Chris Drake
PO Box 988, Noosa, Q, 4567
Telephone: 0487 543210
Email: tech@cryptophoto.com

Response to "Exposure Draft Security Legislation Amendment (Critical Infrastructure) Bill 2020".
By Chris Drake.

11th November, 2020

This act contains penalties – that is an excellent inclusion.

This act contains an amendment which excludes all government. This is obviously a decision by a public servant to prevent them becoming subject to penalties, which I submit is an act of corruption.

It is beyond question that Government itself is critical infrastructure. It is also beyond question that Government intrusions risk and facilitate further intrusions into other critical infrastructure systems.

According to Australian Signals Directorate (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, and are not available under FoI laws, inquiry and other submissions into government cyber problems are almost always "Deemed Confidential" (which also includes the erasure of the fact that the submissions was made from submission records – another obviously corrupt practice), and public servants regularly mislead inquiries, publish false public compliance statements, and simply cannot be trusted to follow adequate cyber practice.

Also according to the ASD, Australian Government departments rarely adhere to guidelines or follow best practices.

- 62% of Australian cyber break-ins are to Government servers.[1] That's 4 new ones every day.[2]
- In my experience (and also found in a UK report), the number of actual intrusions versus acknowledged ones is typically double.
- The average time Australian Government takes to detect a break-in exceeds 6 months[3].

There is no functional mechanism in Australia to report Government cyber vulnerabilities, no working systems to correct cyber problems, no penalties for non-compliance with cyber rules or recommendations, and no repercussions of any kind to public servants who do not care or "no nothing" about cyber and its problems.

The amendment that deems government to not be "critical infrastructure" needs to be removed, and replaced with a new amendment that literally states the opposite. All of government needs to be explicitly classed as critical infrastructure, so that non-compliance penalties can finally apply for the first time, so that everyone finally has the "stick" that is needed to force our public servants to start taking cyber seriously.

---

[1] Australian Signals Directorate: www.asd.gov.au/publications/protect/cyber-security-picture-2013.htm
[2] DPM&C page 16: https://cybersecuritystrategy.dpmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf (+37%) plus ref #2 above
[3] From ASD presentation, and also http://www.zdnet.com/article/businesses-take-over-six-months-to-detect-data-breaches/

i.e. Remove this:

> *(2A) If an asset is owned by: 32 (a) the Commonwealth; or (b) a body corporate established by a law of the Commonwealth 2 (other than a government business enterprise); 3 the asset is not a critical infrastructure asset unless: 4 (c) the asset is declared under section 51 to be a critical 5 infrastructure asset; or 6 (d) the asset is prescribed by the rules for the purposes of 7 paragraph (1)(f). 8 (2B) An asset is not a critical infrastructure asset to the extent to which 9 the asset is located outside Australia.*

Thanks for inviting my feedback. I am a cyber professional with more than 33 years' experience in this field, and more than 10 years deep experience working on attempting to repair government cyber issues. Refer to any of my 5+ senate inquiry submissions or other published works for the 100+ pages of evidence I've submitted that substantiate all claims I've made herein. Note especially: these have all been "Deemed Confidential" and may not be available to you – if you need a full and uncensored copy of my submissions, please get in touch.

Regards,
Chris Drake.