www.sifa.net.au

SIFA Shooting Industry Foundation Australia

Australia's Firearms Experts

Submission

Discussion Paper, Strengthening Australia's cyber security regulations and incentives

September 2021

Discussion Paper, Strengthening Australia’s cyber security regulations and incentives

The Shooting Industry Foundation of Australia (SIFA) thanks the Department of Home Affairs (DHA) for the opportunity to provide a view on strengthening Australia’s cyber security regulations and incentives.

SIFA is the peak body representing the major importers and wholesalers of firearms and firearm related components in Australia. SIFA’s role is to optimise the regulatory and commercial circumstances in which the Australian shooting industry operates.

The annual value of small arms and ammunition imports to Australia to March 2021 was A$772.3 million and exports over the same period was A$166.6 million. The civilian sectors alone (hunting and target shooting) contributed $A2.4B to the Australian economy in 2019, supported an estimated 400 small businesses and more than 19,000 jobs.

In developing this submission, SIFA has considered the details of the call for views, the Australian Government Information Security Manual (ISM) and various responses to Senate Estimates hearings.

Whilst the cyber security issues flagged in the call for views are undoubtedly an important issue for private sector entities, SIFA is of the view that a more significant risk resides in the Governments application and adherence to its own existing cyber security guidance.

In making this argument, SIFA will refer to examples within the DHA portfolio itself which is relevant to our particular industry scenario.

The management of firearms in Australia is a complex multi-jurisdictional arrangement based loosely around the National Firearms Agreement (NFA). This involves the collection, storage and use of sensitive information relating to the identity of licensed firearms owners, details of registered firearms and their storage locations.

The Senate Legal and Constitutional Affairs report, *Ability of Australian law enforcement authorities to eliminate gun-related violence in the community (April 2015)* stated there were 30 different registers and databases across federal, state and territory agencies used to regulate firearms in Australia.

The Australian Criminal Intelligence Agency (ACIC) provides what has been described as “an information brokering service” known as the Australian Firearms Information Network (AFIN). AFIN collects, aggregates, and republishes firearms related data which is sourced from the partner agencies who maintain those 30 different registers and databases.

The obligations of system owners and the cyber security risk mitigations for cross domain solutions such as AFIN are set out in detail in a range of artifacts available from the Australian Cyber Security Center, such as the ISM. In approving access to AFIN by partner agencies, the ACIC system owner must be satisfied that the entity being granted access is capable of safeguarding that protected data.

There are at least three published audits into firearm registries (WA, Qld and NSW) which cast significant doubt on those partner agency's ability to maintain the levels of trust required to access protected AFIN data. In early 2021 the ACIC advised Senate Estimates that "the ACIC has no jurisdiction or management authority for partner agencies local IT systems". Whilst this statement is technically correct, ACIC do have an ongoing obligation to assess the risks to the aggregated data set which they have produced and are primarily responsible for, including suspending access arrangements until all doubt is removed. When questioned about the risks identified in those audit results in Senate Estimates, the ACIC claimed to be unaware of them. How effective are the cybersecurity risk assessments if a damning and very public audit report does not even produce a blip on the security radar?

When questioned in Senate Estimates about the volumes of cross jurisdictional enquiries conducted via AFIN, the ACIC responded that "It would be an unreasonable diversion of resources to breakdown how many times per year each separate jurisdiction queries firearms information in the other jurisdictions". The ISM requires cross domain solutions such as AFIN to "have comprehensive logging capabilities to establish accountabilities for all actions performed by users. Effective logging practices can increase the likelihood that unauthorised behavior will be detected". If effective logging is in place as required by the ISM, then traffic patterns and volumes to and from each domain should already be known.

The aggregated data set within AFIN is classed at a "protected" level. In layman's terms, this is the level applied when the risk is considered sufficient to embarrass Government. Given that the targeted theft of legal firearms from licensed firearm owners by organised crime gangs is cited by agencies such as the ACIC as a significant source of illicit firearms, it could be argued that cybersecurity lapses by any of the partner agencies which make up the AFIN network could enable criminals to target licensed firearm owners in their homes anywhere in Australia, and that this lapse could in fact represent a threat to the life of the licensed firearm owner and their families. Threat to life risks demand a classification above Protected.

All entities whether public or private are resourced constrained and this paper has shown how difficult it is it adhere fully to any codified standards when real world practicalities intervene. When well-resourced portfolios such as the Department of Home Affairs appear unable to fully satisfy the Commonwealths own cyber security expectations, it would seem to be an impossible imposition upon commercial entities given the current economic circumstances.

Individuals, whether we call them consumers or citizens, should enjoy a common standard of privacy safeguards when entities collect and hold their personal information. Government and the private sector should both be held accountable to the same standards and remedies.

[redacted]

David Voss

Policy & Research

[redacted]