

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

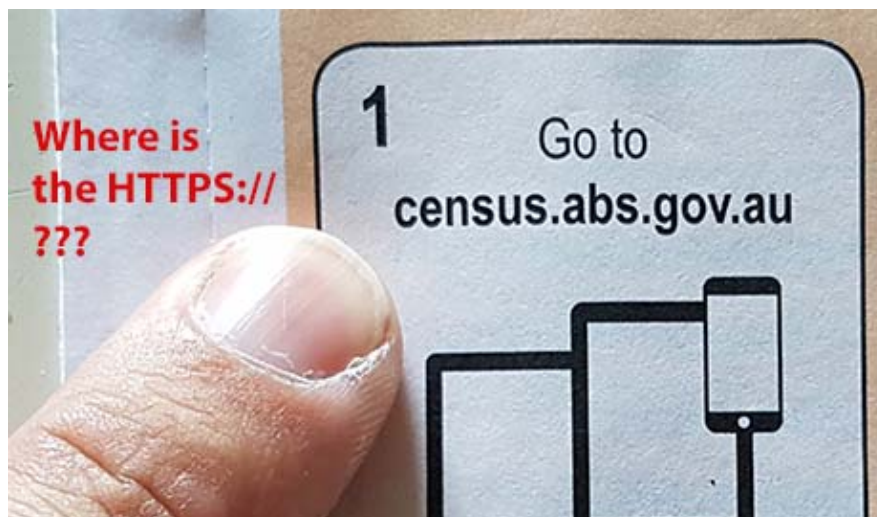
This submission covers technical security matters not present in existing submissions 1 through 90. It also covers procedural security failures again not mentioned in previous submissions. I address terms a, c, f, i and j in respect of the census web site security, and the wide ranging failure of every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

<sup>1</sup> 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:<sup>2</sup> 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).<sup>2</sup> HTTP Strict-Transport-Security response header (HSTS) and Certificate Pinning are two such examples.

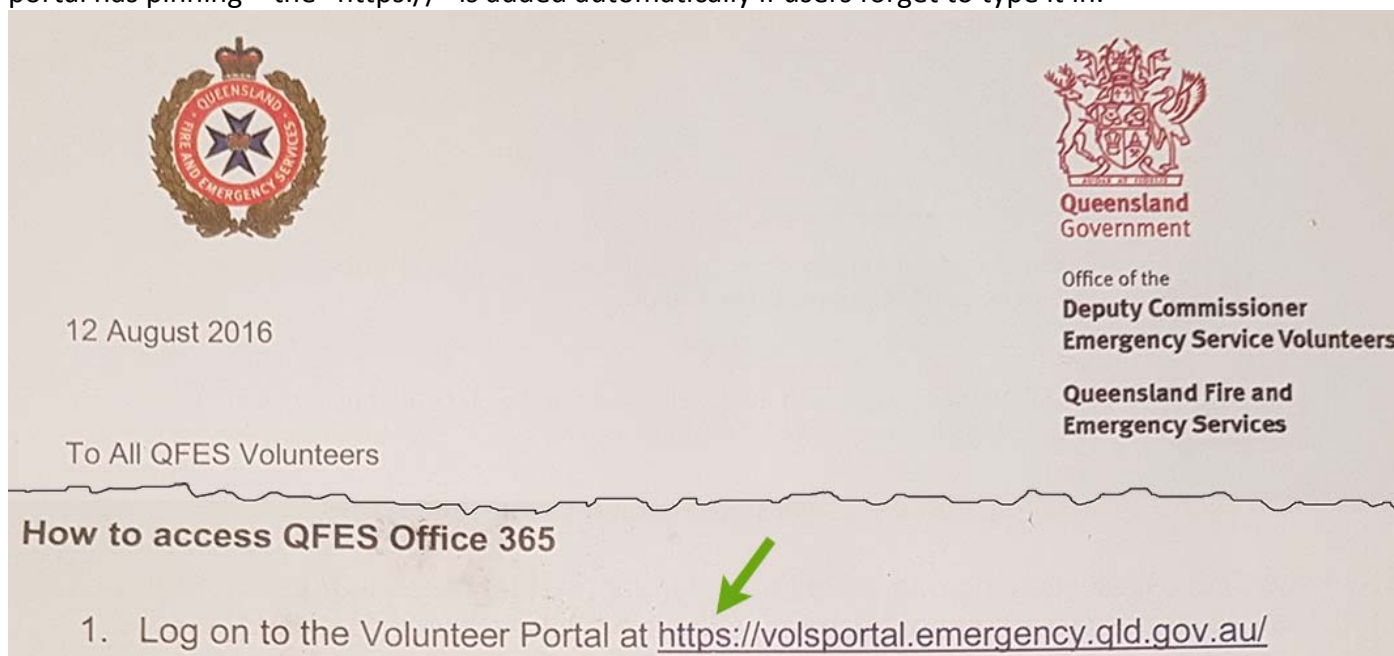
The 2016 Census web site did **not** use either of these mitigations. (Refer evidence – Appendix A)

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.

<sup>2</sup> 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](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 (12<sup>th</sup> 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”<sup>3</sup> 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](mailto: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.

---

<sup>3</sup> 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 11<sup>th</sup> 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.<sup>4</sup> That's 4 new ones *every day*.<sup>5</sup> Compared to the UK<sup>6</sup> 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.<sup>7</sup> 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.

---

<sup>4</sup> Australian Signals Directorate: [www.asd.gov.au/publications/protect/cyber-security-picture-2013.htm](http://www.asd.gov.au/publications/protect/cyber-security-picture-2013.htm)

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

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

<sup>7</sup> 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	