



Response to “Consultation on a new Online Safety Act”.

By Chris Drake.

19th February, 2020

Thanks for inviting my feedback, and for your commitment: “All submissions will be published on our website unless a need for confidentiality is indicated.”. There is **no** need for any confidentiality in my submission; please publish this in full, without censorship.

I was part of the Prime-Ministers advisory committee on network threat blocking, and a consideration raised there is worth repeating here: Any measures created to protect, can equally be used maliciously to attack. Great care will be needed, and should be explicitly demanded, to ensure that all actions taken against anyone are based only on a trusted source with genuine authority, and that the actions are warranted based on genuine need. Evidence needs to exist, and be verified for authenticity, and there needs to be a rapid mechanism to reverse any actions taken against anyone that turn out to be based on false or malicious reports, along with a clear and easy way for these victims to report inappropriate actions and have their services restored. Online crime and retribution are rampant; powerful takedown tools will be a juicy target for bad actors, hackers, activists, disgruntled customers, mischievous children, and others wishing to inflict damage, and faking evidence to do so.

The rest of my response is directed at your “Basic Online Safety Expectations” (BOSE) proposals, and relates mostly to my area of deep experience and skill: technical safety measures for protecting people against cyber-crimes and fraud and the deficient legislative environment that perpetuates these crimes. In the last 2 years, the unrecovered losses that Australians have suffered due to easily preventable online cyber crimes exceeded a billion dollars (source: Au Govt Report).

I disagree with your preamble: “*Online service providers have a responsibility to respect the rights and dignity of users online and to take meaningful action to address and prevent harms being incurred by those using their products or services.*” – that is simply not true. The **true** “responsibilities” of online service providers is set out in the constitutions of the companies operating them, and in law. The principle responsibility (and legal requirement) of most companies is delivering profits to shareholders. Keeping their customers safe is not an actual responsibility at all. As we saw in the Financial Services Royal Commission – companies often go to extreme lengths to exploit their users, with widespread disregard for ethics or common sense, and if you look at any online crime statistics you can observe a relentless increase in global online crime, showing that companies are failing to invest in protection technologies (why should they – it’s not really their responsibility?). “Half of older Australians surveyed reported experiences related to virus, scam, credit card and personal information theft.” That is not their fault – it is the fault of their online service providers, who failed to give them adequate protection against the totally foreseeable everyday threats that plague the world. To be clear – the fault is the providers choosing not to invest in appropriate protection technologies: to quote a first-hand experience I had speaking with a bank CxO “We don’t care, so long as our bank does not lose money”. This was a 3-way conversation I had (HRH Prince Andrew, Duke of York, was the other participant), and the topic was why banks are not purchasing software that defeats attacks that cause customers to lose money (\$1bn lost in Aus in the last 2 years). I was one of the speakers at the cyber-security event where this conversation took place.

I request that you do consider and include my response and recommendations in your action plan. The “2020 Cyber Security Strategy” initiative is already flawed and is unlikely to deliver security improvements.

- The Majority of the Panel for this strategy are current or ex Telstra employees (Telstra inaction is one of the largest contributors to cyber losses suffered by Australians)
- Expert submissions are not being properly considered (Mine was “skimmed” I was told, when I asked if it had been read; and they didn’t exhibit knowledge of my content in discussion).
- The review is being lead by a policy writer, instead of a cyber expert, and has no regard for industry experts (e.g. forging ahead with flawed initiatives that fly in the face of all expert understanding on the topic)
- No measurement is taking place – there is zero understanding of the actual efficacy of their previous initiatives, and no desire to admit or reveal failures.
- The lead policy author has already “Admitted Defeat” – when I asked why a range of solutions will not become part of his policy (like, for example, imposing penalties for security non-compliance against government entities and staff), he explained that “it is too hard”.

Basic Online Safety Expectations Recommendation 1: Compel ASIC to enforce company reporting obligations.

Despite our banking industry suffering regular and large losses to cyber-crime and fraud, not a single one of any of our major banks lists any of their cyber or fraud losses in any of their ASIC filings or shareholder reports.

Shareholders and customers alike have no insight into the cyber competence of their banks. Banks have their own private crime reporting body, which additionally robs Government and others from any knowledge of the true state of the problem.

Banks are the most heavily regulated businesses in Australia. This is for good reason: they are responsible for generating profits to shareholders. They are not responsible for the protection of customers, or even for the ethical treatment of them, as was widely uncovered in The Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry.

It is not just that they cannot be trusted to behave ethically in relating to cyber security – it is that they have little to no obligation to do so, and there is no enforcement of the existing laws that could shed light on their cyber performance. This needs to change.

In addition to reporting cyber and fraud loss, banks need to report insurance claims as well. One of the methods to cover up the scale of their cyber problem is to shift the loss reporting into other accounting categories. This is not appropriate behaviour, and needs to be prevented. Losses need to be reported as losses. Insured-losses need to be reported as losses, along with the insurance payouts that covered them, and all this needs to be made available to shareholders, who have a legal right to know how adequately their company is managing these losses, and how this ultimately affects their dividends.

Basic Online Safety Expectations Recommendation 2: Amend company annual reporting obligations to include cyber and fraud losses.

While existing ASIC laws may solve some reporting cover-ups, ideally, legislation amendments making cyber and fraud loss reporting to shareholders mandatory would be better. As long as there are loopholes

allowing businesses to cover up their cyber ineptitude, there is never going to be meaningful reduction in crime. The potential for public embarrassment and share price falls as a result of enforced cyber reporting are powerful incentives for business to do the right thing and protect themselves and their customers properly in the first place.

Basic Online Safety Expectations Recommendation 3: Introduce mandatory cyber and collateral damage reporting.

When a company (such as a bank, telco, stock-exchange, etc) successfully transfers a cyber or fraud loss to its customer (typically by blaming the victim for “poor cyber hygiene”, for malware, or through oppressive terms-of-service agreements etc), this needs mandatory reporting.

The company needs to be compelled to collect statistics of the losses that have been suffered by its customers, especially in cases where the company believes the fault might lie with the victim. These statistics need to be audited for completeness, with heavy fines for omission and cover-up.

As it stands, there is currently no working mechanism by which consumers can determine which businesses have acceptable cyber protections for their customers. A working method to assess actual customer losses is needed. Remember – companies have no incentive to protect their customers, because company responsibility is to shareholder profits. Giving customers a way to reject poorly behaving companies gives those companies the strong motivation they are currently missing to offer improved protection to win customer business.

Case in point: All of Australia’s top banks are “Major Sponsors” of the “Stay Smart Online” campaign – a misguided government initiative that goes to extreme lengths to “blame the victim” and educate our country that it is their fault when they suffer cyber losses. Those banks include Westpac, ANZ, Commonwealth Bank, NAB, Bank of Melbourne, St.George, IAG. It also includes Telstra – the worst offender at refusing to take any action against the massive problem of telephone scamming sweeping our Nation as well as SMS crime. Clearly – they all have the most to gain, by ensuring that we keep blaming the victim, and to ensure that the largest amount of loss is borne by those victims, and not the banks themselves.

One of our country’s most-expensive ex-politicians, Anna Bligh, is the head of the Australian Banking Association – a well-funded, highly-active lobby group in place to defend the banks against regulation (that is to say – to defend the banks against laws that would protect customers). The ABA and banks are no-doubt going to fight hard against anything that might increase their regulation. We need to be prepared to take on the power of these organisations for the benefit of Australian Banking customers – because right now, protecting customers against cyber threats is NOT any obligation that a bank currently holds, yet the only architecturally possible way to actually protect a customer requires that a bank deploy an effective solution. Right now, no bank has one – the best on offer is technology invented in 1984 – before the web even existed.

What follows, is my complete submission to the 2020 Cyber Security Strategy. I have no confidence that the 2020 Strategy will be properly written or effective, and a great number of my recommendations and other information that follows directly relate to Basic Online Safety Expectations.

Response to “A call for views” on Australia’s 2020 Cyber Security Strategy.

By Chris Drake.

25th October, 2019

Chris Drake is a professional Cyber-Security expert. Refer to the last page of this submission for his credentials and experience details.

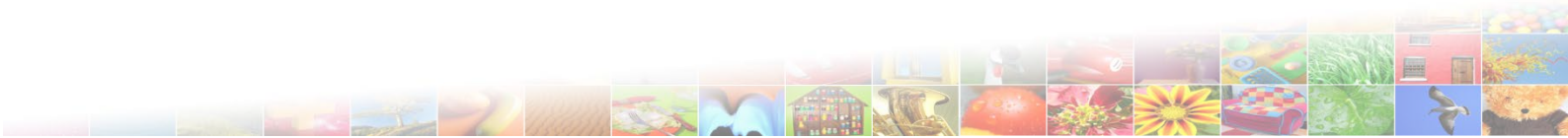
Chris is an internationally respected expert, published author, and thought leader on the cyber security niche relating to **strong protection for everyday people against sophisticated cyber-crimes and fraud**. Chris has worked in this niche for 37 years; his patent for defending people and software against malware is the world’s most widely-cited security patent of all time, he has spoken at numerous local and international conferences on cyber topics, and has won more than a dozen international awards for his work in this field.

Chris has significant recent first-hand experience with a breadth of cyber-security problems suffered by Australian businesses and government. Over the last 3 years, he has had in-depth cyber-security discussions lasting more than an hour each, with more than 500 senior-level cyber executives representing more than 200 top-tier Australian and International businesses and Governments. Chris has personally made extensive use of multiple cyber threat reporting systems, bug bounty programs, and other mechanisms in his quest to help secure Australians. He has also participated in numerous government advisory panels, including the original 2016 strategy, as well as multiple senate inquiries into cyber failures. He is a member of numerous industry working groups relating to cyber security, and was a contributor to several current cyber standards, including FIDO, DKIM, OpenID, and NIST. Chris led the team that wrote the penetration-testing guide for Australia’s Trusted Digital Identity Framework (TDIF, aka, GovPass) under contract to the DTA.

On account of his extensive first-hand experience and broad understanding of **actual cyber practice** throughout business and government, it is likely that there is no better qualified individual than Chris to provide effective recommendations for inclusion in our next strategy. He hopes that you can put aside the Australian affliction of “tall poppy syndrome”, and rather than ridicule or attack his suggestions or motives, stay focussed on the topic: This response exists to help secure Australians: any topic or distraction that is unrelated to the technical discussion of the merit of Chris’s recommendations deserves no place in the discussion.

Publication Note

Please publish this submission. If there are parts herein which are deemed unsuitable for publication, please redact or censor just those portions. Please try not to simply censor my entire submission.



Contents

Response to “A call for views” on Australia’s 2020 Cyber Security Strategy.....	1
Publication Note	4
Recommendations of Chris Drake	7
Recommendation 1: Appoint Chris Drake as an industry representative on the 2020 strategy panel	7
Recommendations relating to “Government’s role in a changing world”.	8
Recommendation 2: Stop undermining the cyber security industry.....	8
Recommendation 3: Stop Blaming the Victim.....	9
Recommendation 4: Educate industry, institutions, and government that THEY should be responsible for keeping their users safe.	10
Recommendation 5: Adapt and Innovate.....	11
Recommendation 6: Measure effectiveness and outcomes.	11
Recommendation 7: Combine all 30+ threat-reporting bodies into one.	12
Recommendation 8: Compel ASIC to enforce company reporting obligations.....	14
Recommendation 9: Amend company annual reporting obligations to include cyber and fraud losses.....	14
Recommendation 10: Introduce mandatory cyber and collateral damage reporting.....	14
Recommendation 11: Discontinue all location-based cyber activities.....	15
Recommendation 12: Discontinue collecting “do nothing” victim statements.	15
Recommendation 13: Ban the public sector from building their own cyber-security products and services.	16
Recommendation 14: Discontinue the suppression of senate-inquiry submission records.	16
Recommendation 15: Discontinue all suppression of public submissions relating to cyber security.....	17
Recommendation 16: Convene a royal commission to investigate misconduct throughout the senate inquiry process.	17
Recommendation 17: Resume the publication of ASD security reports.	18
Recommendation 18: Extend mandatory intrusion reporting to all Government departments.	18
Recommendation 19: Amend consumer protection and competition laws to include Government.	18
Recommendation 20: Hold business responsible for losses of their customers.....	19
Recommendation 21: Introduce mandatory, publically-audited, minimum cyber security requirements for companies and government departments handling personal data of Australians.	19
Recommendation 22: Fix government scrutiny and compliance.	20
Recommendation 23: Fix government procurement.	20
Recommendation 24: Amend the ASD advice.....	20
Recommendation 25: Comply with the ISM and all ASD Essential recommendations.	21
Recommendation 26: Roll out mandatory TLS across all .gov.au domains.	21
Recommendation 27: Overhaul the Freedom of Information (FoI) act.....	21
Recommendation 28: Reform official Government cyber-security roles.....	22

Recommendation 29: Mandatory cyber auditing (with no self-reporting).....	22
Recommendation 30: Prohibition on sharing identity information with non-compliant departments.....	23
Recommendation 31: Repair cyber-response capability throughout government.....	23
Recommendations relating to “Enterprise, innovation and cyber security”.....	23
Recommendation 32: Providers need to do more to protect users.....	23
Recommendation 33: Comment on equipping purchasers to protect themselves.	24
Recommendation 34: Discard “minimising upfront costs for industry” wording.	25
Recommendation 35: Best practice Identity and Authentication must be made available to all.....	25
Recommendation 36: Software goods must be digitally signed.	25
Recommendation 37: Mandatory security update provision.....	25
Recommendation 38: Remove Digital-Identity-Services from Government.	25
Recommendations relating to “A trusted marketplace with skilled professionals”.....	26
Recommendation 39: Update your understanding of global industry standards.	26
Recommendation 40: Trust.	26
Recommendation 41: Update cyber training standards.....	27
Recommendation 42: Buy instead of Build.....	27
Recommendation 43: Mitigate the skills shortage by fixing some problems.....	27
Recommendation 44: Penalties and liability enforcement.	27
Recommendation 45: Survey the Australian Cyber Security Market.	27
Recommendation 46: Sponsor Australian products through EPL listing.	28
Recommendations relating to “A hostile environment for malicious cyber actors”.....	28
Recommendation 47: Block threats first.	28
Recommendation 48: Prioritize prevention.	28
Recommendation 49: No expanded law capability is needed.....	28
Recommendation 50: Properly designed digital identity promises to all but eradicate online crime.	28
Recommendation 51: Cyber-insecurity levy.....	29
Recommendation 52: Penalties imposed on attack supporters.....	29
Recommendations relating to “A cyber-aware community”.	29
Recommendation 53: Totally discontinue your blame-the-victim approach.....	29
Recommendations relating to “Other issues”.	30
Recommendation 54: Discontinue behaviour-change campaigns.	30
A note about insurance.....	30
A note about Telstra.	30
Chris Drake’s Comments relating to Australia’s Cyber-Security Strategy 2016 & 2020.....	32
My observation of failures from the 2016 strategy:-.....	32
Attachment 1: Submission to the Senate Inquiry into the Digital delivery of government services.....	37
Attachment 2: Submission to the Senate Inquiry into the 2016 Census.	38

Attachment 3: Submission to the Senate Inquiry into the Future of Work and Workers.	39
Attachment 4: Submission to the Senate Inquiry into the Circumstances in which Australians’ personal Medicare information has been compromised and made available for sale illegally on the ‘dark web’.....	40
Attachment 5: Submission to the Review of national arrangements for the protection and management of identity information	41
Attachment 6: Full text of “Deemed Confidential” advice letters informing that embarrassing Submissions will be hidden from existence.	42
About Chris Drake	43

Recommendations of Chris Drake

Recommendation 1: Appoint Chris Drake as an industry representative on the 2020 strategy panel

- The 2016 strategy correctly identified that industry collaboration is “increasingly important”, and states that ensuring our online interests are protected requires government and industry “working together”.
- “Industry” includes the manufacturers of the products and services which are ultimately required to keep people safe. No other participant has better understanding of the threats and solutions available, than the companies who make the solutions to solve those threats.
- “Industry” also includes the businesses who own and operate the services which need to adapt to better secure their customers – the telco’s who need to better prevent fraudulent telephone scam calling, the internet service providers who need to better defend against phishing, malware, and online scams, the banks who need to better prevent their customers losing money, and so forth.
- Chris lead the industry team which developed the TDIF Penetration testing guide for the federal Government; our collaboration produced what is currently the world’s most effective and comprehensive strategy for ensuring that the TDIF strongly defends against contemporary and future perceived threats, with nothing declared “out of scope” (thus avoiding the major drawback of legacy pen-testing guides). Chris is ideally suited to do this kind of work once again, which all but guarantees that our 2020 strategy will have an effective and meaningful impact on reducing cyber-crime. Our country desperately needs cyber-crime reduction.
- Chris knows what is really going on, both in Government, and in Industry. He knows what is working, and what is failing. He has been at the “coal face” of this debate for many years, and believes there is no better qualified individual than himself, to assist with drafting the 2020 policy.

Recommendations relating to “Government’s role in a changing world”.

Recommendation 2: Stop undermining the cyber security industry.

Australia produces many of the world’s leading solutions in a variety of cyber-security industries, from quantum communications to advanced authentication. These are **extremely effective** products that demonstrably solve very complex and difficult problems.

Unfortunately, there is an extremely unhelpful, frequently recurring defeatist theme in all government communications relating to cyber security, which is actively destroying our industry. Take the recent discussion paper for example:

“we can never be totally cyber secure” (page 14)

“Australia’s 2020 Cyber Security Strategy cannot be a magic bullet” (page 20)

“A new Cyber Security Strategy ... would be unrealistic to expect it to solve all problems” (page 20)

These abundant and pithy throw-away comments are exacerbating the problem and causing extreme damage:

- When cyber-failures occur, the people in a position to solve the problem tend not to, because they have been repeatedly told it is difficult or impossible.
- When innovative solutions that genuinely solve problems are presented, they are mistrusted and not tested and not deployed, because the buyer has been repeatedly told that “we can never be secure”.
- When victims suffer losses, these defeatist statements are being used as excuses.
- Responsible parties are not seeking out solutions when they should be, because they keep being told misleading defeatist advice.
- This defeatist language is preventing everyone from understanding that solutions can and do exist.
- Case in point: the concept of “prevention” is totally missing from the discussion paper page 8, which covers only detection, deterrence, and response! This just one example of the insidious and deeply damaging side-effect of defeatist thinking. Everyone knows that prevention is better than cure, but we’ve been so poorly trained to accept defeat, that even the concept of prevention gets left out of the discussion paper!
- This language is educating CISO’s and others to accept cyber failure!

Regardless of whether someone thinks it’s smart or funny or “realistic” to regurgitate those offensive defeatist attitudes, they have no place whatsoever in any government strategy or messaging. Churchill single-handedly overturned similar defeatist thinking throughout his entire cabinet in May 1940, which lead directly to eventual allied victory in WWII. We too need to tackle this intellectual disease, and fully eradicate all acceptance of failure. Cyber security *is* a war: we need to act like we can win, otherwise we cannot!

In short: Stop telling our market that our products do not exist or do not work.

Please remove all those defeatist statements, and stop issuing any and all related defeatist language. Please circulate instructions to this same effect to all government agencies and contractors who issue advice (e.g. The “ASD’s Stay Smart Online program”, and so forth)

Recommendation 3: Stop Blaming the Victim.

This is my most important recommendation, so let me repeat it in bold:

Stop Blaming the Victim.

Every time you say any of the following, you are blaming the victims; which is to say - you are inadvertently educating the only people who can genuinely keep them safe (their providers), that it should **not** be the role of those providers to keep them safe.

“Australians continue to fall victim because they fail to observe, or are unaware of, basic online security practices” (p.7) – this is **BLATANTLY UNTRUE** – they become victims, because their providers have not given them solutions that mitigate the well-known, totally foreseeable, everyday problems of human behaviour.

“Cyber security has always been a shared responsibility” (p.8) or

“raise national awareness of online threats” (p.5) or

“Australians need the right knowledge to make cyber-smart consumer choices” (p.16) or

“we need to know how to be more consistent in practicing secure online behaviours” (p.16) or

“increased consumer focus on cyber security” (p.17) or

“Our hope is for all Australians to play a role” (p.18) or

Almost the entirety of the “ASD’s Stay Smart Online program” (p.32), or

“behaviour change initiatives” or “user awareness” (p.16)

Stop doing/saying all the above. It should NOT be the job of 25 million Australians to all be cyber experts. Even if it was their job, **which it is not**, there is no practical way you could ever possibly reach all those potential victims with your message, let alone manage to get them to understand and remember such a large and complex message, and that’s not even starting on the absurdity of believing that it’s even possible for a user to be safe, when their provider has not supplied the security that is architecturally necessary to make safety possible in the first place.

By way of example; the Australian Communications Alliance, (representing Telstra, Optus, and Vodafone), back in 2012, publically called for a total ban of SMS messaging for banking in Australia because it is unsafe.¹ Today, 7 years later, every bank in Australia uses SMS for bank security, despite the existence of hundreds of vastly superior solutions in the market. Besides being impossible to properly educate Australians on being cyber-safe, we are stuck in the position of the companies with whom those users need to be safe, actively refusing to use appropriate technologies to make that safety possible. This is, in part, directly attributable to this “Blame the Victim” mentality. For as long as you keep telling everyone, banks etc included, that it’s the Victims’ fault – they have no incentive, and don’t even realize they should try, to provide adequate protection to their users.

It SHOULD be the job of companies that provide services TO Australians to comply with and offer sensible cyber-security protections, **so that those users are SAFE even when they are not cyber experts.**

¹ See <https://www.itnews.com.au/news/telcos-declare-sms-unsafe-for-bank-transactions-322194>

Recommendation 4: Educate industry, institutions, and government that THEY should be responsible for keeping their users safe.

The overwhelming majority of contemporary cyber-crimes relate in some way to impersonation or trickery. From a cyber-security architecture point of view, the “attacker” takes up a position in-between the victim, and some organisation. What this literally means, is that there is nothing you can do at the “victim end” to effectively prevent these crimes, unless you have also done something at the “organisation end” as well (or instead).

For example – the only way it is architecturally possible for someone who is about to be scammed by an attacker impersonating (for example) the ATO – is if the ATO has deployed cyber security which helps defeat impersonation of the ATO.

Or, another example, the only way a bank can guarantee that “friendly fraud” is impossible (for example – elder abuse, or children using their parents accounts and devices to move money without permission etc), is if the bank itself provided those potential victims with working security to defeat it (for example; biometric authentication, instead of SMS-text-messages). The same applies to email frauds (gmail, Hotmail, yahoo, etc), social frauds (Instagram, facebook, twitter), and all other “friendly fraud” situations.

Or, yet another example, co-workers using only passwords (because the organisations they use only offer passwords) are at extreme risk of compromise, because it’s easy to observe typed password entry (or view it on security videos), or for that matter any of a dozen other problems that relate to passwords (like phishing, guessing, keyloggers and other related sniffers and scrapers, dictionary-attacks, social-engineering, serverside thefts and cracking, re-use, email-recovery, hacking, password-manager compromise, and plain old reading-them-off-post-it-notes). NONE OF THIS IS THE USERS FAULT. All these problems are easily mitigated, but they all require the provider to give the user solutions which keep them safe (such as password-less authentication for example).

The above are just examples to help you understand the breadth of this recommendation – they are not limiting or exhaustive – there are literally hundreds of other examples where effective security is impossible at the user end, but relatively simple if offered by the provider end (i.e. offered by industry, institutions, and government to their users). We need to tell them they can and should do this, and examine incentives to make it happen.

This is not an easy recommendation – the tide of flawed thinking and the vast assembly of resources all aimed at blaming victims overwhelming. Effort needs to be expended to produce **effective** education that aims to convince the people in positions of responsibility to actually deploy protection, and probably also to **educate victims that it is not their fault**, and that those victims should pressure their providers to offer effective security.

One difficulty that needs to be overcome is that organisations do not currently have any incentive to protect their users. For example – the role of a company is to maximise profit for shareholders. Wasting effort or money on protecting losses that their customers face, is not *theoretically* a company responsibility when those losses are not being suffered by the company itself (e.g. usually, because the company successfully blames the victim and thus avoids company losses by shifting the full loss to the victim – a situation that has caused more than \$1b in reported unrecovered losses by Australians over the last 2 years).

This is literally a billion dollar problem, with everyone who is in a position to solve it having no motivation to do so, and through misguided existing “blame the victim” education – not realizing that they should even try.

Recommendation 5: Adapt and Innovate.

Discussion-paper Paragraph #1 correctly says “we need to adapt our approach” after acknowledging that things are getting worse. The concept of “Innovation” requires discarding practices that don’t work, and embracing new solutions.

Change and adaptation in Cyber-Security is very **very** difficult.

From my extensive contact with around 500 C-level cyber executives, I can safely report that the #1 factor they take into account when considering new technology, is their own personal reputation. There is an absolute resistance against trying anything new, against considering any different approaches, and against doing anything whatsoever that all their peers are not already doing. The entire industry is paralysed with “copy each other” mentality.

Instead of asking “What does it solve” or “how effective is it”, CISO’s and others are obsessed with “Who else is using it”, and “what publications (e.g. Gartner) has it been featured in”, and “how can they be sure the company will be around” – all questions that affect their own personal reputation (as an advocate for the solution), and have nothing whatsoever to do with efficacy. Case in point: at the SINET61 conference in 2016, with a panel on-stage representing companies who had active cyber-security accelerator programs, I posed the question (eliciting a large audience applause): “Can you share an example of a time when you have on-boarded innovative Cyber Security from an Australian start-up” to the panel, which included Mike Burges (CISO, Telstra), Steve Glynn (CISO ANZ Bank), John Haig (Head of Security & Risk, Dun & Bradstreet), and Nick Scott (Head of Security, NAB Bank). **None of them had any example.** Not even one used any of the technology that their own programs turned out, let alone anything else innovative from anyone else in our industry.

Many of my recommendations herein require that Australia take a different direction to the protection of our citizens – one which is genuinely and **measurably effective**, but ones which will raise eyebrows because it will be hard to point to “who else is doing it”, and this will challenge the “my reputation comes first” mentality of any cyber experts considering my advice. Innovation is not easy – it requires clever people to take action that will draw attention, and in our Tall-Poppy-afflicted culture, that makes people uncomfortable.

Unfortunately, right now, we are not measuring effectiveness on any meaningful scales, making it extremely difficult to understand just how pointless our existing approach actually is. One rough measurement we do have is the annual scale of the problem, which does show a relentless worsening of the situation: more people and more business are falling victim more often, and greater sums of money are being lost, more breaches are taking place, and greater damage is being done. Overall, it is absolutely clear that what we are currently doing IS NOT WORKING.

We need to change. Not just to pay lip service to the idea of adaptation and innovation, **but to actually do it.** My recommendations herein are an excellent starting point.

Recommendation 6: Measure effectiveness and outcomes.

There is no measurement being made of the effectiveness of any Australian cyber strategies.

I counted about 40 measurable outcomes in the 2016 Strategy, and it contained 33 action points itself. Not only was there no measurement taking place of whether or not any of these multi-million-dollar initiatives are working – even the very concept of effectiveness-measurement is missing.

What we do know is that everything is getting worse.

If you do not measure it – you can not know which parts are not working.

As Einstein is supposedly quoted as saying:

“Insanity is doing the same thing over and over, and expecting different outcomes”

Let us stop repeating our mistakes – so we need to measure what we’re doing, so we know which ones are mistakes.

Every initiative that the 2020 strategy includes absolutely needs to spell out exactly how the effectiveness of that initiative will be measured, and for measurement to take place.

To be clear: "measuring effectiveness" means exactly that - **not** milestone completions, **not** budget spending, **not** staffing numbers, **not** events, **not** rhetoric, and **not** any other pointless metrics - it means "Is this effort improving the *ACTUAL* security situation in Australia".

- The last public report covering government intrusions was in 2013, where Government-server intrusion (63%) dwarfed all other incidents. Since then, Government is being increasingly silent, while passing laws compelling enterprise to be more open.
- Problems can't get fixed while they're hiding under the carpet!
- The 9-month-late "Review of national arrangements for the protection and management of identity information" and associated submissions has not been released. Why not? Why is it more important to avoid government embarrassment than it is to protect Australians?

Recommendation 7: Combine all 30+ threat-reporting bodies into one.

The staggering duplicity of threat-reporting in Australia is decimating our ability to respond. With so many different places, it's impossible to know how to report crimes and vulnerabilities, and it's impossible for each of those many bodies to take effective corrective action.

This will not be a popular or easy to implement – there is no-doubt a huge blur of state, federal, and some private boundaries, fiefdom's seeking to protect their mini empires, power and budgets and prestige – but at the end of the day, when these are all combined into one single agency – the pooled resources of talent, personnel, and budget can then make a very real and effective one-stop-shop for actually solving cyber issues – instead of the rag-tag mess that currently exists, where by-and-large the only purpose almost all of them serve is an ineffective and dubious statistics-gathering nature. Crimes never get solved. Perpetrators never get investigated or prosecuted. Monies never get returned. Scams never get shut down. Vulnerabilities never get fixed. And nothing ever gets effectively measured.

Some that I know of 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 - Australian Federal Police (for government-related cyber-crime, and agency related scams, and also including ACT Policing) <https://www.afp.gov.au/contact-us/report-commonwealth-crime>
- ACSC - Australian Cyber Security Centre (part of ASIO's cybercrime, cyberterrorism, cyberwarfare division) <https://www.cyber.gov.au/report>
- 8 different State Police forces (for non-government cyber-crime):
 - Australian Capital Territory Police
 - New South Wales Police
 - Northern Territory Police

- Queensland Police
- South Australia Police
- Victoria Police
- Western Australia Police
- Tasmania
- 5 JCSC's - Joint Cyber Security Centres - in Melbourne, Sydney, Perth, Adelaide, and Brisbane
- Scamwatch from the ACCC <http://www.scamwatch.gov.au/>,
- Stay Smart Online (<https://www.staysmartonline.gov.au/>)
- ISAC: the interbank private sharing network (private for banking - they don't want anyone else knowing what they're doing wrong!)
- CrimeStoppers (<https://www.crimestoppers.com.au/>)
- ASIC; Australian Securities and Investments Commission (financial and investment scams and fraud)
- ATO - Australian Taxation Office (directly; for tax and ATO related scams)
<https://www.ato.gov.au/General/Online-services/Identity-security/Verify-or-report-a-scam/>
- APRA - Australian Prudential Regulatory Authority (directly, for superannuation related scams)
- Australian Criminal Intelligence Commission (including the Australian Crime Commission and the former CrimTrac Agency) <https://www.acic.gov.au/>
- AUSTRAC - Australian Transaction Reports and Analysis Centre - mandatory for banks and exchanges
- Department of Home affairs (directly, for immigration related scams)
- Department of Immigration and Border Protection (including the Australian Border Force) [not sure if this is part of the above or not]
- Department of Veterans' Affairs for veteran-directed scams and fraud
- ASD - Australian Signals Directorate for defence-related scams, high-tech government attacks, and critical infrastructure issues
- DIO - Defence Intelligence Organisation – weaponisable threats
- ACLEI - The Australian Commission for Law Enforcement Integrity for corruption issues (is deliberate disobedience, lies, cover-ups, misleading senate inquiries, and flagrant disregard for the ISM and FoI law a corruption issue?)
- Department of Human Services for Medicare, Centrelink and child support fraud and scams
- IDCARE – a not for profit support service <https://www.usc.edu.au/idcare>
- Internet Crime Complaint Center (Global, run by the FBI) <https://www.ic3.gov/default.aspx>

And that's not including all the other joint cyber-security networks, security working groups, meetups, forums, events, threat-sharing schemes, and representative bodies like AISA, AIIA, etc.

As you can see – many of those are run by affected parties (and no doubt there are dozens more I'm not aware of in this category) – the reason they have to do this, is because the existing reporting system is so horribly fragmented and broken, that it cannot be relied upon – necessitating other departments (ATO, defence, etc) to fund and run their own cyber-crime reporting portals!

When we have just one body responsible for all this work, everyone will know how and where to make reports, and that body will know that it's getting all the reports, it will have a complete view of the situation, and it will have the resources necessary to take action.

For example - victims won't have to report directly to the ATO, but the ATO will be assured that it timely receives all victim reports, because it will have confidence in the procedure in place at this single reporting portal to properly convey the message. Additionally, this single portal will then have a dependably complete picture of ATO attacks.

We can't solve this problem if we don't adapt. Amalgamation might sound hard, but the benefits are so staggeringly immense that it will absolutely be worth it.

Recommendation 8: Compel ASIC to enforce company reporting obligations.

Despite our banking industry suffering regular and large losses to cyber-crime and fraud, not a single one of any of our major banks lists any of their cyber or fraud losses in any of their ASIC filings or shareholder reports.

Shareholders and customers alike have no insight into the cyber competence of their banks. Banks have their own private crime reporting body, which additionally robs Government and others from any knowledge of the true state of the problem.

Banks are the most heavily regulated businesses in Australia. This is for good reason: they are responsible for generating profits to shareholders. They are not responsible for the protection of customers, or even for the ethical treatment of them, as was widely uncovered in The Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry.

It is not just that they cannot be trusted to behave ethically in relating to cyber security – it is that they have little to no obligation to do so, and there is no enforcement of the existing laws that could shed light on their cyber performance. This needs to change.

In addition to reporting cyber and fraud loss, banks need to report insurance claims as well. One of the methods to cover up the scale of their cyber problem is to shift the loss reporting into other accounting categories. This is not appropriate behaviour, and needs to be prevented. Losses need to be reported as losses. Insured-losses need to be reported as losses, along with the insurance payouts that covered them, and all this needs to be made available to shareholders, who have a legal right to know how adequately their company is managing these losses, and how this ultimately affects their dividends.

Recommendation 9: Amend company annual reporting obligations to include cyber and fraud losses.

While existing ASIC laws may solve some reporting cover-ups, ideally, legislation amendments making cyber and fraud loss reporting to shareholders mandatory would be better. As long as there are loopholes allowing businesses to cover up their cyber ineptitude, there is never going to be meaningful reduction in crime. The potential for public embarrassment and share price falls as a result of enforced cyber reporting are powerful incentives for business to do the right thing and protect themselves and their customers properly in the first place.

Recommendation 10: Introduce mandatory cyber and collateral damage reporting.

When a company (such as a bank, telco, stock-exchange, etc) successfully transfers a cyber or fraud loss to its customer (typically by blaming the victim for “poor cyber hygiene”, for malware, or through oppressive terms-of-service agreements etc), this needs mandatory reporting.

The company needs to be compelled to collect statistics of the losses that have been suffered by its customers, especially in cases where the company believes the fault might lie with the victim. These statistics need to be audited for completeness, with heavy fines for omission and cover-up.

As it stands, there is currently no working mechanism by which consumers can determine which businesses have acceptable cyber protections for their customers. A working method to assess actual customer losses is needed. Remember – companies have no incentive to protect their customers, because company responsibility is to

shareholder profits. Giving customers a way to reject poorly behaving companies gives those companies the strong motivation they are currently missing to offer improved protection to win customer business.

Case in point: All of Australia's top banks are "Major Sponsors" of the "Stay Smart Online" campaign – a misguided government initiative that goes to extreme lengths to "blame the victim" and educate our country that it is their fault when they suffer cyber losses. Those banks include Westpac, ANZ, Commonwealth Bank, NAB, Bank of Melbourne, St. George, IAG. It also includes Telstra – the worst offender at refusing to take any action against the massive problem of telephone scamming sweeping our Nation. Clearly – they all have the most to gain, by ensuring that we keep blaming the victim, and to ensure that the largest amount of loss is borne by those victims, and not the banks themselves.

One of our country's most-expensive ex-politicians, Anna Bligh, is the head of the Australian Banking Association – a well-funded, highly-active lobby group in place to defend the banks against regulation (that is to say – to defend the banks against laws that would protect customers). The ABA and banks are no-doubt going to fight hard against anything that might increase their regulation. We need to be prepared to take on the power of these organisations for the benefit of Australian Banking customers – because right now, protecting customers against cyber threats is NOT any obligation that a bank currently holds, yet the only architecturally possible way to actually protect a customer requires that a bank deploy an effective solution. Right now, no bank has one – the best on offer is technology invented in 1984 – before the web even existed.

Recommendation 11: Discontinue all location-based cyber activities.

Australia is far too vast to expect everyone to go somewhere for activities that relate to online topics like cyber security. Not only are our cities thousands of kilometres apart, 48% of Australians do not even live in a metropolitan area at all.

It makes no sense to have any "centres" – it robs regional and smaller city Australians of resources they need, and it is entirely unnecessary. Dial-in and Video-conferencing facilities are abundant and low-cost.

There is also a considerable amount of interstate bickering, duplicity, and one-upmanship, which is wasting resources and is detrimental getting on with the job of securing Australians.

Case in point: the "Joint Cyber Security Centres" should **not** be proud – they should be **deeply ashamed** of their monumental resource wastage from establishing locations in Melbourne, Sydney, Perth, Adelaide, and Brisbane. See also my recommendation 7 – none of these should exist at all.

Recommendation 12: Discontinue collecting "do nothing" victim statements.

Almost all our current cyber-crime reporting endpoints take no action from reports. This is not acceptable.

Every time a victim makes contact, the very first action that needs to take place, and immediately, must be to prevent more victims.

If it was a telephone scam, the calling route needs to be immediately barred. If it was a payment scam, the money reception endpoint needs blocked so no other victims can pay into it. If it was phishing, the site needs to be taken down.

It is absurd to think that merely collecting statistics from victims is a good idea. Once the victims discovers (usually at the end of a timewasting and painful reporting experience) that no action will be taken – they will never in future

report any more crimes, because they know there is no point. They will tell their friends not to bother too, because they now know that there is no point – that the money is lost – that nobody will do anything about it.

This in turn makes the collection of those statistics pointless – you no longer have any true representation of the scale of the problem.

When the 2020 Strategy goes into effect, there must not be any reporting entity in Australia that is not actively committed to taking action on each and every report they receive. Without this requirement, there can be no useful purpose to any kind of reporting at all.

Recommendation 13: Ban the public sector from building their own cyber-security products and services.

Cyber security is extremely complex, and requires experienced experts to get everything right. There are simply not enough cyber workers in Australia to expect that the public service would ever have access to the experts they might need to build quality solutions.

In addition, it is inappropriate to use taxpayer funds to hire expensive contractors and more public servants to build things that directly compete against our existing industry products and services.

Government projects routinely cost 10 to 1000 times more to make than if they had just purchased an industry solution in the first place. Government ICT projects almost always fails, usually at spectacular expense, are never properly secure, are never commercialised, are usually duplicitous, and rob Industry of jobs, income, adoption, commercialisation opportunities, and rob the Australian Public of quality secure services, and online protection.

Government are not under any obligation to (and routinely do not) comply with consumer protection laws. They have no effective oversight or auditing. There is almost no compliance with the ISM and other security standards, there are no penalties for refusal to comply or for failure, and no transparency.

According to ASD reports, cyber intrusions into Government Systems outnumber all intrusions to every other system combined – a rate of 4 new intrusions every day, with each one taking an average of 9 months before discovery. Reports about the scale of cyber problems in government are routinely classified, are not available under FoI laws, and public servants regularly mislead inquiries, publish false public compliance statements, and simply cannot be trusted to follow adequate cyber practice.

The only way to deal properly with such a massive problem is to outlaw it entirely. Industry are experts at what they do. Buy and use their products and solutions – unlike government, industry are accountable, laws do apply to them which they must follow, penalties do exist for non-compliance, and they have access to genuine experts in their fields.

Recommendation 14: Discontinue the suppression of senate-inquiry submission records.

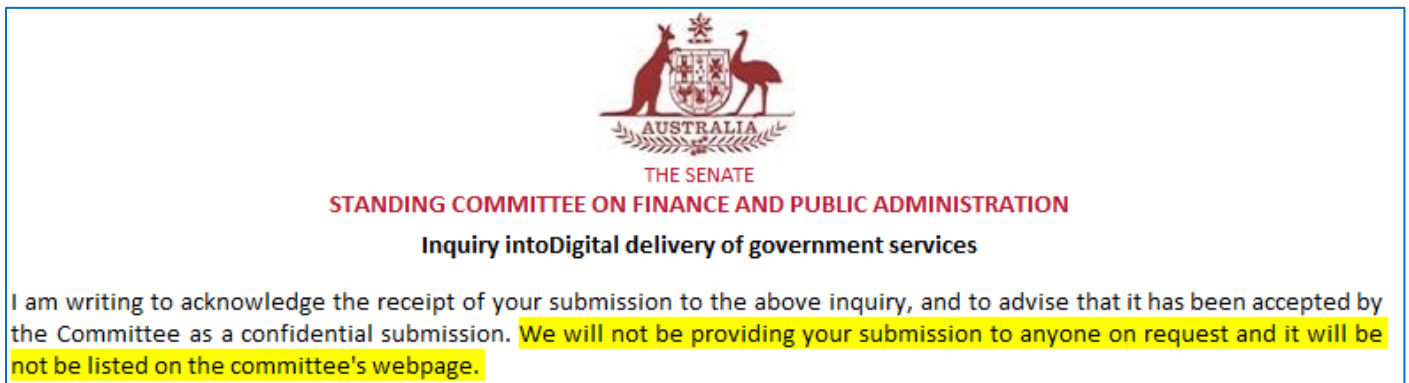
All records of me having made cyber-security-related submissions to the following senate inquiries have been deliberately hidden.

- Senate Inquiry into the 2016 Census.
- Senate Inquiry into the Digital delivery of government services.
- Senate Inquiry into the Future of Work and Workers.
- Senate Inquiry into the Circumstances in which Australians' personal Medicare information has been compromised and made available for sale illegally on the 'dark web'.

The fact that submissions can be “deemed confidential” and completely censored (rather than published with redactions) is itself highly questionable, but the widespread practice of **deliberately destroying the records of submissions as well** is an unmistakably corrupt practice.

It is bad enough that the public service itself are in charge of managing senate inquiries into public service disasters, but when they are given carte blanche to totally suppress everything that makes them uncomfortable, including all records of themselves engaging in this practice, it goes far beyond acceptable. Everyone, Senators and the general public alike, absolutely have a right to know how often this suppression practice is taking place, and against whom this power is being wielded. It’s bad enough that our country has a near totally dysfunctional Freedom-of-Information system along with near zero transparency on government operations, but when even the very practice of oversight itself is being so widely corrupted, action needs to be taken to prevent this continued abuse of process!

One example:-



Recommendation 15: Discontinue all suppression of public submissions relating to cyber security.

Along with the above submissions, all of my other submissions to public cyber consultations, have also been suppressed, as will almost certainly be this one I’m writing now as well (Before working on this submission, I wrote asking the Department to guarantee its website pledge: “Responses received will be made publicly available.”, but in their reply they refused.).

All public submissions to government inquiries, reviews, and consultations should be published. If confidential material needs to be suppressed, there should be a formal review process (with rights of reply and appeals) and any censorship should use “blacking out”, instead of the existing practice of a total cover-up of submissions.

Recommendation 16: Convene a royal commission to investigate misconduct throughout the senate inquiry process.

Senate inquiry proceedings are broadcast online. This should be a rare opportunity for the public to gain insight into the oversight process of their government, and how it operates. It should also be a place where public servant misconduct should be brought under a microscope, so they can learn from their mistakes, and implement change to improve their systems, like their severely-lacking cyber security practices.

From the questions and answers posed in the inquiries I have participated in to-date, it is abundantly clear that my submissions were neither read nor considered by Senators. Post-hearing, I made contact to ask if senators received my submission at all, and no Senator was able to confirm they did.

Additionally, my requests to appear as a witness at inquiries were denied, and the deliberately deceptive and outright malicious responses from some of the department heads under questioning was nothing short of disgusting. Frequent blatantly-false answers were given and never questioned, important questions were conspicuously avoided and the “avoidance” accepted as an “answer” (for example: the question “Was the department in compliance with the ASD mitigation strategies” was answered with a long-winded explanation of what the ASD mitigation strategies are, with no mention whatsoever of compliance [my suppressed-submission detailed dozens of items of non-compliance, with evidence] and no answering of the question; and this was accepted as an “answer” and the topic moved on). Third parties (such as Industry in general) are routinely (and often wrongly) blamed for failures, but are never given right of reply.

Ultimately, these inquiry findings are catastrophically flawed, having been based on blatantly false testimony, missing submissions, refused witnesses, and “zero interest” questioning, yet the useless findings that result go on to become part of Australian government policy.

The process is utterly broken, and desperately needs fixing.

More than a year after each of the 4 inquiries I participated in had ended, **all** of the many cyber-vulnerabilities that I had detailed in my submissions was still active and unpatched on government systems.

Recommendation 17: Resume the publication of ASD security reports.

The Australian Signals Directorate produces reports on the state of cyber security throughout government. Several years ago, these ceased being made public.

There is a general culture throughout Australian Public Service to withhold and censor all material that is embarrassing in nature. This needs to end. There are already no penalties for non-compliance, no repercussions for failure to adopt adequate cyber practice, and no oversight mechanisms (most cyber-related departments are exempt from the FoI act, and those who are not, openly violate FoI principals and simply deny all cyber-related requests and refuse to release anything embarrassing). The current practice of “blanket-ban” on government cyber-failure-publicity is robbing our nation of the only incentive that used to exist to help encourage agencies to be secure.

Bring back these reports. The ASD themselves express frustration at having no working mechanisms to compel departments to adopt their advice – these reports can make a big difference.

Recommendation 18: Extend mandatory intrusion reporting to all Government departments.

The cover-ups are preventing remediation, and there is already no penalty for failure or non-compliance. The fact that the word “security” is involved typically provides everyone at-fault the perfect excuse for hiding their mistakes. There needs to be public reporting of all incidents. No other method exists that is working to bring departments into compliance. Public ridicule is a powerful incentive – use it to keep us safe.

Recommendation 19: Amend consumer protection and competition laws to include Government.

It is grossly unfair that industry has to compete against government in the first place (for example – when government decides to build its own cyber security and identity solutions, instead of just buying already-built and working solutions from Australian providers), but when the Government does not have to abide by normal consumer rules, it's doubly unfair.

For example – DTA marketplace price-caps would be illegal² if they weren't Government. "Clear and reasonable rules that protect consumers and keep risky businesses out of the market are good for everybody." (p.11) – **this needs to apply equally to Government.**

Recommendation 20: Hold business responsible for losses of their customers.

eBay does nothing to take-down obvious scams. Telstra does nothing to prevent scam phone calls. Banks do everything in their power to shift losses to their victims. None of those businesses buy cyber protection for users, because they believe it's cheaper and easier to avoid/insure the losses – blatantly disregarding the costs this imposes on their victims.

A business is obliged to provide profit to shareholders, but not obliged to offer protection to its customers. This is precisely the problem that the concept of "legislation" exists to solve.

For example – Chinese sellers of fake-capacity SD cards and USB memory sticks rake in \$millions of fraud dollars by selling low-value worthless devices to hundreds of thousands of Australian victims on eBay and other sites. Each victim only suffers "tens of dollars" in loss (along with the destruction of whatever photos, memories, and other data they lost from using the fake device). This low-single-loss all but guarantees that nobody in Authority takes any action. (See also my recommendation 7 – someone needs to travel to China to locate the factory producing these counterfeit-capacity devices, and shut it down).

The eBay refund process is extremely time-consuming – often taking more than an hour (spread out over more than a week) to claim a meagre refund, and often only when the victim spends more money than the item cost to return it (and, breaking the law – shipping counterfeit goods by post is a criminal offence). This appears to be a deliberate decision by eBay (and PayPal) to minimise losses to their business: the greater the obstacles they place on the refund pathways, the less refunds they have to make, and the more profit they get to keep. This also explains why I have never been able to convince eBay to take down the dozens of low-value scams I have identified and tried hard to get them to remove.

Enough is enough. When just one victim suffers a crime that has been facilitated by an uncaring provider, that provider needs to be held fully responsible for the losses of that crime, not just to the victim who reported it, but to every other victim as well who did not take the time to deal with the reporting process. When eBay knows a seller sold 1000 fake memory cards, it needs to refund all 1000 buyers as soon as just one buyer proves one was a fake.

This, and all similar situations, needs to be law.

Recommendation 21: Introduce mandatory, publically-audited, minimum cyber security requirements for companies and government departments handling personal data of Australians.

These mandatory requirements need to include making the option of AAL3-strength logins available to all customers, using best-practice TLS website security on all pages, operating telephone mutual-authentication for inbound and outbound calls to prevent scammers and imposters, mandatory digital signing of code and applications they supply to consumer computers and connected devices, and so on.

The vast majority of all cyber-crime is easily prevented, but the companies and governments in a position to deploy prevention have no incentive to do so. Put this incentive in place.

² See <https://www.accc.gov.au/business/anti-competitive-behaviour/cartels/price-fixing>

Recommendation 22: Fix government scrutiny and compliance.

This statement: “Government’s activity is also regulated strictly by law and subject to extensive external and independent scrutiny to protect the privacy of Australians” (page 9) needs serious examination: who said it? What makes them think this is true? Why is this in direct contradiction to every experience I’ve had? – If there really is any scrutiny at all, it’s either wrong or being ignored (if you talk to the ASD, their #1 complaint is that departments ignore them).

This is a HUGE topic. I invite you to read my 5 attached recent submissions (all suppressed) to senate inquiries and reviews for extensive examples of Government non-compliance with laws and standards, and strong evidence that no scrutiny is taking place and little to no corrective action is being taken.

Recommendation 23: Fix government procurement.

Australian cyber vendors should not have to find every department who needs their protection, and deal with the lengthy sales and crushingly difficult procurement process.

Those departments should KNOW they need to secure themselves, and should actively seek out our solutions and buy them. The DTA marketplace is totally dysfunctional – almost the only thing departments can buy, are contractors to build new solutions that compete against industry!

See also – my reform recommendations for the ASGN – someone needs to survey our industry, so government can be provided with an Australian-supplier-catalogue of products and services to choose from.

Recommendation 24: Amend the ASD advice.

ASD advice exists that bans the use of “strong security” techniques for low and unclassified purposes. This needs to be changed. “strong” does NOT mean “slow” or “expensive” or “inconvenient” or “hard” etc – all advice discouraging “best practice” in all situations needs to be removed.

In addition, I strongly question the appropriateness of using “risk analysis” methods for determining cyber protective requirements. It is simply impossible to adequately determine the cost to individuals of the compromise of their personal information, or for any layperson (including many cyber-trained professionals) to fully appreciate the breadth of different consequences behind a breach. The word “risk” itself is also ambiguous; a breach risks both department reputation, and typically also many other 3rd parties, and with such a staggeringly vast arsenal of attacker techniques (including misusing stolen information in confidence tricks) it’s utterly impossible to appreciate the full extent of risk to those parties. (simple example: a pet-registration database might seem low value to a council, but an attacker can use that in dozens of ways – such as bypassing victim passwords by exploiting recovery mechanisms that asked “What is the name of your Dog”)

Best-practice highly-secure modern cyber solutions are often less expensive, faster, easier, and always more secure than most legacy ones. There is no excuse for using risk-management methodologies to produce excuses for allowing legacy low-security protection of anything.

Prevention is always the best strategy. It’s not difficult or expensive to simply specify “the best” in almost all circumstances. Discontinue accepting compromise – it’s unnecessary and counter-productive.

There are many other questionable items of legacy advice from the ASD. It would be a good idea to convene a committee in collaboration with industry to update this advice to accommodate contemporary technologies and solutions.

Recommendation 25: Comply with the ISM³ and all ASD Essential recommendations.

To the best of my knowledge, there has never been an audit that has demonstrated full best-practice cyber compliance of any government department – State or Federal. The most recent 3 audits I am aware of are here: <https://www.qao.qld.gov.au/report/managing-cyber-security-risks> - all 3 departments were easily breached, and as usual - none came close to adequate compliance.

Functional auditing and severe penalties for non-compliance need to be put in place – I’ve tried extremely hard for many years, and on more than 100 occasions, to try and get half a dozen departments to comply with some rudimentary and basic best-practice cyber security, with no success. The practice of ignoring the problem and refusing to comply needs to end, and this can only happen when consequences are introduced for failures.

Recommendation 26: Roll out mandatory TLS across all .gov.au domains.

HSTS, HPKP, and Expect-CT should all be enabled for the entire gov.au TLD and all subdomains.

There is no excuse for not using TLS in 2019 and beyond – these security technologies will force all departments to be secure, whether they like it or not (and, the bulk of government departments do not like it – but they should never be entitled to their misguided opinions when citizen identity/security is at risk).

Update Oct 2019: the latest ISM makes ubiquitous TLS mandatory “Security Control: 1552; Revision: 0; Updated: Oct-19; Applicability: O, P, S, TS **All web application content is offered exclusively using HTTPS.**” – so enabling HSTS/HPKP/etc across all gov.au domains will guarantee that all departments are compliant!

Ubiquitous TLS on gov.au is a minor adjustment that can easily be made in less than one day of effort. Any department that does not already support it will find their web site temporarily stops working, at which point they can follow the simple and free instructions that make their site secure – and bring them into ISM compliance with control 1552 above.

Recommendation 27: Overhaul the Freedom of Information (Fol) act.

There are too many exemptions in place that allow (and are increasingly now used by) departments to cover up embarrassment, despite this practice being clearly and specifically banned in the Fol act itself.

There are also too many departments with broken cyber security who are not subject to the Fol act at all.

There are government-owned “commercial” entities that compete against Australian businesses and handle Australian personal data on behalf of government, who are also immune to the Fol act.

There is no working review process for Fol violations, and from the recent experience of myself and others, there is a sudden shift throughout the public service to deliberate non-compliance with the act (complaints about Fol compliance violations have doubled in the past 12 months).

³ See <https://www.cyber.gov.au/ism>

No lawyer should ever be involved in any FoI request: it is an insurmountable conflict of interest – the duty for which lawyers are employed is to protect an agency, while the letter and intent of the FoI act is to release information, even which is embarrassing, about the agency.

There needs to be a department of FoI, staffed by officers who are not affiliated with the departments who receive FoI requests, who should travel to those departments to oversee the fulfilment of the requests and compliance with the act.

It is grossly unfair to expect public servants who have made mistakes, broken laws, refused to comply with cyber standards, or engaged in other wrongdoing, to be forced to engage in the handling of FoI request that seek to shine light on their own misbehaviour. As it stands, those miscreant persons are abusing the FoI process to protect themselves, confident in the knowledge that there are no penalties for violating the FoI act, and no laws that exist to compel them to comply with review directions (if any review ever gets done, which take more than a year to begin anyway).

Recommendation 28: Reform official Government cyber-security roles.

It is mandatory for many departments to have Information Technology Security Adviser staff (ITSA)⁴. Unfortunately, within the departments having the poorest cyber security practices, these roles are either unfilled, or have unsuitable personnel in them:

- All department ITSA roles should be made known to the public,
- all ITSA roles must be staffed,
- all ITSA staff must be properly qualified and those qualifications made public,
- unqualified persons should never be permitted to provide cyber advice – not to the department, and not to the public on behalf of the department either,
- all cyber advice provided to the department and the public be attributed: the large number of blatantly false security representations made by departments to Australians is disgusting, and in every case I find, advice is always anonymous, and every investigation I've made has lead to the department refusing to identify who supplied the advice. This reveals to me the fact that these departments almost certainly fully understand that their advice is false, thus refuse to identify the source as a result.
- ITSA staff be required to accept cyber-security and privacy reports and complaints directly from the public,
- Staff be compelled to act on all cyber reports within a reasonable and short timeframe,
- that all cyber reports received be published within a short and reasonable time frame after remediation, and always within 3 months of reception, whether or not remediated, or at least in compliance with best-practice global vulnerability reporting standards.
- no cyber reports be disregarded/hidden/ignored or otherwise not acted upon or reported.
- A rapid and functional process be implemented to remove dysfunctional ITSA role-holders.

Those sound obvious, but are almost entirely not taking place in the majority of government departments.

Recommendation 29: Mandatory cyber auditing (with no self-reporting).

Every department touching identity information should be required to undergo annual compliance auditing against all mandatory ISM controls, by a competent party not affiliated with the department, and be fully compliant with all

⁴ See for example: https://www.dpc.sa.gov.au/data/assets/pdf_file/0003/47442/ISM-guideline-4b.pdf

strategies to mitigate cyber security incidents (not just the top-4, or essential-8, but all of them.

<https://acsc.gov.au/infosec/mitigationstrategies.htm>).

All these audits must be published, a mechanism to receive public submissions objecting to misleading or false audit findings should be established, misleading auditors be banned from conducting further audits, and penalties need to be imposed for failure to comply.

Suggested penalties might include:

- Remove staff from roles
- Transfer of staff away from departments
- Demotion of staff
- Permanent prohibition of staff from holding any public service cyber roles in any departments
- Staff dismissal when deliberate misconduct is found (such as making false public statements about compliance)
- Mandatory destruction of identity information until such time as compliance can be adequately demonstrated

Recommendation 30: Prohibition on sharing identity information with non-compliant departments.

No identity information should ever be shared with any department that does not have a current and fully-passed cyber audit. Any reports to or by an ITSA providing evidence that any department is in breach of their security requirements should result in the immediate revocation of their compliance, and the immediate cessation of identity sharing, and destruction of identity information held by that department.

Recommendation 31: Repair cyber-response capability throughout government.

There urgently needs to be a non-government process or perhaps an open royal commission with strong powers and penalty tools to undertake a repair of the near-total lack of cyber security response capability throughout government – my work is just the tip of the iceberg; a more thorough process needs to be undertaken to find all the other problems which are being covered up, and to repair them all.

Recommendations relating to “Enterprise, innovation and cyber security”.

Recommendation 32: Providers need to do more to protect users.

It is imperative that providers do more to protect users. It’s not difficult, nor expensive, but they just don’t. In my experience, the reasons they do not adequately secure their users include:

- Too much victim-blaming advice exists, giving them the impression that security for customers is not their responsibility.
- They do not have any formal requirements to protect their users; they have a duty to their shareholders, not their customers.

- Staff are usually more concerned with their own reputation, than security. They don't use new products that offer better protection, because they are too afraid to change.
- Sometimes they fear that user-experience might be negatively impacted, or customer on-boarding might be hampered. Neither of these are necessarily the case; and even the alternative – making best-practice security available but optional, is regularly refused.
- “Me too” mentality pollutes the industry – no matter how obviously poor solutions are failing to secure (eg. SMS for baking), and no matter how many experts explain how certain technologies are broadly useless, providers keep offering little or no or useless security solutions. For example – more than 15 years ago, Bruce Schneier, the world's most respected cyber professional, debunked the 2FA myth: https://www.schneier.com/blog/archives/2005/03/the_failure_of.html - yet today, this flawed and near useless idea from 1984 is almost exclusively the only “better security” anyone offers besides passwords.
- Common sense does not exist. Inexplicably, nobody seems to question bogus cyber advice, nobody bothers to test cyber claims, nobody pays attention to the causes of past cyber breakins, and nothing actually improves.

My recommendations (3, 4, 9 and 10) for action that government can take to solve this problem appear above.

My advice to Enterprise is for Management to take on high-level oversight of the cyber process. Security staff are simply not equipped to make security deployment decisions. They need to be told by their management what kinds of threats to protect against (such as: offer protection to their customers), because right now, cyber staff are refusing to do this.

Recommendation 33: Comment on equipping purchasers to protect themselves.

(Discussion paper page 11). A purchaser can never be adequately equipped to protect themselves. The nature of most modern threats makes the idea of such protection an architectural impossibility. The only feasible way to defend the vast majority of cyber-attacks is to introduce protection at the provider end. One of many examples - unless the provider offers a solution, there is simply no way an end user could use any other solution and be protected against provider-impersonation attacks – the root cause of most modern losses.

I disagree with many statements made on page 11. “Impairment of product operation” is an unlikely possibility – so remote it's possible that no such situation even exists at all. “Cost prohibition” is never a suitable excuse for insecurity – “cost” always refers to what a provider needs to expend to be secure, and never includes the losses or remediation costs a victims suffers as a result of that provider insecurity. If a vendor cannot cost-compete in a marketplace with a secure product, they should never be allowed to enter the marketplace with an insecure one as a compromise. That said – good security really is not expensive; vendors just need incentive to incorporate it. It is typically a small once-off development integration cost, and once deployed, usually remains in place for all the vendor products for the rest of time. “Accept the risk if they believe in the benefits” is not a sensible suggestion. Practically no customers will ever exist who fully comprehend the nature of cyber risks – what might seem a low-risk option to them, might well be the insertion point for malicious activity that has devastating consequences far beyond anything the customer could have imagined. In many situations these days, the purchaser of products is using those products to protect the information of their own customers. “Accepting the risk” is not a simple statement, because the “risk” applies not just to the purchaser, but extends to everyone who might be impacted by the security failure of the purchase.

Recommendation 34: Discard “minimising upfront costs for industry” wording.

(p. 12). Australians reported unrecovered losses exceeding \$1bn over the last 2 years, and the total cost of cyber-crime is reportedly \$29bn annually. It makes no sense to include language about minimising costs, particularly when the losses being suffered as a result of cyber-cost-avoidance is currently being borne by others (the users of industry services – not by industry itself).

Government exists principally to protect its citizens. Restrict your language to this purpose. Industry will deal with whatever costs are necessary, and always keep in mind that a “cost” to secure a business directly translates to “revenue” for a cyber security provider. This is a good thing: it provides employment, growth, improving protection, and new products and services to keep us even safer in future. Penny-pinching compromise and ineffective freeware junk-security are necessarily avoided if we genuinely seek long-term benefits for society

Industry money-saving at vast public expense is unacceptable.

Recommendation 35: Best practice Identity and Authentication must be made available to all.

The NIST SP-800-63 series (e.g. <https://pages.nist.gov/800-63-3/sp800-63b.html>) offers current best-practice guidelines on many effective cyber security techniques.

Enterprise needs to be compelled to make strong security at least an option that their discerning customers can adopt when they so wish – such as, for example, Authentication-Assurance-Level-3 (highest) protected logins.

Recommendation 36: Software goods must be digitally signed.

It is not expensive to get verified and buy code-signing certificates. Vendors need to be compelled to offer this protection when delivering software goods to Australian consumers. Without signatures, goods can be trojanised or substituted with malware, and/or customers be required to disable their security in order to use the product, greatly increasing their exposure to other security threats as a result.

Recommendation 37: Mandatory security update provision.

Companies that are failing to provide security updates (e.g. phone firmware, SIM card replacements, routers and modems, baby monitors, TV’s and IoT devices, etc) should be charged a fine, and that fine spent on updating or replacing the insecure products. Australia passed a law letting us force anyone globally to reduce their security and insert back doors – a new law forcing the enhancement of security and the fixing of security problems is far less controversial!

Recommendation 38: Remove Digital-Identity-Services from Government.

Private industry, not government, should be tasked with the broadest possible set of roles and functions for digital-identity.

Government is un-trustable, unaccountable, beyond reach of laws and penalties, and has repeatedly proven incapable of implementing even the most basic of security protections for identity information (Case in point: the DTA's TDIF failed every single assessed criteria of its privacy impact statement).

Government are far more capable at compelling private industry to comply with laws and have penalties and protections in place to enforce them, and private industry are far more capable of being cyber-responsible than government, as well as more likely to be trusted. Take the TDIF away from DTA – the current (their 4th failed attempt) is a wreck again, and enough-is-enough!

Government also never commercialise their developments, and typically produce failures at vast public expense, and rarely if ever consider the broader application of their developments.

Digital identity is a global phenomenon, and every government in the world already readily adopts multiple industry developed solutions. The same is not true for any government-developed ones – many nations deeply distrust each other, and would never accept another nation's digital identity products.

The only feasible operator of a truly globally useful, truly privacy respectful, truly secure, digital identity solution is an industry solution.

Recommendations relating to “A trusted marketplace with skilled professionals”.

Recommendation 39: Update your understanding of global industry standards.

“visible and trusted industry standards, do not yet exist in most cases.” (page 13) – not true - AAL3 Authentication for example, the NIST sp800 suite, EPL-listing, OWASP, etc.

Recommendation 40: Trust.

The word “Trust” is frequently used in security, but is difficult to define or enforce, and is a huge and growing problem among vendors.

Many vendors lie, deceive, or twist truths, and most providers (including government) do **not** do what they say (they only pretend to be secure or care about security, when the truth is different - they do not care about the customer, they care about themselves (and shareholders) - if they care at all.)

Foreign cyber professionals tend to vastly exaggerate their credentials and experience, if not be outright deceiving in their CV's. This is common overseas practise. Australians are often the opposite – playing down their skills and experience (tall poppy avoidance).

It would be extremely helpful if a working definition of the many aspect of “trust” be developed, so when someone says something like “trusted market”, everyone knows what exactly that is supposed to mean, who verifies that trust, who enforces compliance, who audits and certifies and ensures it's appropriate and deserved.

Recommendation 41: Update cyber training standards.

Some cyber training standards are woefully outdated (I quit my CISSP when many of their lessons I knew to be wrong, and I discovered they had no mechanism to correct them!). Many industry professionals know and understand which certifications and trainings are real, contemporary, and useful, and which are outdated or irrelevant.

It would be helpful if an authoritative review of materials and their associated mechanisms (if any) for corrections and updates be performed, and for “dud” material and training and update-mechanisms to be called out, for deficiencies to be corrected, and for quality advice informing everyone of the suitability of these standards be published. It’s a good idea to train people, but a bad idea to train them with wrong information!

Recommendation 42: Buy instead of Build.

There needs to be more adoption of security technologies, and less hiring of professionals to re-invent the wheel – particularly in Government.

Recommendation 43: Mitigate the skills shortage by fixing some problems.

If better cyber products were deployed and used, and improved compliance existed, there would not be such a crushing need for more professionals.

The IMD World Digital Competitiveness rankings put Australia 53rd out of 63 countries ranked for its output of science graduates, and 44th for its digital technology skills. Under a subcategory for ‘capital’, Australia ranks 36th for “funding for technological development” and 34th for venture capital. This shockingly poor performance is unacceptable!

Recommendation 44: Penalties and liability enforcement.

There need to be more enforcement of laws, and more penalties legislated against providers who do not offer adequate security to Australians. The widespread practice of disclaiming all liability and responsibility in online “terms of services” etc needs to be overruled by legislation that makes it a legal obligation of providers to offer adequate security to Australians.

The internet is 30 years old now. The anarchistic “everyone for themselves” ways of old are no longer appropriate in today’s openly hostile online environment. Providers need to be compelled to wake up and get secure.

Recommendation 45: Survey the Australian Cyber Security Market.

Find out who is in it and what products we make, and what services we offer. Find out how big we are, where we operate, and how well we are doing. Measure this periodically, so you can understand whether our market is growing or shrinking. Make knowledge of our solutions available throughout government, and BUY our products when appropriate. Recommend our solutions to other Australians when offering cyber advice.

Recommendation 46: Sponsor Australian products through EPL listing.

Out of 1400 global EPL-listed⁵ cyber products, only 1 is from an Australian company! We make many of the world's leading solutions in cyber. Sponsor our assessment and inclusion in this globally-accepted standard for high-quality cyber products.

Recommendations relating to “A hostile environment for malicious cyber actors”.

Recommendation 47: Block threats first.

See recommendation #7 – get rid of all the confusing dozens of cyber reporting entities – re-deploy all those duplicitous staff on prevention and take-down duties.

Recommendation 48: Prioritize prevention.

There is VASTLY too much focus on detection, deterrence, and response (indeed – page 8 – does not even list prevention whatsoever!) – we need to get our priorities right:

Prevention is better than cure!

Ensure that Prevention always comes first in all cyber advice and initiatives.

Recommendation 49: No expanded law capability is needed.

We already have adequate laws, but these existing capabilities' are simply not used right now (and are mostly unreachable)

Drop the idea of expanded powers, and invest in encouraging existing powers to actually be used (see recommendation #7 – amalgamate the duplicity)

Recommendation 50: Properly designed digital identity promises to all but eradicate online crime.

The world still needs a working, privacy-respectful, digital identity infrastructure. Experts and industry need to be engaged to design and build this.

With strong working Identity, almost all online crime (and a lot of offline crime too) is eliminated.

Nearly all crime depends on the perpetrator's identity being hidden. A working global digital identity solution would help prevent unacceptable anonymity, making scams inoperable, making malware almost impossible, identifying hackers and terrorists, and defeating almost all forms of fraud. Modern cryptographic solutions exist to make this strongly privacy-preserving and highly secure. Tech exists so can prove “you are you” without anyone knowing who you are or tracking you, while still (and only when necessity permits) facilitating your actual identification in emergency or terror situations.

⁵ See <https://www.cyber.gov.au/publications/evaluated-products-list>

These solutions need to be made available by industry, and consumed and championed by government, and in so doing, promise to almost entirely eliminate global fraud and cyber-crime in the process.

Recommendation 51: Cyber-insecurity levy.

A levy or per-customer tax or other kind of “mitigation fee”, charged to all companies providing inadequately-secure services (e.g. no AAL3) to Australians needs to be imposed. Presently, online providers are not obliged to protect their customers. This is a big problem, since they are the only ones in the position to offer adequate protection. A fee charged against them would provide the missing incentive they need to offer that security, as well as revenue that could be spent helping any less capable ones to achieve compliance.

Recommendation 52: Penalties imposed on attack supporters.

Australian operators and foreign operators with Australian presence, who support attacker infrastructure (e.g. Amazon hosted penetration scanners, Go Daddy-registered websites hosting unauthorised vulnerability exposures, ISP’s facilitating DDoS attacks, VPN providers refusing to identify fraudsters, etc) should be required to receive attack reports from victims, and to expediently remove the attack, identify the perpetrator, or destroy the offending infrastructure. Those operators should be handed heavy fines for non-compliance or unnecessarily delayed response.

Presently, there are little to no disincentives for operators to take any action against attackers, and in my long history of attempting to take down more than 100 different kinds of attacks and frauds around Australia and the world, the #1 response I receive on practically every occasion is “Sorry, we can’t do anything because of customer privacy”. Their public response is to protect the privacy of the criminal and allow the attack to continue, instead of curbing the damage that their systems are permitting. Attacks rage on with the full knowledge of the operator facilitating them in the vast majority of the large number of situations I have first-hand experience of.

Recommendations relating to “A cyber-aware community”.

Recommendation 53: Totally discontinue your blame-the-victim approach.

The entirety of your “cyber aware community” discussion paper section is blatantly offensive. This is **completely the wrong approach**.

It is obvious beyond any doubt that the idea of expecting millions of ordinary Australians to all become cyber experts is completely ridiculous. Your page 17 lists a panel of 4 insulting statements ridiculing everyday people for not doing or knowing something that should never be their responsibility in the first place.

There is NO POSSIBLE WAY that any initiative to “help people secure themselves” can succeed. You can never reach them all with any message. You can never design any message that could be suitably understood. The vastness of the problem makes it impossible to educate them properly. They could never possibly remember it all even if you tried. And, worst of all, there is NOTHING THEY CAN DO that could generally be considered “effective” against any modern sophisticated adversary anyhow – you cannot educate them, because they simply do not have the opportunity to secure themselves. It is a cyber-architectural impossibility.

The ONLY way that Australians can be secured, is when adequate security is adopted and offered to us by the providers of the products and services we use.

The entirety of this “cyber-aware community” messaging needs to be flipped on its head – and converted into a campaign to educate the people in a position to protect us (providers), so they know they can and should, because it is ONLY they who can.

Refer to my recommendation #3 for more details.

Recommendations relating to “Other issues”.

Recommendation 54: Discontinue behaviour-change campaigns.

As above (53) and recommendation 3:

“best practice behaviour change campaigns” (p.17) – is the wrong approach. Stop blaming the victims – it is not their fault, and they are not in any position to fix it.

A note about insurance.

Insurance is not doing what you think.

Cyber-insurance is providing a mechanism to industry for the cover-up of cyber reporting. It facilitates the transfer of intrusion costs in accounting systems to conceal the extent of breaches and serves to keep shareholders in the dark regarding inadequate company cyber protection.

Insurance provides a safety-net which makes it “OK” for companies to remain insecure. Safe in the knowledge that their costs will be covered, they are free to avoid the now unnecessary expenditure on adequate protective solutions.

Insurance worsens the outcomes for customers and end users. The role of an insurance company, same as any, is profit for shareholders. The most effective cost-reduction method for insurance is to shift losses to other parties, which in the case of cyber attacks, means away from themselves and who they insure, and on to the victims. The presence of cyber-insurance is exacerbating user losses – contributing to increasingly oppressive language in terms, to increasingly ruthless refusals to compensate for losses, and to reduced transparency.

A note about Telstra.

Telephone scams are a vicious contributor to Australian cyber and fraud losses. I personally receive frequent scam calls, and I personally know many elderly (and other!) victims who have suffered huge and un-recovered losses. I frequently make attempts to get Telstra to take-down offending infrastructure, and to install spoofing protection that prevents imposter message-ID transmissions, and to disconnect or blacklist the incoming overseas infrastructure responsible for these calls. In every one of my many and long attempts, I have been met at every turn by ruthlessly obstructive behaviour from both Indian and on-shore Telstra staff, and abject refusals to take any action.

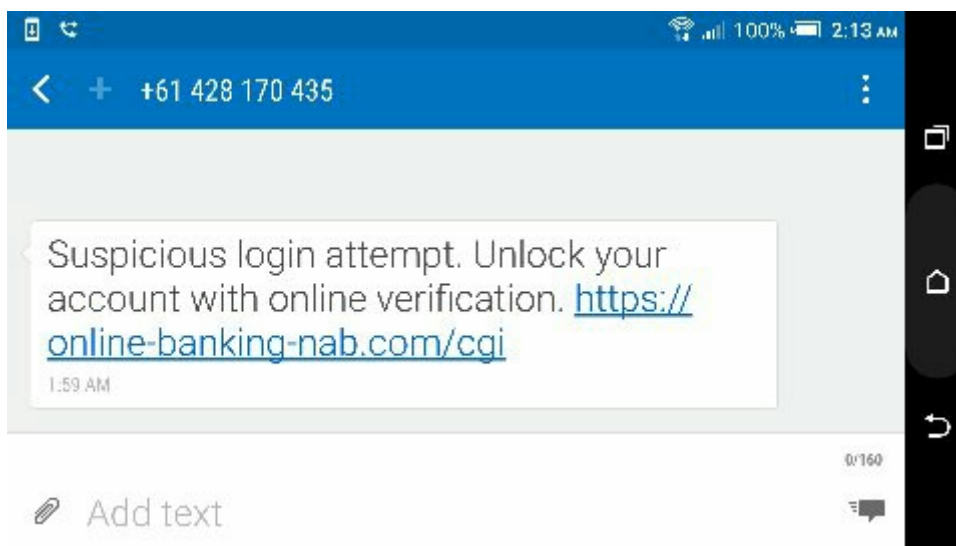
The sheer callous refusal to take any action to curb the staggering losses that their inaction facilitates beggars belief.

Urgent action is needed to punish Telstra (and maybe others – I've not looked at the others) for the losses that their tolerance of these scams is causing.

One suggested punishment is to enforce a deadline by which they must demonstrate a working and rapid response to all scam call reports, and to cover the cost of any and all infrastructure spending necessary to make that possible, with significant financial penalties for non-compliance, for lateness, and for operational failures, with the obligation to repay losses incurred by subsequent victims should Telstra fail to timely take action to prevent repeat offenders.

It is in the Telco power to end this scourge, and they are showing no signs whatsoever of voluntarily doing so. It is long past due that they be compelled into responsibility.

Update – within an hour of writing the above, I received the following phishing broadcast, sent my SMS Text message, a Telstra mobile subscriber number. Earlier today, I spent an hour on the phone to Telstra support pleading for them to take down a voice phishing caller who also called me. The operator admits that they receive huge volumes of complaints about this same issue, but point-blank refused to do anything, refused to escalate my complaint, refused to take the details, refused to identify his manager or any other more senior staff, and supplied bogus technical information relating to how Calling-Line-Identification technology works (I questioned him after his fake excuse, upon which he then admitted he has no idea whatsoever of how that technology works). This strongly suggests that Telstra staff have been directed to lie to customers about fraud issues, and to put forward false-impressions that they cannot do anything, using fake technical pretences.



(Yes, I was up past 2am working on this submission)

Chris Drake's Comments relating to Australia's Cyber-Security Strategy 2016 & 2020.

Our 2016 policy, its update, and the 2019 "Call for Views" contained alleged and encouraging "progress" and other statements, but overlooked including all the failures.

In my experience, this is a common theme in Government publications:-

- There is little or no examination of failure.
- This is far too much spin doctoring of alleged "achievement", and most cyber-security rhetoric (especially government) bears little resemblance to actual reality.
- Measurement is not taking place, or is being suppressed/classified. When no empirical study of the efficacy of actions is done, nobody can possibly know if their actions are working!

My observation of failures from the 2016 strategy:-

I should not have had to do this – your discussion paper should have included all failures AS WELL as the alleged successes. Not knowing that it failed is itself a fail (failure to measure).

Page 3:-

"this Strategy will help bring more Australian technologies to market" – did it? Can I see the list?

"boosting STEM participation" – did it? Are there numbers? My google search today shows no fix.

"support and create innovative Australian companies." – how was this done? Where is the list of who benefited?

"The Government will show leadership" – where are the statistics measuring government cyber incidents?

ACSC – "will ensure cyber security is given the attention it requires" – is there a report? What incidents did they attend? How many departments comply? Why do they never reply to incident reports unless threatened with FoI? Why are inquiry submission suppressed? Why are cyber reports classified?

"This strategy will develop partnerships between the Australian public and private sectors" – did it? With whom?

"... support home-grown cyber security capabilities" – did it? Which ones?

"We will change and adapt when needed" – have you? In what areas? Who decides "when needed"? What percentage of Government departments fully comply with the ISM and all ASD mitigation strategies? Who is auditing government self-reporting of compliance? Who is being disciplined for misrepresenting compliance?

"I look forward to working with [...] the private sector" – did he? Who? All my approaches were rejected.

Page 2:-

"While governments can take the lead in facilitating innovation and providing security". What innovation has it facilitated? What security has it provided? N.B. Advice is not security, especially when efficacy is unmeasured.

"The rate of compromise is increasing and the methods used by malicious actors are rapidly evolving". True and true; unfortunately, security adaptation is not happening: adoption of evolved security is not taking place, and far too much effort is going into cover-ups, victim-blaming and fake security statements instead of revealing the increasing failures.

Page 4:-

“We must embrace disruptive technologies;” which new cyber ones has Government “embraced” since 2016?

“the Australian Cyber Security Centre has lifted Government capabilities to a new level” – this, in my extensive experience, is untrue. Govt cyber capability is almost non-existent in the half-dozen departments I’ve tried to reform over the last 4+ years.

“banks and telecommunications companies, have strong cyber security capabilities” – not true in my vast experience, plus, what “capabilities” they have are targeted at protecting themselves, NOT their customers. This is not my opinion, it is my observation, plus it is stated company policy from multiple banks I’ve spoken with.

Page 5:-

“The Australian Government will take a lead role”. Who lead this? With whom were partnerships forged?

“Australia’s cyberspace must also be a shared responsibility. It will be important that businesses ... work with governments ... to improve our cyber defences and create solutions to shared problems”. Yes, very important, but HOW do we do this? Cyber-procurement is a total shambles, "build instead of buy" rules all major projects, and there seems to be no genuine consideration of "value for money". Vendors should not have to know who in government needs their products - *Government* should know they need them (e.g. because it's in the ISM or "Essential 8" etc), and they should seek out Australian vendors to buy from.

“Strategy’s initiatives will be reviewed and updated annually and the Strategy reviewed and updated every four years.” – was it? Who lead the reviews? Where can I read them? What was measured? Why was I not invited to help? Where are the updates?

“[Actions]will be co-designed with stakeholders from the private sector” – which ones were? Who from the private sector was involved? Why not me?

“Many of these actions also rely on working with all Australians—because we all have a part to play” – WRONG WRONG WRONG. This is the most annoyingly misguided advice that keeps rearing its ugly head time and again. Good Cyber Security is EXTREMELY COMPLICATED, and the vast majority of opportunities to protect everyone lay NOT with the end users, but with their providers. Telling everyone, end-users and providers alike, that it’s the role of the end-user to be safe, is educating the providers that it’s OK to keep blaming the victims, even when the providers don’t give those victims adequate security in the first place. **Individuals need to be protected.** It is blatantly irrational to hope that 24.6 million Australians can all become cyber experts to keep themselves safe. If any of them “have a role to play”, the only reason is because someone did not give them adequate protection in the first place. If you don’t know what that protection is – there is a major failure in your cyber strategy: it should NOT be the Job of a solution vendor to educate the market, least of all the government, and not at all any government purporting to provide cyber-education. That Government should know what’s out there to solve critical problems, especially when it’s Australian-Made, it should be using this itself already, and it should be promoting it, or even mandating it, to every provider who has Australian customers.

“This Strategy charts a new way forward for Australia’s cyber future, one that is creative, collaborative and adaptable.” – there is still too little collaboration, and what exists is far too one-sided (and sometime not even genuine), most severely lack transparency, and are immune to correction when wrong.

Page 6:-

“Cyber Partnership” – ministers are almost entirely unavailable, and do nothing to help in cyber situations. They do not appear to read (or maybe receive) my senate-inquiry submissions. They don’t return my emails or phone calls. Our voice in meetings does not seem to make any difference, and I am not invited to most meetings in the first place.

“We will also sponsor research to better understand the costs of malicious cyber activity” - This needs involvement of a statistician, and to get rid of the time-wasting burden placed on victims. “Doing nothing” when a victim reaches out for help, other than wasting an hour of their time collecting statistics that will never be acted upon is disgraceful.

“We will better **detect, deter and respond** to cyber security threats” – nice, but, this is missing the MOST important part: “**PREVENT**”. In my vast experience, there is also little to no “respond” taking place either.

“Australian governments and the private sector will work together to share more information” – this is broken. I’ve been *repeatedly* blocked, as have others under the excuse “vendors might obtain commercial advantage”. We make the products that keep you safe. Excluding us when you’re under attack is plain crazy.

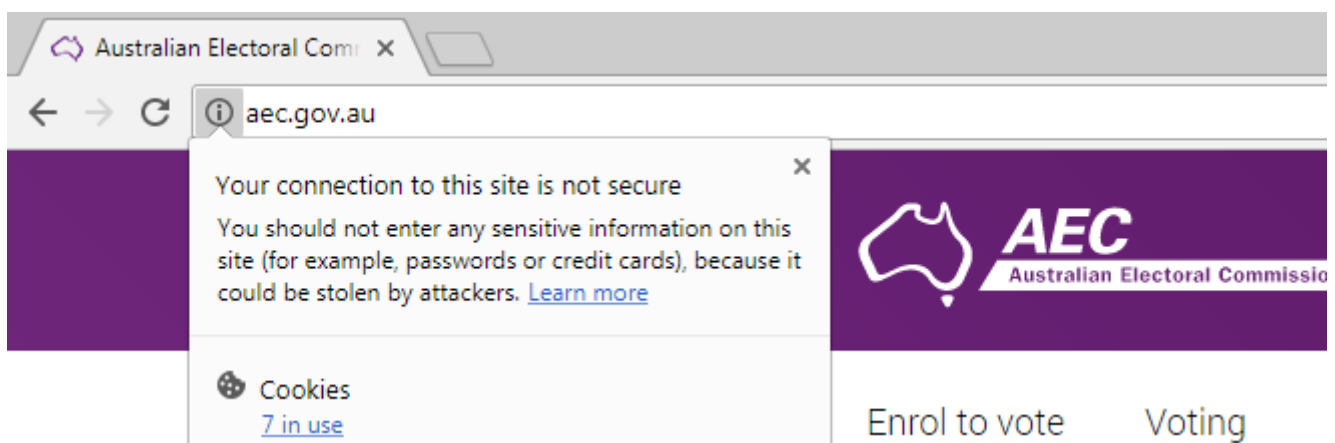
“streamline the cyber security governance for Commonwealth Government agencies and clearly identify lead responsibilities.” – in my **vast** experience to-date, this is absolutely not happening. Australian government rhetoric surrounding cyber-security practices and the handling of citizen identity information bears almost no relation whatsoever to actual department practices. Rules are almost never followed, security issues are practically never addressed, failures are covered up, inquiries are misled, and there exist no working mechanisms to correct mistakes or fix security problems. Citizens are fed blatantly false assurances regarding the cyber security posture of government departments, usually from anonymous and unskilled sources, who refuse to be identified when challenged. There are no penalties for ignoring the rules, Departments routinely refuse to correct cyber issues, and cyber testing is rare and usually fails. In the comfort of anonymous or private forums, many government cyber professionals express these same opinions, along with their frustration at not being able to compel departments to change.

- Every department I’ve contacted (AEC, DHS, ABS, ASD, former DTA, PM&C, AUSTRAC, Defence, ACSC, plus some state and local governments, and others I’ve forgotten), no exceptions, point-blank refuses to fix any of the large number of cyber security and privacy issues I’ve brought to their attention.
- Almost every department claims that they have no security problems (despite **evidence** to the contrary that I supply).
- All department claims of "we have no security problem" are unsigned, unattributed, and obviously not from any security professionals.
- All departments routinely block every cyber-security-related FoI request I make (all relate to cyber failures).
- Departments censor (remove) all controversial public comments that are made on systems they control, especially ones relating to cyber security.
- No departments I’ve found appear to have any actual ITSA or similar (supposedly mandatory) roles with staff actually in them (I did notice an advert appeared seeking to fill one of those roles after I began applying pressure - so perhaps I made one tiny bit of difference to one department there).
- Departments all refuse to identify any of their IT security staff - they refuse to name names, they refuse to provide contact details. My conclusion: they do not have staff in these roles.
- The OAIC FoI review process is a sham (backlog of 1+ years, and no power to right wrongly refused FoI reports anyhow).
- There appears to be a highly organised FoI "officer" scheme or training in place to block every request that might embarrass government from being honoured (despite the law clearly banning that behaviour).
- "Consumer Protection" laws do not apply to government: when government break them, all action I've taken to right those wrongs has resulted in department lawyers telling me the sections of legislation that make them exempt.
- All senate inquiry reports I file that embarrass government become deemed "confidential": this is a way to hide the content AND EXISTENCE of these reports from everyone - they are removed from the record, they are never available to anyone. From observation of inquiry broadcasts over the internet, senators appear not to be provided with these reports (or at the very least -they do not read them).
- Every inquiry senator I contacted failed to confirm they ever read or received my submissions.
- I never get invited to participate in anything I apply for (to give evidence at inquiries, or to participate in reporting).
- As best I can tell - all inquiry and report-writing that takes place is not genuine. This includes the PM advisory panels I did manage to be on. They have an agenda "get some law or other passed", and industry

involvement in the process is a sham - simply so government can pretend they consulted before they did what they already have planned. Our recommendations do not get considered.

- Some departments providing security advice to citizens source dubious content from the internet to base their advice on, and then refuse to be corrected when they're wrong, refuse to acknowledge evidence proving them wrong, refuse to study the efficacy or suitability of their advice, censor criticism about their flawed advice, refuse to publish corrected advice, and continue repeating their advice despite the volume of material weighing against them.
 - Most departments actively mislead the public about their security and privacy practices – for example – the DTA web site in relation to the TDIF, under the heading “How we protect your privacy”, linked to a privacy impact assessment (PIA) document – giving the false impression that this document proved that the DTA protected privacy, when in reality, inside the PIA details it actually reported that the DTA **failed every single privacy control that was tested**.
 - Australia Post, a government-owned "body corporate" existing through specific government acts, is considered a "commercial entity", and thus it is allowed to escape FoI scrutiny.
 - The Australian Signals Directorate (ASD) – our peak body informing all other departments on the topic of cyber security, is immune to FoI scrutiny too.
 - Public servants are highly misleading when appearing in senate inquiries: they fail to report their own mistakes, and they readily point to industry failures as a means to divert attention from their own mistakes, and some departments cover up the failures of other departments when questioned by senators (e.g. The ASD head, when asked in the government-service-failure inquiry if a department was compliant with ASD advice, chose a lengthy reply summarising ASD advice as his tactic to avoid answering the question, which worked).
 - The way the privacy law is written gives all departments a "get out of jail free" excuse not to fix security problems: the ASD (who provide security advice, including the operation/oversight of so-called "approved" secure cloud etc) is not the same department as the ones *with* the privacy data, so no single department has security responsibility over this data, so no department is ever in breach when it's insecure.
- A. Australian Government systems are utterly insecure (this is a well-reported fact - 62% of Australian cyber break-ins are to Government servers. That's 4 new ones every day. Sources: Australian Signals Directorate “Cyber Picture 2013” and DPM&C Strategy page 16:
- B. There is no working mechanism to fix it.
- C. There is no motivation to fix either of the above.
- D. Senate inquiries pertaining to government failures are 100% whitewash - public servants totally control these, and they do not allow exposure of embarrassment.
- E. Reviews and inquiries never seem genuine, and always exclude me and the submissions I make - uncovering public service failure appears never to be acceptable in final reports.
- F. Nobody in the public service seems accountable - there are no penalties for doing the wrong thing.
- G. The system in place to cover all that up is well oiled.

I have hundreds of documents verifying all my above claims which contain even greater numbers of embarrassing problems that the few above that I've recalled.



Here's how ASD lawyers responded to me when I submitted a privacy complaint regarding **their "security"-approved systems** being implemented with no security whatsoever to collect voter enrolment details.

" As the ASD does not have possession or control of a record containing your personal information collected by the AEC, my initial view is that the ASD is not required to take reasonable steps to protect the security of such information. "

That bears repeating in bold!

The ASD is not required to take reasonable steps to protect the security of [voter] information.

Official legal (written) public position,
– Australian Signals Directorate (our peak official body responsible for cyber security in government)

Here is an excerpt from the "First Annual Update" to our Cyber Security Strategy that came out at the very same time that the ASD and the AEC were point-blank refusing to switch on security for Australian Voters and their enrolments:-

Australia's Cyber Security Strategy: 2017 Update
© Commonwealth of Australia 2017 ISBN 978-1-925362-45-9 Australia's Cyber Security Strategy: 2017 Update (PDF)

US ELECTION INTERFERENCE



The hack and release of sensitive information from the US Democratic National Committee by Russian cyber actors in the lead up to the 2016 US Presidential election demonstrated how targeted disclosures of stolen information can interfere with processes underpinning Western democracy. The interference broke new ground for unacceptable behaviour and tested concepts around public attribution, response and effective deterrence. It also encouraged discussion over the security of electoral systems, including on-line voting.

Commonwealth of Australia, Department of the Prime Minister and Cabinet, Australia's Cyber Security Strategy: 2017 Update

This is a situation that repeats over and over and over. Government rhetoric tells absolutely false information about their actual cyber security practices, which in my vast experience are embarrassingly obviously beyond repair, even when the headlines are awash with examples of the problem.

Page 7:-

"co-design national voluntary cyber security guidelines" – these are outdated, with wrong information. They probably need to include recommendations to products and vendors to make these guidelines actually work (there is no point telling people to be secure, if you do not tell them how!).

"shut down safe havens for cyber criminals." - How many attacks reported by Australian personal (non govt, non business) Victims got shut down through these mechanisms? Is there a list of the attacks reported (e.g. phone scams, ebay fraud, ransomware, etc). Every attempt I've made to shut down scams and frauds has met with no success, and I've tried *hard*. I've worked with the FBI on USA fraud, and they got results (arrest, extradition, and 37 years imprisonment of the offending cyber-crime gang). Why can't we?

Page 8:-

“the Government will also support Australia’s cyber security sector to expand and promote their capabilities to the global market.” - Did it? Can the Government supply a list of who is in this sector, and what they do? Trick question: I know they cannot. I've never been surveyed for example... Who, if anyone, in my industry benefitted from this? Where was the promotion done? Why has nobody in my government ever contacted me for either my advice, or to use my products? How many other Australian Vendors have also never heard from anyone in our government who needs their solutions? With no exception, every successful Australian Cyber business I’ve asked (a lot) has said they owe their success to leaving Australia and selling overseas.

“With better focussed cyber security research and development” – we do not need more research – we need commercialisation; almost everything you need already exists in Australia – what is needed, is for Government to USE IT.

“Cyber Security Growth Centre” – major failure. They have never even surveyed our industry – they’re supposed to grow us, but have no idea who we are or what we do or how big the industry is, no regard for the size of our country or where vendors are located or the costs to vendors trying to use their services.

“particular focus on support for cyber security start-ups” – which ones? What support did they receive? How many government departments are now buying products from those start-ups? If none, why not?

Page 9:-

“The Government will also further improve national cyber security awareness and work to ensure all Australians understand the risks” – WRONG WRONG WRONG – see my explanation earlier (Recommendation 3).

I invite you to peruse some of the following public submissions I have made to assorted government inquiries and reviews. Every one of these has been “suppressed”, along with the records of me making these submissions.

Attachment 1: Submission to the Senate Inquiry into the Digital delivery of government services.

20th September 2017

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

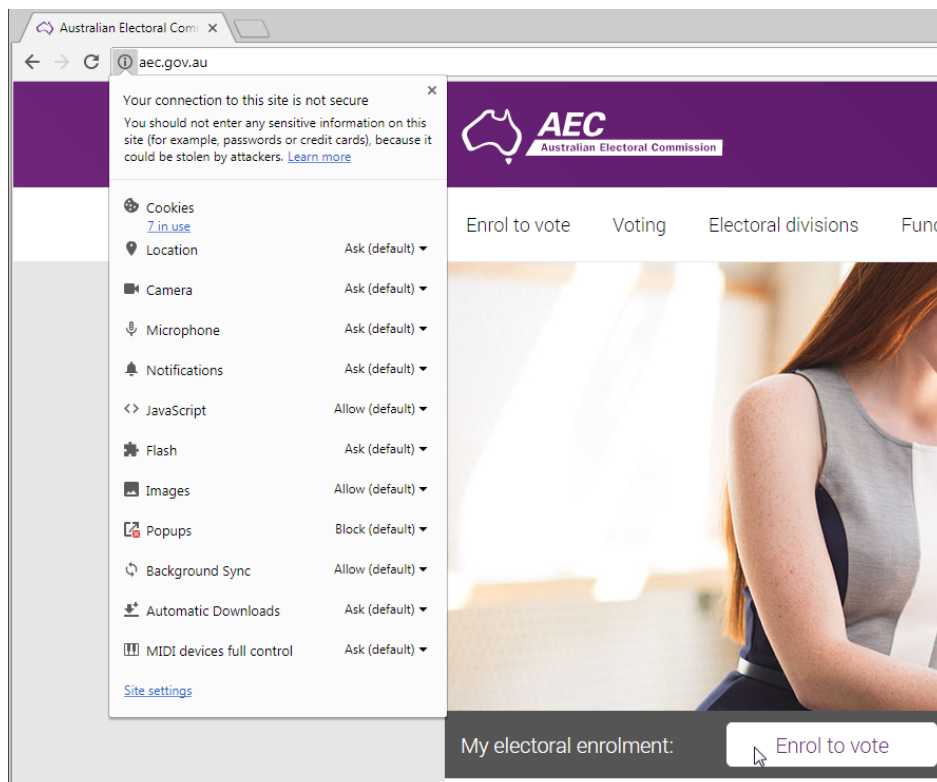
My name is Chris Drake. I am a computer security professional and expert with 35 years cyber experience, I have won numerous international cyber security and innovation awards, spoken at many international conferences on the subject of cyber security, I run multiple security-related businesses, and I 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.

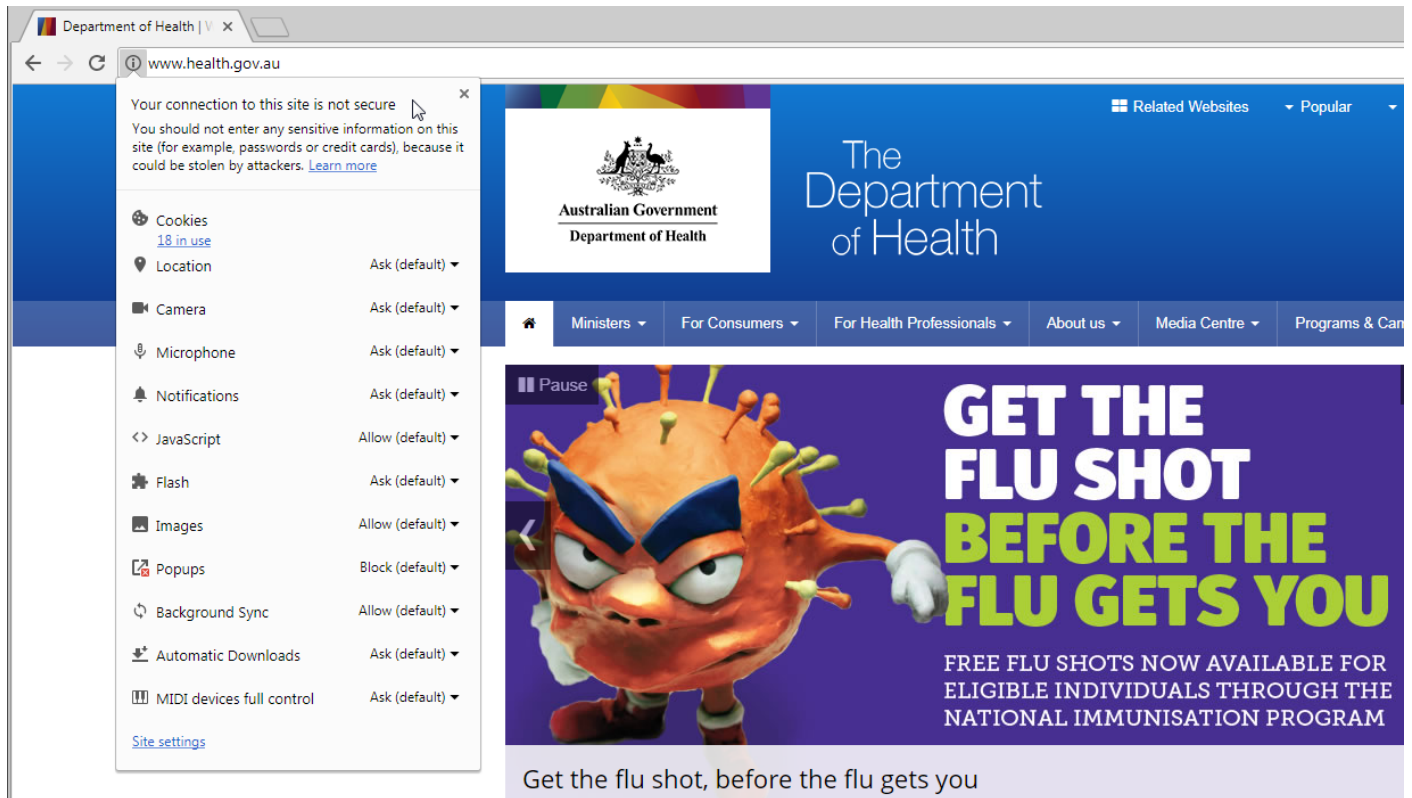
As I said in the previous section, failure to engage appropriately skilled programmers and reviewers, and failure to engage a reputable penetration systems testing team reveal systematic security failures within DHS/HPOS.

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: Cytelegic Intelligence Reports, Marc 2015 through March 2016: <http://cytelegic.com/cytelegic-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-gugpjw>

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 with 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

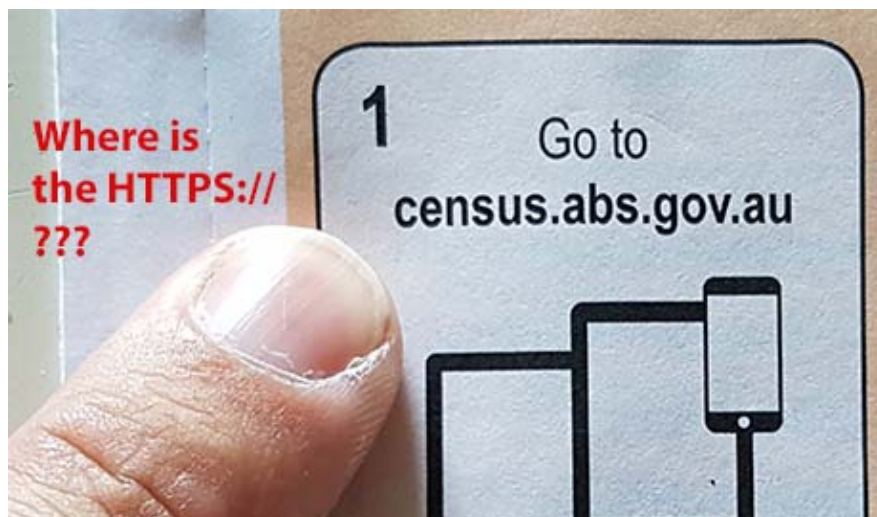
This submission covers technical security matters not present in existing submissions 1 through 90. It also covers procedural security failures again not mentioned in previous submissions. I address terms a, c, f, i and j in respect of the census web site security, and the wide ranging failure of every 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.

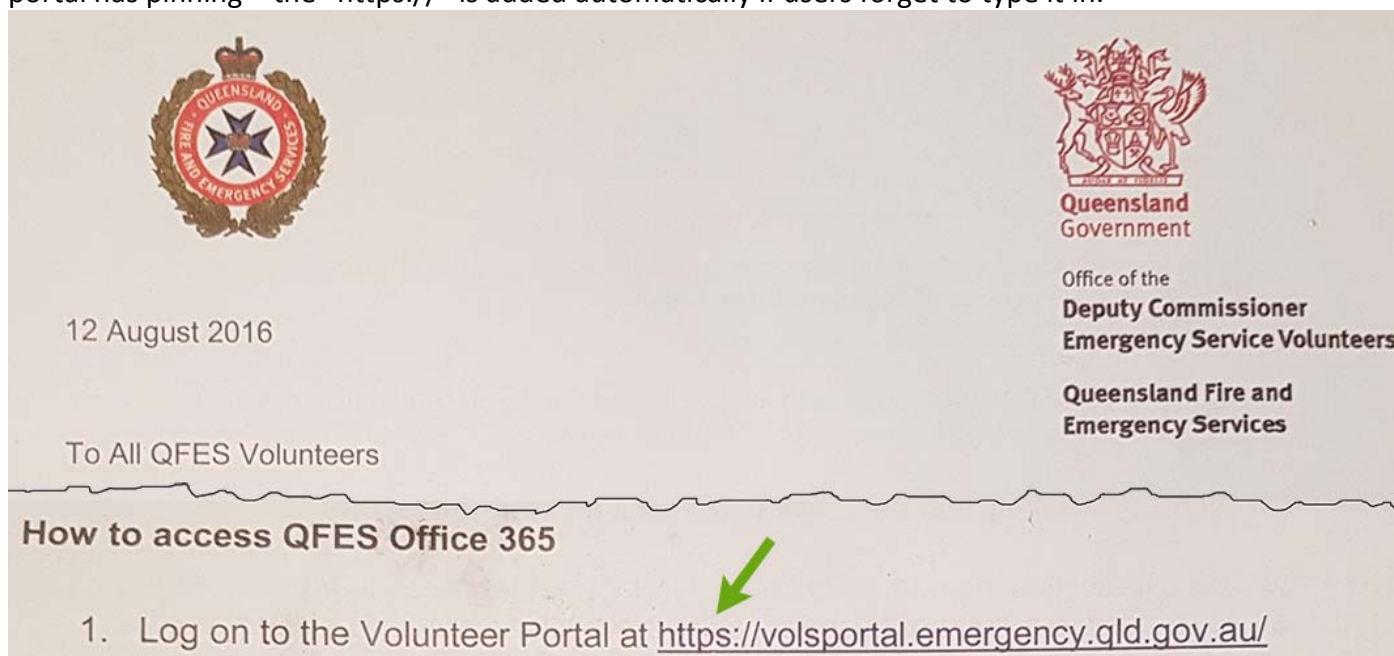
The 2016 Census web site did **not** use either of these mitigations. (Refer evidence – Appendix A)

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	100 s
 census. abs.gov.au	GET	302 Found		Other	283 B 0 B	50 ms 48 ms		
 welcome /eCensl... http://census. abs.gov.au/		200 OK	document	http://census. ab... Redirect	3.4 KB 9.2 KB	229 ms 225 ms		

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

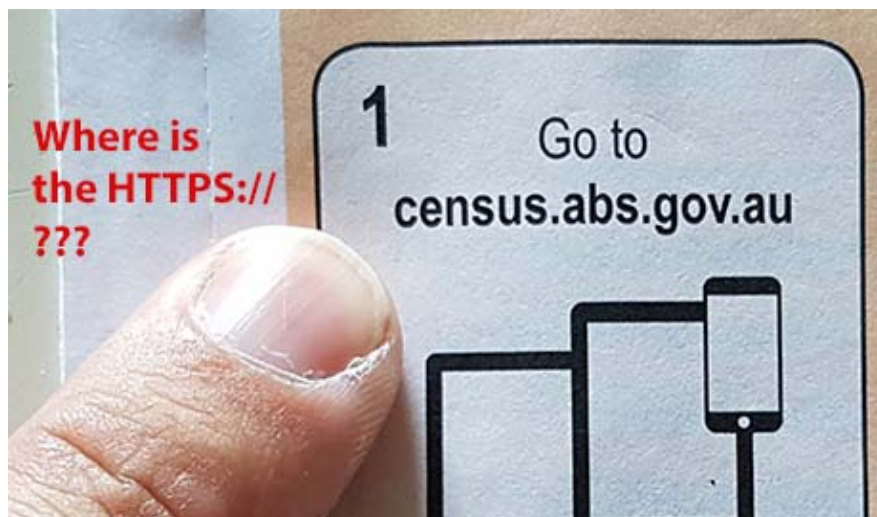
This submission covers technical security matters not present in existing submissions 1 through 90. It also covers procedural security failures again not mentioned in previous submissions. I address terms a, c, f, i and j in respect of the census web site security, and the wide ranging failure of every 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.

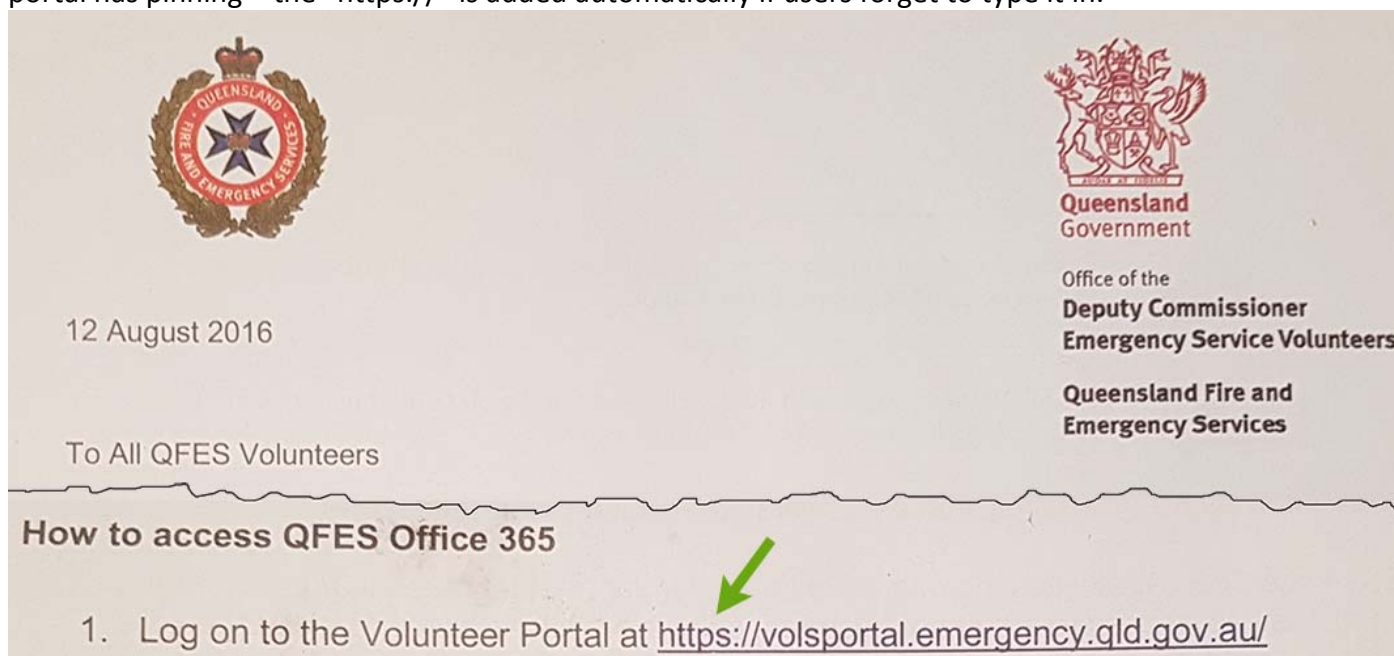
The 2016 Census web site did **not** use either of these mitigations. (Refer evidence – Appendix A)

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	100 s
 census. abs.gov.au	GET	302 Found		Other	283 B 0 B	50 ms 48 ms		
 welcome /eCens...	http://census. abs.gov.au/	200 OK	document	http://census. abs.gov... Redirect	3.4 KB 9.2 KB	229 ms 225 ms		

1st November 2017

Submission to the Senate Inquiry: **Future of Work and Workers.**

My name is Chris Drake. I am a computer security professional and expert with 35 years' experience, graduate of several international accelerator programs, grant recipient, owner/operator of multiple online businesses, employer, and participant in numerous Australian State and Federal Government Information and Communications Technology (ICT) related programs.

I respond to term "d" only:

- d. [the adequacy of Australia's laws, including industrial relations laws and regulations, policies and institutions to prepare Australians for that change;](#)

Small business employs the most Australians (source: ABS), while small and medium business combined (SME) employ almost 70% of our total workforce.

The digitisation of roles performed by Australian SMEs will create large numbers of new roles for the digitisation organisation; however, more often than not in Australia nowadays, this organisation is not Australian: those jobs lost locally are replaced by jobs in foreign countries.

Government policy has a major detrimental effect on SME growth, which is rapidly worsening in our increasingly digitised world as follows:

1. Government procurement of products and services (excluding employment of contractors, see next) from the SME market is limited.
2. Government in-house development of bespoke products and services is destroying valuable opportunities, income, and international market prospects for Australian SME's.
3. The opportunity for SME's to sell to government is extremely limited, overly complex, and "backwards" (i.e. Government should buy what it needs from Australian SME's **more often** than SME's should be expected to know who in government wants to buy from them and look/wait for related tender opportunities)

Today's digital world moves quickly. It is not uncommon for "start ups" (a small business) to become "Unicorns" (billion dollar employers of vast numbers of workers), but to do this, adoption (and usually mass adoption) of the product or service on offer is **always** required. Australian government is in the unique position to provide mass adoption, and thus catapult Australian businesses to large scale (and usually international) success. In my considerable experience in this area, Government typically always fails us.

Every ICT project built by or for Australian Government (e.g. Identity, Health, etc) represents a destroyed SME opportunity. Because Government is not a business, they do not plan to build re-useable and re-sellable products or services, and they typically have no concern for international markets, and often also no consideration for local, state or commercial markets either. Government ICT projects (which regularly fail at spectacular expense) are typically never sold to other customers, and never earn sustainable revenue, and never produce sustainable employment. Worst of all, had government sourced their project from Industry or an SME instead of building their own, this would have provided the key "mass adoption" event that often results in a globally dominating or "unicorn" business for the Australian provider, and almost certainly creating a range of new opportunities for other Australian SMEs to capitalise on this success.

The Australian Security Intelligence Organisation (ASIO) reported in October 2018 that it is unable to investigate all "harmful espionage" and "foreign interference" against Australia due to the large scale of "malicious" activity directed against Australian government and business. In short; foreign nation-state cyber-attacks against Australia are endemic and out of control. Australia needs improved on-shore ICT trade for many reasons, not least security.

My recommendations are as follows:

1. Government departments be trained to:
 - A. Understand the benefits that their procurement decisions have on the Australian workforce, and be encouraged to seek out and use local products and services.
 - B. Understand the positive national-security implications of procurements made from Australian suppliers, and the negative espionage risks from foreign suppliers, and that free-trade or other agreements do not force them to buy foreign solutions.
 - C. **Seek out** local products and services (as opposed to tenders etc). It is far easier for a government who needs something to find it, than it is for the SME who provides it somehow know that the department is looking.
2. Commonwealth ICT development rules be updated to ensure all activities comply with Commonwealth Procurement Rules (value for money, risk, etc), which themselves must take into account the value to Australian business, society, and employment, of ICT build and procurement decisions, and the risk of foreign espionage and attack.
3. Innovation in government be fostered more heavily, but be required to partner with industry suppliers since this earns those suppliers the valuable adoption they need for rapid commercial growth. The QLD Government "TWiG" (Testing Within Government) program is an example, although there also needs to be the opportunity for SME's to propose new projects to government, and not just government think up their own projects.

If Australia would like the Future of Work to include workers based in Australia, it needs to take steps NOW to ensure that those new future jobs are in Australian-based companies. The world is being digitized, and digital is global. Our future jobs will go overseas if we don't do more now to foster local suppliers of the digitized future.

Yours sincerely
Chris Drake

Attachment 4: Submission to the Senate Inquiry into the Circumstances in which Australians' personal Medicare information has been compromised and made available for sale illegally on the 'dark web'.

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.

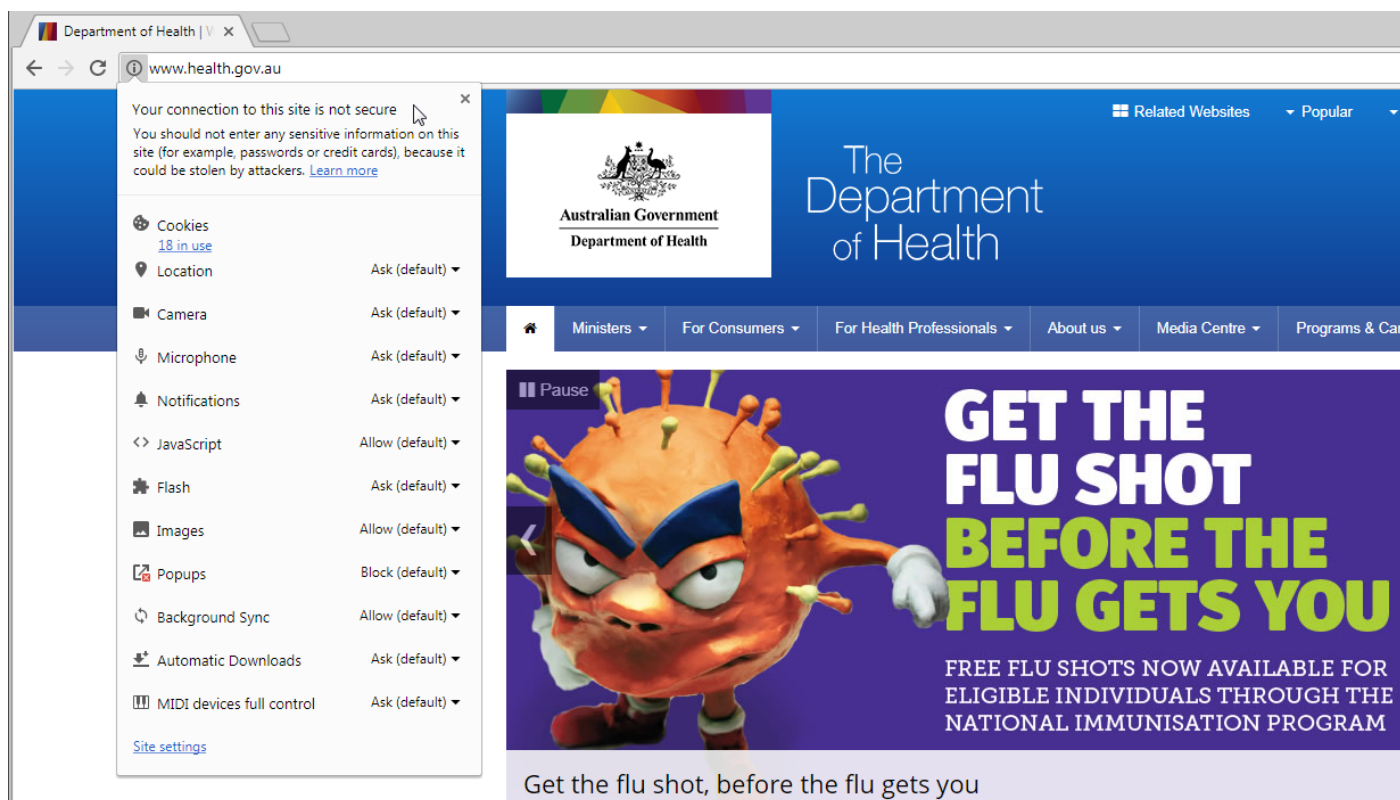
During a closed session with the ASD last year a private group of professional security engineers including myself were treated to a candid presentation on the state of cyber security within Australian Government. We were told that the ASD does not have power to compel government departments to deploy 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

Attachment 5: Submission to the Review of national arrangements for the protection and management of identity information

12th October 2018

Submission to the Review of national arrangements for the
protection and management of identity information

My name is Chris Drake. I am a computer security professional, operator of an American accredited Identity Registrar and vendor of identity-protection cyber security products and services. I'm security-cleared, I have 35 years cyber experience, and I wrote the pen-testing portion of our upcoming Trusted Digital Identity Framework (TDIF) for the DTA. I've made significant contributions to international identity standards, I serve on multiple identity and cyber security committees, I regularly attend and often speak at national and international cyber security events, and I have several decades of first-hand experience with Australian State and Federal governments across a range of cyber security topics.

I respond with particular emphasis to items 1 and 2 in the Scope – to paraphrase:-

[I will identify and analyse the key obstacles and risks associated with national arrangements for the protection and management of identity information across legislative frameworks and relating to practices and systems for the collection and use of identity information.](#)

[I will recommend reforms to enhance and strengthen the protection and management of identity information in Australia; hopefully to be included in the next iteration of the National Identity Security Strategy.](#)

Executive Overview:

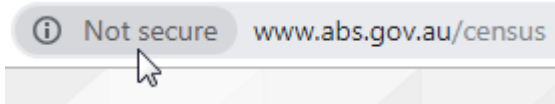
Australian government rhetoric surrounding cyber-security practices and the handling of citizen identity information bears almost no relation whatsoever to actual department practices. Rules are almost never followed, security issues are practically never addressed, failures are covered up, inquiries are misled, and there exists no working mechanisms to correct mistakes or fix security problems. Citizens are fed blatantly false assurances regarding the cyber security posture of government departments, usually from anonymous and unskilled sources, who refuse to be identified when challenged. There are no penalties for ignoring the rules, Departments routinely refuse to correct cyber issues, and cyber testing is rare and usually fails. In the comfort of anonymous or private forums, many government cyber professionals express these same opinions, along with their frustration and not being able to compel departments to change.

I write with first-hand experience regarding wide-sweeping cyber-security failures at all levels of government with regard to the handling of citizen identity and other data.

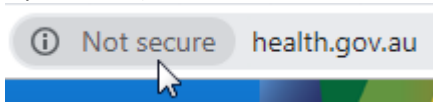
I've spent the last 12+ months battling numerous government departments (AEC, DTA, Austrac, ASD, Defence, Medicare...) using FoI requests, privacy breach notices, 3 separate senate inquiries, phone calls and letters to ministers, [ITSA](#) and other supposedly responsible security staff, media pressure, requests to join committees and reviews, and other methods in an attempt to get them to implement the most basic of security practice: TLS - aka - "switch on https:// for their web site" - which is a "mandatory" [ISM](#) control that all departments supposedly must adopt:-

*Control: 1447; Revision: 0; Updated: Apr-15; Applicability: UD, P, C, S, TS; Compliance: **must**; Authority: AA*
Agencies must use TLS.

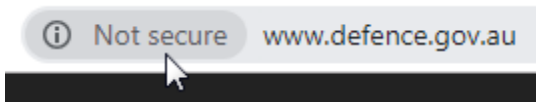
e.g. Remember [#CensusFail](#)? Was not secure then, still not today:



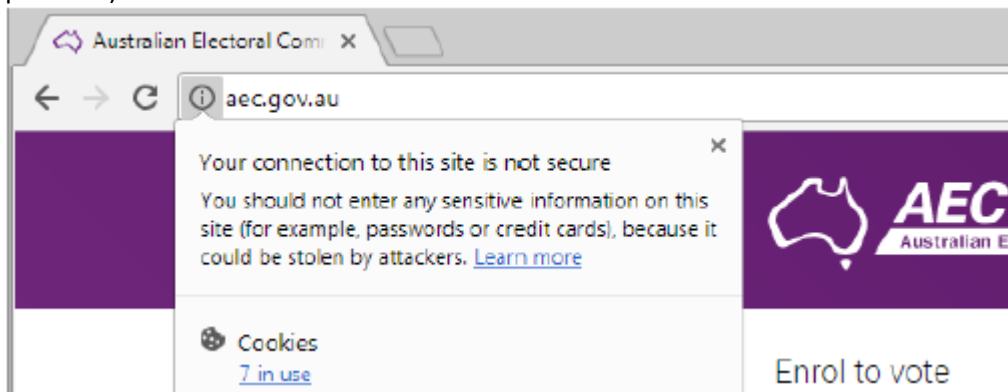
e.g. Remember [#MedicareFail](#)? Was not secure then, still not today (little wonder more than a million Aussies have Opted Out!):-



e.g. There's just no excuse for this ever:



Remember the Russians messing with elections? Voter security isn't someone the AEC has ever done yet on any election or postal vote (they did recently turn this on, although they claimed in writing it was not related to my pressure)



My summary is this: nobody whatsoever in government genuinely cares about the security of citizen identity data, or should ever be entrusted to its handling at this point in time.:-

- Every department, no exceptions, point-blank refuses to fix any of the large number of cyber security and privacy issues I've brought to their attention.
- Almost every department claims that they have no security problems (despite **evidence** to the contrary that I supply).
- All department claims of "we have no security problem" are unsigned, unattributed, and obviously not from any security professionals.
- All departments routinely block every FOI request I make (all relate to cyber-security failures).
- Departments censor (remove) all controversial public comments that are made on systems they control, especially ones relating to cyber security.
- No departments I've found appear to have any actual ITSA or similar (supposedly mandatory) roles with staff actually in them (I did notice an advert appeared seeking to fill one of those roles after I began applying pressure - so perhaps I made one tiny bit of difference to one department there).
- Departments all refuse to identify any of their IT security staff - they refuse to name names, they refuse to provide contact details. My conclusion: they do not have staff in these roles.
- The OAIC FOI review process is a sham (backlog of 1+ years, and no power to right wrongly refused FOI reports anyhow).
- There appears to be a highly organised FOI "officer" scheme or training in place to block every request that might embarrass government from being honoured (despite the law clearly banning that behaviour).
- "Consumer Protection" laws do not apply to government: when government break them, all action I've taken to right those wrongs has resulted in department lawyers telling me the sections of legislation that make them exempt.

- All senate inquiry reports that embarrass government become deemed "confidential": this is a way to hide the content AND EXISTENCE of these reports from everyone - they are removed from the record, they are never available to anyone. From observation of inquiry broadcasts over the internet, senators appear not to be provided with these reports (or at the very least -they do not read them).
- Every inquiry senator I contacted failed to confirm they ever read or received my submissions.
- I never get invited to participate in anything I apply for (to give evidence at inquiries, or to participate in reporting).
- As best I can tell - all inquiry and report-writing that takes place is not genuine. This includes the PM advisory panels I did manage to be on. They have an agenda "get some law or other passed", and industry involvement in the process is a sham - simply so government can pretend they consulted before they did what they already have planned.
- Some departments providing security advice to citizens source dubious content from the internet to base their advice on, and then refuse to be corrected when they're wrong, refuse to acknowledge evidence proving them wrong, refuse to study the efficacy or suitability of their advice, censor criticism about their flawed advice, refuse to publish corrected advice, and continue repeating their advice despite the volume of material weighing against them.
- Most departments actively mislead the public about their security and privacy practices – for example – the DTA web site in relation to the TDIF, under the heading "How we protect your privacy", linked to a privacy impact assessment (PIA) document – giving the false impression that this document proved that the DTA protected privacy, when in reality, inside the PIA details it actually reported that the DTA **failed every single privacy control that was tested**.
- Australia Post, a government-owned "body corporate" existing through specific government acts, is considered a "commercial entity", and thus it is allowed to escape Fol scrutiny.
- The Australian Signals Directorate (ASD) – our peak body informing all other departments on the topic of cyber security, is immune to Fol scrutiny too.
- Public servants are highly misleading when appearing in senate inquiries: they fail to report their own mistakes, and they readily point to industry failures as a means to divert attention from their own mistakes, and some departments cover up the failures of other departments when questioned by senators (e.g. The ASD head, when asked in the government-service-failure inquiry if a department was compliant with ASD advice, chose a lengthy reply summarising ASD advice as his tactic to avoid answering the question, which worked).
- The way the privacy law is written gives all departments a "get out of jail free" excuse not to fix security problems: the ASD (who provide security advice, including the operation/oversight of so-called "approved" secure cloud etc) is not the same department as the ones *with* the privacy data, so no single department has security responsibility over this data, so no department is ever in breach when it's insecure. Here's how ASD lawyers responded to me when I submitted a privacy complaint regarding their approved systems being implemented with no security whatsoever to collect voter enrolment details:-

" As the ASD does not have possession or control of a record containing your personal information collected by the AEC, my initial view is that the ASD is not required to take reasonable steps to protect the security of such information. "

That bears repeating in bold. It is the *written* advice FROM the ASD - Australia's body responsible for cyber security in government, that: " **THE ASD IS NOT REQUIRED TO TAKE REASONABLE STEPS TO PROTECT THE SECURITY OF [VOTER] INFORMATION** "

Or to summarise the many hundreds of hours I've wasted discovering all that mess above:

- A. Australian Government systems are utterly insecure (this is a well-reported fact - 62% of Australian cyber break-ins are to Government servers. That's 4 new ones every day. Sources: Australian Signals Directorate: <https://acsc.gov.au/publications/protect/cyber-security-picture-2013.htm> and DPM&C page 16: <https://cybersecuritystrategy.homeaffairs.gov.au/sites/all/themes/cybersecurity/img/PMC-Cyber-Strategy.pdf>)
- B. There is no working mechanism to fix it.
- C. There is no motivation to fix either of the above.
- D. Senate inquiries pertaining to government failures are 100% whitewash - public servants totally control these, and they do not rat on their own.

- E. Reviews and inquiries never seem genuine, and always exclude me and the submissions I make - uncovering public service failure appears never to be acceptable in final reports.
- F. Nobody in the public service seems accountable - there are no penalties for doing the wrong thing.
- G. The system in place to cover all that up is well oiled.

I have hundreds of documents verifying all my above claims which contain even greater numbers of embarrassing problems that the few above that I've recalled.

In my opinion, I doubt that this "Review of national arrangements for the protection and management of identity information" has any genuine reason for taking place, other than to support an already planned government agenda. I was told by the DTA that they are not legally allowed to use Citizen data for a purpose other than what it was collected for - so if I had to guess, this review is also a fake, and exists simply to facilitate a move by departments to lift that restriction (regardless of what might be delivered in any final review).

In summary:-

1. Australian legislative frameworks are powerless to protect Australian identity information. The rules are simply ignored, there is no mechanism in place to fix cyber issues, and there are no penalties for failure. Consume Protection simply does not apply to government, and public claims about government being "secure" are almost always false and misleading.
2. Practices and systems for the collection, use, sharing of identity information are almost universally insecure. See page 2 of this report – after more than year of my intense campaigning and more than 100 individual contacts across a range of departments, multiple critical government systems that collect citizen identity information still remain insecure as I write - and even clearly and conspicuously advertise this blatant lack of security by warning "Not Secure" to every web visitor to loads their site!



Worse – there is no working mechanism to correct this glaring oversight.

Worse still – this is a direct violation of ISM controls

Worst of all – departments confronted by this obvious problem and ISM violation respond by denying that it's not secure.

Recommendation:

1. That HSTS, HPKP, and Expect-CT all be enabled for the entire gov.au TLD and all subdomains. There is NO EXCUSE for not using TLS in 2018 and beyond – these security technologies will force all departments to be secure, whether they like it or not (and, the bulk of government departments do not like it – but they should never be entitled to their misguided opinions when citizen identity is at risk).
2. That private industry, not government, be tasked with the broadest possible set of roles and functions for identity. Government is un-trustable, unaccountable, beyond reach of laws and penalties, and has repeatedly proven incapable of implementing even the most basic of security protections for identity information. Government are far more capable of compelling private industry to comply with laws and have penalties protecting in place to enforce them, and private industry are far more capable of being cyber-responsible than government, as well as more likely to be trusted.
3. That an overhaul of the FoI act and practices be performed – there are too many exemptions allowing departments to cover up embarrassment, and there is no working review process.
4. That all department ISTA roles be made known to the public, that all ISTA roles be staffed, that all ISTA staff be properly qualified, that no unqualified persons be permitted to provide cyber advice, that all cyber advice provided be attributed, that ITSA staff be required to accept cyber-security and privacy reports and complaints directly from the public, and compelled to act on them within a reasonable and short timeframe, that all cyber reports be reported and made public, that no cyber reports be disregarded/hidden/ignored or otherwise not acted upon or reported.

5. That the practice of branding inquiry submissions “Confidential” be banned – if confidential material needs to be suppressed, there should be a formal review process and censorship using “blacking out”, instead of a total cover-up of submissions.
6. That every department touching identity information be required to undergo annual compliance auditing against all mandatory ISM controls, be fully compliant with all strategies to mitigate cyber security incidents (not just the top-4, or essential-8, but all of them. <https://acsc.gov.au/infosec/mitigationstrategies.htm>), that these audits be published, and that penalties be imposed for failure to comply.
7. No identity information should ever be shared with any department that does not have a current and fully-passed audit. Any ISTA reports providing evidence that any department is in breach of their security requirements should result in the immediate revocation of their compliance, and the immediate cessation of identity sharing.
8. That a non-government process with strong powers and penalty tools be undertaken to repair the near-total lack of cyber security response capability within government – my work is just the tip of the iceberg; a more thorough process needs to be undertaken to find all the other problems which are being covered up, and to repair them all.

Find below, included in full, the following supplementary documents:

1. My submission to the 2017 Senate Inquiry: Digital delivery of government services. – deemed confidential by the public servants running the inquiry, and suppressed from all records.
2. My Submission to the Senate Inquiry into the 2016 Census. – also deemed confidential by the public servants running the inquiry, and suppressed from all records.
3. My Submission to the 2017 Medicare Senate Inquiry: again deemed confidential by the public servants running the inquiry, and suppressed from all records.
4. My Submission to the Senate Inquiry: Future of Work and Workers. (to strengthen my point that Identity services should be run by Industry, not Government).

I specifically deny permission for this submission and any of my inclusions to be deemed “confidential” or to be suppressed from submission or other records. If information contained within is considered confidential in nature, you may “black out” only those sections which are necessary to support your confidentiality requirements.

Yours sincerely
Chris Drake

20th September 2017

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

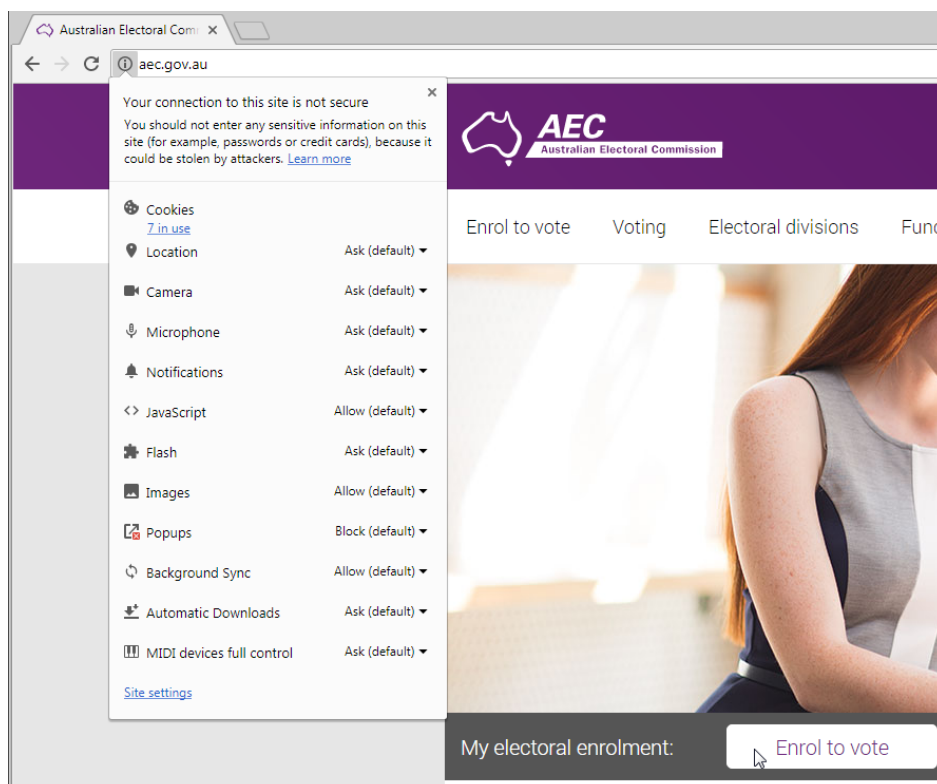
My name is Chris Drake. I am a computer security professional and expert with 35 years cyber experience, I have won numerous international cyber security and innovation awards, spoken at many international conferences on the subject of cyber security, I run multiple security-related businesses, and I 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.

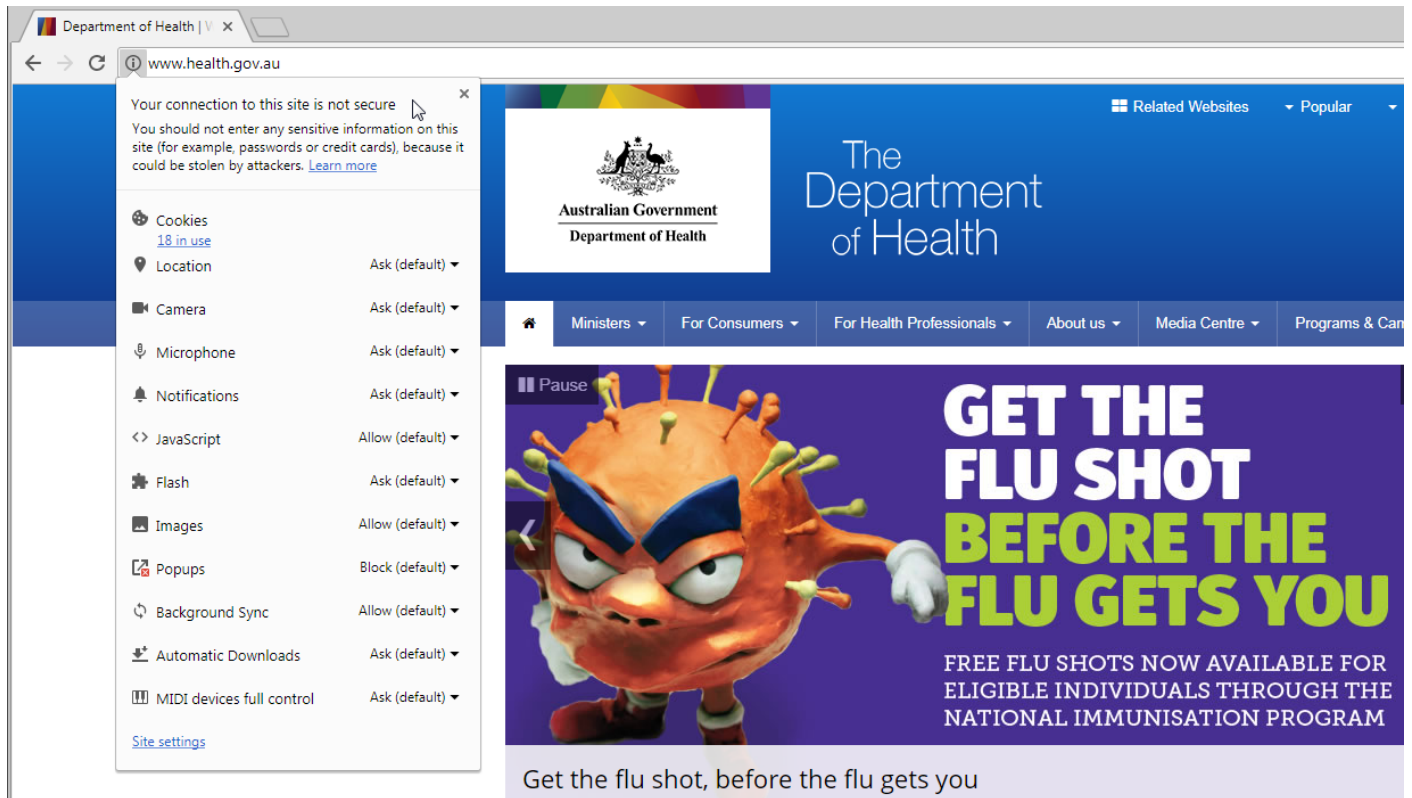
As I said in the previous section, failure to engage appropriately skilled programmers and reviewers, and failure to engage a reputable penetration systems testing team reveal systematic security failures within DHS/HPOS.

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-gugpjw>

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 with 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

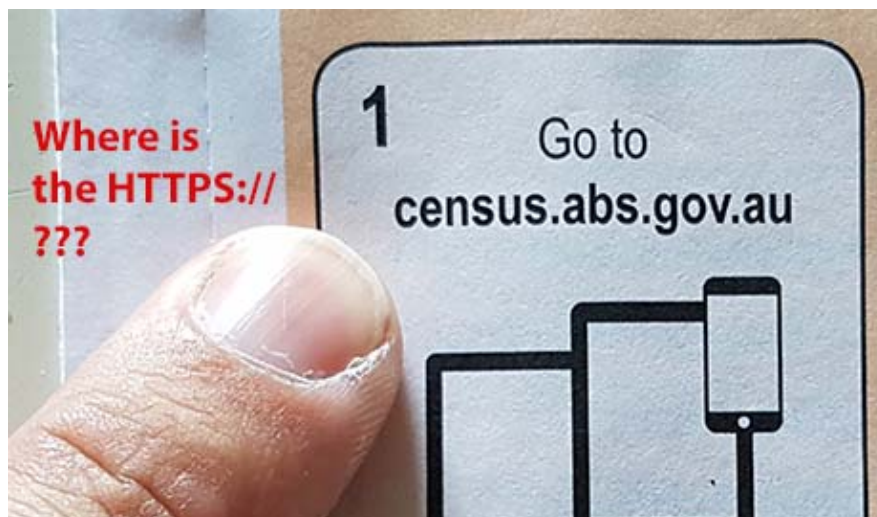
This submission covers technical security matters not present in existing submissions 1 through 90. It also covers procedural security failures again not mentioned in previous submissions. I address terms a, c, f, i and j in respect of the census web site security, and the wide ranging failure of every 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.

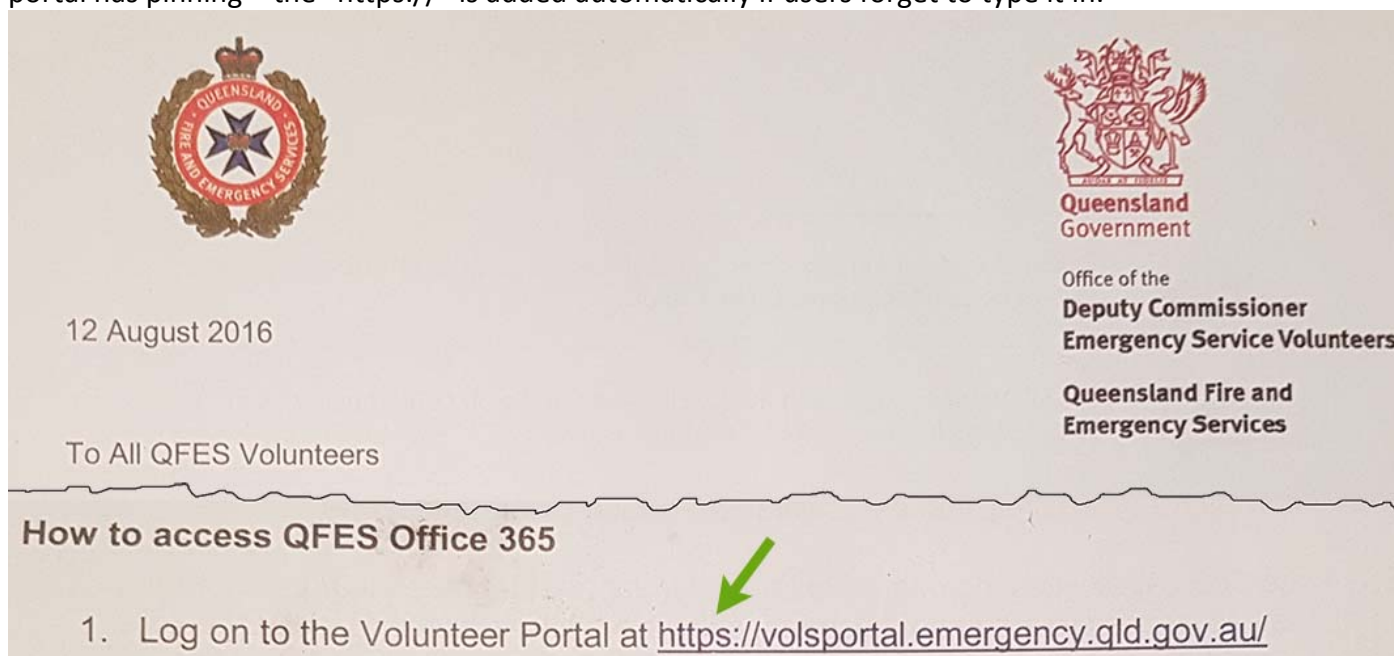
The 2016 Census web site did **not** use either of these mitigations. (Refer evidence – Appendix A)

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	100 s
 census. abs.gov.au	GET	302 Found		Other	283 B 0 B	50 ms 48 ms		
 welcome /eCens...	http://census. abs.gov.au/	200 OK	document	http://census. abs.gov. ... Redirect	3.4 KB 9.2 KB	229 ms 225 ms		

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.

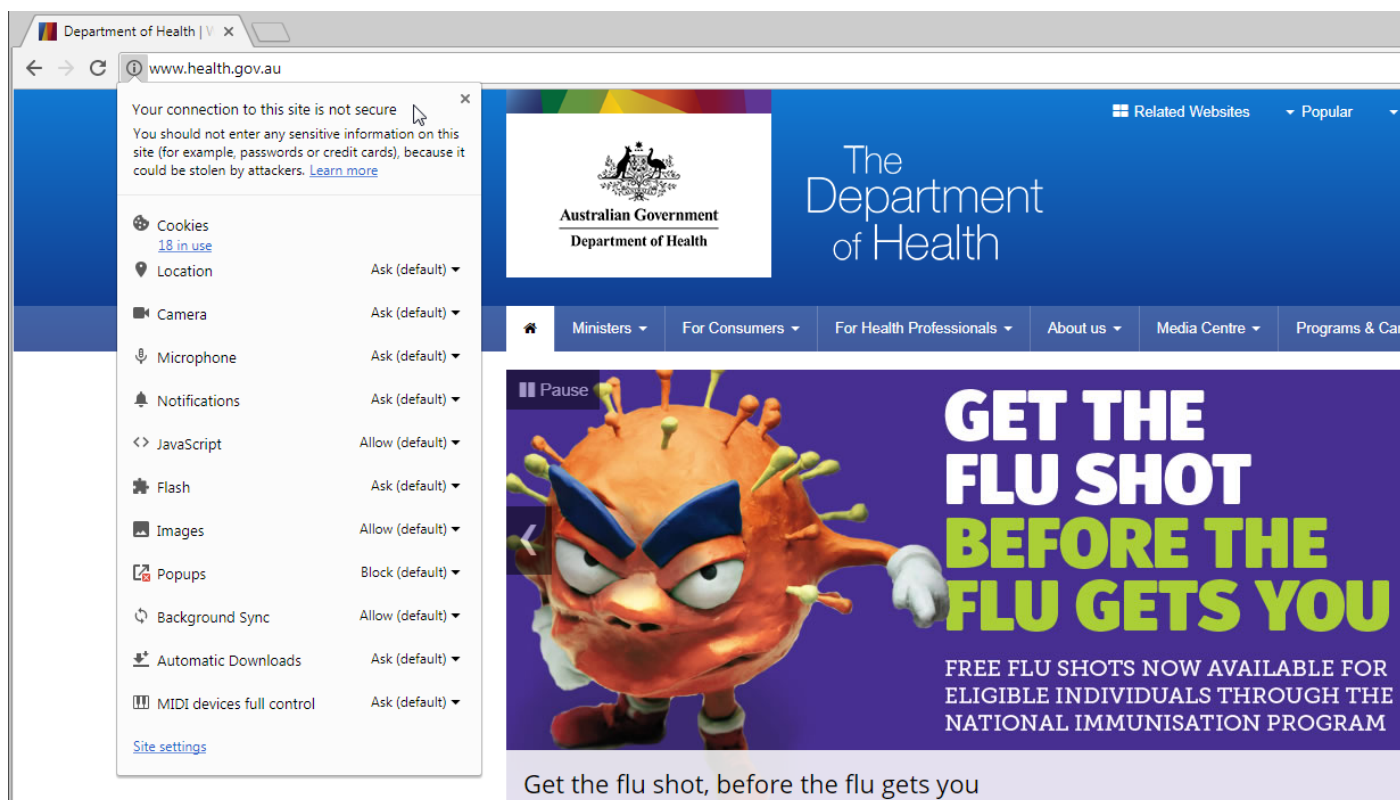
During a closed session with the ASD last year a private group of professional security engineers including myself were treated to a candid presentation on the state of cyber security within Australian Government. We were told that the ASD does not have power to compel government departments to deploy 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

1st November 2017

Submission to the Senate Inquiry: **Future of Work and Workers.**

My name is Chris Drake. I am a computer security professional and expert with 35 years' experience, graduate of several international accelerator programs, grant recipient, owner/operator of multiple online businesses, employer, and participant in numerous Australian State and Federal Government Information and Communications Technology (ICT) related programs.

I respond to term "d" only:

- d. [the adequacy of Australia's laws, including industrial relations laws and regulations, policies and institutions to prepare Australians for that change;](#)

Small business employs the most Australians (source: ABS), while small and medium business combined (SME) employ almost 70% of our total workforce.

The digitisation of roles performed by Australian SMEs will create large numbers of new roles for the digitisation organisation; however, more often than not in Australia nowadays, this organisation is not Australian: those jobs lost locally are replaced by jobs in foreign countries.

Government policy has a major detrimental effect on SME growth, which is rapidly worsening in our increasingly digitised world as follows:

1. Government procurement of products and services (excluding employment of contractors, see next) from the SME market is limited.
2. Government in-house development of bespoke products and services is destroying valuable opportunities, income, and international market prospects for Australian SME's.
3. The opportunity for SME's to sell to government is extremely limited, overly complex, and "backwards" (i.e. Government should buy what it needs from Australian SME's **more often** than SME's should be expected to know who in government wants to buy from them and look/wait for related tender opportunities)

Today's digital world moves quickly. It is not uncommon for "start ups" (a small business) to become "Unicorns" (billion dollar employers of vast numbers of workers), but to do this, adoption (and usually mass adoption) of the product or service on offer is **always** required. Australian government is in the unique position to provide mass adoption, and thus catapult Australian businesses to large scale (and usually international) success. In my considerable experience in this area, Government typically always fails us.

Every ICT project built by or for Australian Government (e.g. Identity, Health, etc) represents a destroyed SME opportunity. Because Government is not a business, they do not plan to build re-useable and re-sellable products or services, and they typically have no concern for international markets, and often also no consideration for local, state or commercial markets either. Government ICT projects (which regularly fail at spectacular expense) are typically never sold to other customers, and never earn sustainable revenue, and never produce sustainable employment. Worst of all, had government sourced their project from Industry or an SME instead of building their own, this would have provided the key "mass adoption" event that often results in a globally dominating or "unicorn" business for the Australian provider, and almost certainly creating a range of new opportunities for other Australian SMEs to capitalise on this success.

The Australian Security Intelligence Organisation (ASIO) reported in October 2018 that it is unable to investigate all "harmful espionage" and "foreign interference" against Australia due to the large scale of "malicious" activity directed against Australian government and business. In short; foreign nation-state cyber-attacks against Australia are endemic and out of control. Australia needs improved on-shore ICT trade for many reasons, not least security.

My recommendations are as follows:

1. Government departments be trained to:
 - A. Understand the benefits that their procurement decisions have on the Australian workforce, and be encouraged to seek out and use local products and services.
 - B. Understand the positive national-security implications of procurements made from Australian suppliers, and the negative espionage risks from foreign suppliers, and that free-trade or other agreements do not force them to buy foreign solutions.
 - C. **Seek out** local products and services (as opposed to tenders etc). It is far easier for a government who needs something to find it, than it is for the SME who provides it somehow know that the department is looking.
2. Commonwealth ICT development rules be updated to ensure all activities comply with Commonwealth Procurement Rules (value for money, risk, etc), which themselves must take into account the value to Australian business, society, and employment, of ICT build and procurement decisions, and the risk of foreign espionage and attack.
3. Innovation in government be fostered more heavily, but be required to partner with industry suppliers since this earns those suppliers the valuable adoption they need for rapid commercial growth. The QLD Government "TWiG" (Testing Within Government) program is an example, although there also needs to be the opportunity for SME's to propose new projects to government, and not just government think up their own projects.

If Australia would like the Future of Work to include workers based in Australia, it needs to take steps NOW to ensure that those new future jobs are in Australian-based companies. The world is being digitized, and digital is global. Our future jobs will go overseas if we don't do more now to foster local suppliers of the digitized future.

Yours sincerely
Chris Drake

Attachment 6: Full text of “Deemed Confidential” advice letters informing that embarrassing Submissions will be hidden from existence.



**THE SENATE
STANDING COMMITTEE ON FINANCE AND PUBLIC ADMINISTRATION**

Tuesday, 24 October 2017

Mr Chris Drake
PO Box 988
Noosa Heads. QLD 4567

Email: tech@cryptophoto.com

Dear Mr Drake,

Inquiry into Digital delivery of government services

I am writing to acknowledge the receipt of your submission to the above inquiry, and to advise that it has been accepted by the Committee as a confidential submission. **We will not be providing your submission to anyone on request and it will be not be listed on the committee's webpage.**

Your submission is protected by parliamentary privilege. Parliamentary privilege refers to the special rights and immunities attached to the Parliament or its members and others necessary for the discharge of the parliamentary functions without obstruction and fear of prosecution. This means that you cannot be prosecuted or disadvantaged because of anything you have provided in evidence, or because you gave such evidence. If you believe that anyone has disadvantaged you in any way as a result of the submission you have made, please advise the Secretariat.

Please note, you should not release this submission without the approval of the committee. The unauthorised disclosure of a submission is not protected by Parliamentary Privilege.

Thank you for your participation in this inquiry. Should you require any further information concerning the committee's inquiry, please contact the committee secretariat on 02 6277 3439.

The Committee is required to report by **4 December 2017**. A copy of the report will be loaded onto the Committee's website and may be accessed at http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Finance_and_Public_Administration.

Yours sincerely

Ann Palmer
Secretary

PO Box 6100, Parliament House Canberra ACT 2600 Tel: (02) 6277 3439 Fax: (02) 6277 5809
Email: fpa.sen@aph.gov.au Internet: www.aph.gov.au/senate_fpa

About Chris Drake

Foreword: Australians suffer a cultural affliction known as “tall poppy syndrome”. It is in our nature to despise, criticize, cut-down, and distrust high-achievers and public figures. Please be aware that you’re in Australia, and probably you are Australian, and are yourself almost certainly so afflicted. If, while reading this, you find yourself critical of my motives, hating my words, or thinking anything about “Chris Drake” – please STOP – take a breath, and try to return to the topic. This is about Cyber-Security – not about “Chris Drake”. If you’re thinking I’m arrogant already – perhaps take a break right now! Disrupting “tall poppy” is an important step to securing Australia!

- I'm a veteran cyber expert with 37+ year's continuous experience. I'm trying to fix Australian cyber-insecurity.
- I'm a graduate from the **excellent** Israeli Landing-Pad Program by Austrade.
- I'm a Microsoft-Ventures cyber graduate (India) and an Advance.org cyber graduate (San Francisco)
- My cyber-security company has raised more than \$1M through several federal Government grants.
- I was on the PM's cyber panel. I've been part of two cyber advisory committees (e.g. network threat blocking).
- I've participated in 3 senate inquiries relating to cyber.
- I've been involved in numerous QLD state-Government innovation initiatives, attended many QLD events,
- I've made use on more than 100 occasions of cyber vulnerability reporting mechanisms throughout Australia.
- I've personally met ASD staff several times, and spoken at and attended private lectures they've given.
- I've made extensive use of FoI-Act requests relating to cyber security issues, and filed one Privacy-Breach notice.
- I've reported more than 3 critical government vulnerabilities in the last 3 years.
- I've worked with the AFP and FBI for many years, and testified in Cleveland putting BayRob in jail for 37 years.
- I wrote the penetration-testing guide of our Trusted-Digital-Identity-Framework, TDIF (under contract to DTA).
- I'm a vocal AIIA member in cyber advocacy groups, and regular attendee at cyber forums and events.
- My company and I have won more than a dozen prestigious international awards relating to cyber security.
- I own many patents, including the worlds #1-cited security patent of all time (authentication & anti-malware)
- I've worked in Anti-Virus research at IBM. I'm in the partner programs of Microsoft, Checkpoint, IBM, and others.
- I've personally hand-coded 3 cipher algorithms under contract to the Australian Air Force.
- I've taken one of my products through the ASD (formerly DSD at the time) cyber evaluation process.
- I am a USA-accredited digital identity registrar and run a secure online identity service
- I'm an AUSTRAC-registered digital currency exchange, participated in their training, and got audited
- I helped write the OpenID, OWASP, and FIDO standards, and some of the NIST sp800 series.
- I've submitted several cyber-bugs to international bounty programs and reporting systems.
- I've had meetings of 1+ hours each with more than 500 cyber experts in 200+ different global organisations.
- I'm a member of a dozen cyber working groups. I've won several state and national GovHack awards.
- I've spoken at about 50 local and international cyber events, and attended many more.
- I've sued and successfully defended cyber patent and trademark lawsuits in the USA
- I own and operate an Australian cyber business in the field of secure authentication.
- Cyber-security in Australia is a shambles, and I genuinely want to try and help fix it.

Most of my submission is not my opinion – it is fact which I can support with extensive evidence.

There is no substitute for experience. Anyone who hasn't lodged a vulnerability report, participated in an inquiry, filed an FoI, used a cyber service, joined a cyber group, lodged a cyber tender, built a standard, been at a working group, sold a cyber product, run a cyber business, tested an assumption, etc – is not truly qualified to comment on the related topic. I've done all those things, usually many times, recently.