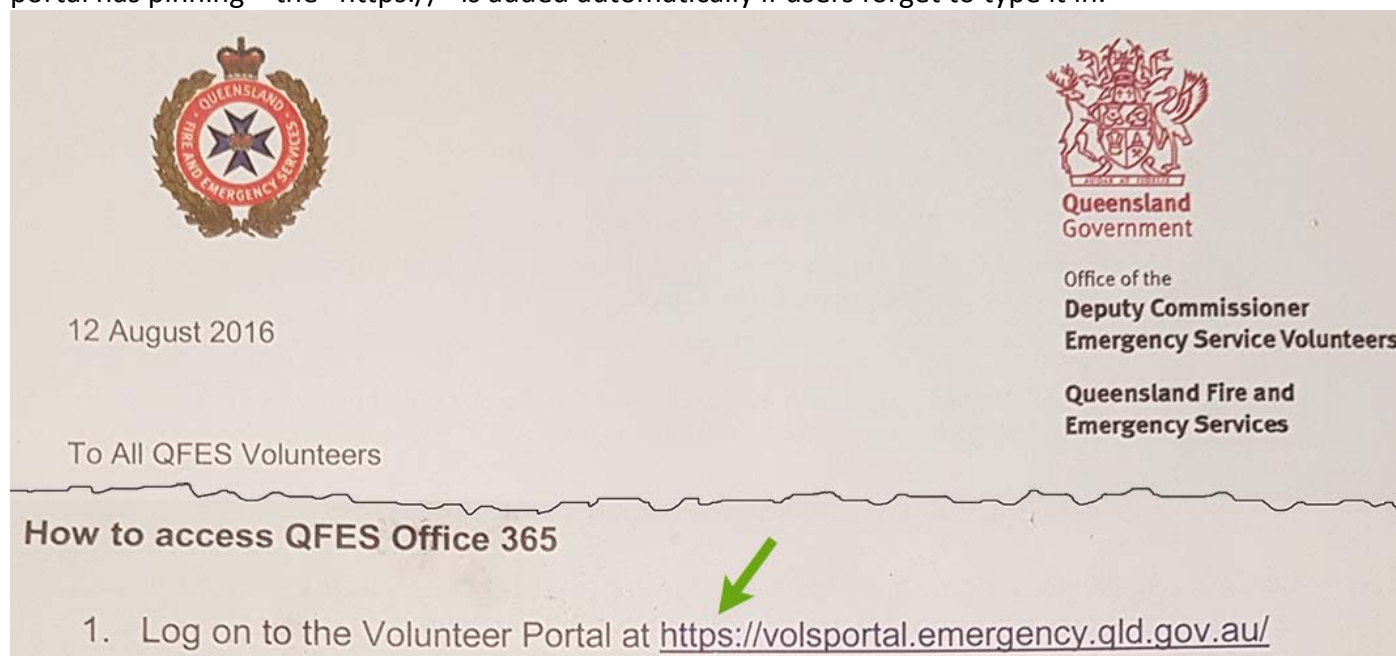
The 2016 Census web site did **not** use either of these mitigations. (Refer evidence – Appendix A)

One of the world’s best-known free services for testing website security configuration is Qualys SSL Labs. The 2016 Census blocked this service, making it impossible to test the website security, and thus hiding the abovementioned trio of mistakes from most people who might have tried to check. Had this block not been present, the Census entry page would have failed best-practice testing. A properly secured web server achieves an “A+” test result, which is only possible with TLS bootstrap mitigations like the abovementioned.

Without HSTS, Pinning, and/or “https://” printed on forms, it is technically impossible for the census itself to have been protected against a wide range of attacks, such as rouge wifi, man-in-the-middle, “ssl-strip”, or in general any active attempt to eavesdrop on information entered by citizens into the census website.

In short: security does not, and can not, work – if you do not turn it one from the start. All competent security professionals know and understand this.

Here is an example of well-implemented security. Observe the entry point requires TLS from the start. This portal has pinning – the “https://” is added automatically if users forget to type it in.



As a firefighter, my security and privacy are properly protected. As a Census user, they were not.

² Securing the SSL/TLS channel against man-in-the-middle attacks, The Open Web Application Security Project, 2012
https://www.owasp.org/images/4/4b/OWASP_defending-MITMA_APAC2012.pdf

2. Failure to recognise the TLS oversight before, during, and after the census.

The lack of TLS reveals an absolutely catastrophic failing of every conceivable security control used during the census: It was ignored, overlooked, not understood, not noticed, or perhaps even actively rejected (ignorant user-experience workers may not have known about HSTS, HPKP, etc, and somehow lobbied to have security turned off in favour of making the forms look easier to users [i.e. without the https:// prefix]). These people included:

- every person on the project.
- the people who made the forms, printed the forms, checked the forms.
- every programmer
- every contractor
- every security review overlooked it
- every tester
- every feedback mechanism failed (I personally reported this oversight many times)
- every pentester
- If the ASD was involved (I'm lead to believe they were not), they too somehow inexplicably overlooked this.

3. Failure to acknowledge (receive?) and act upon security reports made during the census.

I reported this mistake as soon as I noticed (12th August), and on approximately 50 occasions since then I have repeated my report – I made contact via numerous public online feedback mechanisms, in public government forums, in response to the majority of newspaper reports on their web sites, in blogs, in security groups I am a member of, in person to the Australian Privacy Foundation, directly to The Australian Newspaper, and directly by email to at least 3 different government ministers, the Census themselves, Data61, Alastair MacGibbon, and Sen C. Ketter.

No corrective action was ever taken.

There are many different ways to report security problems in Australia – in my opinion, **far too many**. Some that I know and use include CERT Australia (<https://www.cert.gov.au/>) AusCERT (<https://www.auscert.org.au/>) ACORN | Australian Cybercrime Online Reporting Network (<https://www.acorn.gov.au/>) ACIC Australian Cybercrime Online Reporting Network (<https://www.acic.gov.au/>) AFP (for gov-related cyber crime), State Police (for non-gov cyber crime), ASIO/ASD, Scamwatch <http://www.scamwatch.gov.au/>, stay safe online (<https://www.staysmartonline.gov.au/>) and for banking: the interbank private sharing (isac?) network, and that's not including all the joint cyber-security networks, security working groups, meetups, forums, events, and representative bodies like AISA, AIIA, etc.

It is my considerable and experienced observation that all of these resources fail almost all the time. I have made dozens, perhaps hundreds, of security reports over the years to many of those places, as well as many international equivalents (not listed above). In almost every case, no action results: and to be clear – the vast majority of my reports relate to critical security problems, usually with serious consequences, and usually affecting huge numbers of users.

If the ABS receives anything at all from any of those networks, it appears they too take no action.

4. False representations made to the Australian public regarding Census security.

Many security assurances were provided to the Australian people regarding the census, including the census web site “The connection from the user's computer to the online form is protected using, at a minimum, 128-bit TLS encryption”³ and public statements made by the Prime Minister and others.

I reported these false statements, with evidence supporting my report, and asking for the identity of the security assessors, and I received the below ignorant email response from Census (how and why they totally ignored the security evidence I supplied directly to them, and why they quoted back to me the same false and contradictory information I reported in their response, is definitely worth investigating!) [my highlighting].

The photo of the census web form missing the “https://” as seen on page 1 of this submission, and my disclosure regarding TLS, HSTS, and HPKP were in my report to abs.

From: Courtney Macgregor courtney.macgregor@abs.gov.au

Good morning,

The ABS has not published the names and results of the independent assessment.

To enable users with older unsupported browsers to access help documents the help pages were http enabled. All other Census pages including the Census Landing Page, Census Login Page and all pages of the Census form from the Census Login page through to the submission and Thank you page were https: and were secured at a minimum by 128bit encryption.

Thank you
Australian Bureau of Statistics

The false security representations still remain to this day.

5. Failure to timely invite me to contribute to this inquiry.

It is worth investigating how I was not invited to make a submission to this inquiry, and how all the security groups I am a member of also did not receive any invitation or notice: my name and my security reports would have been available in many relevant places, and I am subscribed to many groups.

It is also unfortunate that despite the multiple contacts I have made to government and ABS, it was only recently that I became aware of this inquiry, and only today when Nick Xenophon's office attended to my complaint about being sidelined from it, that I became aware that it's possible to make my own submission.

You cannot run a thorough enquiry, if you do not make appropriate efforts to solicit expert feedback. It's especially telling that this TLS mistake has not appeared in any of the prior 90 submissions, despite the internet being littered with my reports, and many dozens of people having receive my report directly by email.

³ How secure is my personal information? <http://www.abs.gov.au/websitedbs/censushome.nsf/home/privacy>

6. This TLS mistake is good!

The best part about this TLS oversight, is how thoroughly it reveals the extent of security ineptitude right across the spectrum of government and private sectors.

- We have a really-easy to understand problem: someone forgot to turn TLS on for the entry point, a show-stopping critical mistake.
- We have something that is highly noticeable that went unnoticed/ignored past every single point in all security processes.
- We have no corrective action being taken to fix the problem after it's reported, we have Census employees rejecting incoming security reports with false representations, and we have census web sites making false "https:" claims despite the glaring omission of "https:" on every census form and communication that was published. We even have an inquiry that, at this 11th hour, carries no prior mention of this obvious error.

The reason all this is good – is that it's much easier to fix a problem, when everyone can see that there **is** a problem.

This beautifully horrifying oversight is the perfect opportunity for Government to make sweeping corrective actions throughout almost the entirety of all its online security processes!

If properly handled and exploited – this TLS mistake stands to be the example that will help make all Government services in Australia significantly more safe and secure for all Australians!

I make myself available to propose recommendations to be included in the output of this inquiry.

62% of Australian cyber break-ins are to Government servers.⁴ That's 4 new ones *every day*.⁵ Compared to the UK⁶ and population/site adjusted, the true number is more likely to be double. Personally Identifiable Information (PII) has dominated the cybercriminals "most wanted asset" list for at least the last year.⁷ TLS is missing from more than 90% of all government web sites, and HSTS/HPKP is missing from more than 99% of them. Fixing TLS, making people aware of its importance, and fixing every security system in place that is somehow failing to educate our government on best-practice, can all now be accomplished with this 2016 Census-security oversight.

It was bad, but incredible good and healing can now come from this.

Yours sincerely
Chris Drake.

⁴ Australian Signals Directorate: www.asd.gov.au/publications/protect/cyber-security-picture-2013.htm

⁵ DPM&C page 16: <https://cybersecuritystrategy.dpmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf> (+37%) plus ref #4 above

⁶ <http://www.zdnet.com/article/government-is-hit-by-9000-security-breaches-a-year-but-reporting-them-remains-chaotic/>

⁷ Source: Cytegitic Intelligence Reports, Marc 2015 through March 2016: <http://cytegitic.com/cytegitic-intelligence-reports/>

Appendix A. Census web site security test.

Here's the evidence I recorded during the running of the census, even after having allowed sufficient time for my reports of this oversight to have been implemented (the thing to look for, which is not there, is the "Strict-Transport-Security:" header), and of course the missing https:// prefix on the printed paper forms.

```
#curl -i census.abs.gov.au
HTTP/1.1 302 Found
Date: Fri, 23 Sep 2016 12:11:57 GMT
X-Frame-Options: deny
Location: https://stream10.census.abs.gov.au/eCensusWeb/welcome.jsp
Content-Length: 0
Cache-Control: max-age=3600
Expires: Fri, 23 Sep 2016 13:11:57 GMT
Connection: close
Content-Language: en-US
```




```
#curl -i https://census.abs.gov.au
HTTP/1.1 302 Found
Date: Fri, 23 Sep 2016 12:12:00 GMT
X-Frame-Options: deny
Location: https://www.census.abs.gov.au/eCensusWeb/welcome.jsp
Cache-Control: max-age=3600
Expires: Fri, 23 Sep 2016 13:12:00 GMT
Vary: Accept-Encoding
Content-Length: 236
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>302 Found</title>
</head><body>
<h1>Found</h1>
<p>The document has moved <a
href="https://www.census.abs.gov.au/eCensusWeb/welcome.jsp">here</a>.</p>
</body></html>
```

```
#curl -s -i https://www.census.abs.gov.au/eCensusWeb/welcome.jsp | more
HTTP/1.1 200 OK
Date: Fri, 23 Sep 2016 12:13:33 GMT
X-Frame-Options: deny
Access-Control-Allow-Origin: https://stream22.census.abs.gov.au
Access-Control-Allow-Methods: POST
Access-Control-Allow-Headers: Origin, X-Requested-With, Content-Type, Accept
Cache-Control: no-store, max-age=3600
Content-Length: 9435
Expires: Fri, 23 Sep 2016 13:13:33 GMT
Vary: Accept-Encoding
Connection: close
Content-Type: text/html; charset=UTF-8
```

<!DOCTYPE html>
(etc)

A third possible mitigation - preload lists, is also unused (below connects first to insecure port 80, proving this mitigation is not in place)

Name Path	Method	Status Text	Type	Initiator	Size Content	Time Latency	Timeline – Start Time	1.00 s
 census.aps.gov.au	GET	302 Found		Other	283 B 0 B	50 ms 48 ms		
 welcom /eCensl		200 OK	document	http://census.ab... Redirect	3.4 KB 9.2 KB	229 ms 225 ms	