Patrick Fair ASSOCIATES

**UPDATE**

# Mandatory Ransomware Reporting and Rethink on Security of Critical Infrastructure Reform

## 1. Government announces Ransomware Strategy including mandatory ransomware reporting

On 13 October 2021 the Minister for Home Affairs, the Hon Karen Andrews MP, announced the Federal Government's Ransomware Action Plan. The key elements of the action plan are:

1) Additional operation activity, listed as:
   a) establishment of multi-agency Operation Orcus led by the Federal Police targeting cyber criminals in response to "the surging ransomware threat".
   b) Awareness raising and "clear advice" for critical infrastructure and business of all sizes.
   c) Joint operations with international counterparts to detect, investigate, disrupt and prosecute individuals involved in exploiting ransomware.
   d) Active calling out of those who provide safe havens to cyber criminals.
2) Legislative reforms:
   a) Mandatory ransomware cyber incident reporting to the Federal Government.
   b) Creating a new offence of cyber extortion.
   c) An aggregated offence for cybercriminals that target critical infrastructure.
   d) "Modernising legislation" to ensure the ability to track down, seize or freeze the proceeds of cybercrime.

The Minister's press release adds that:

- The government plans to criminalise the act of dealing with stolen data knowingly obtained in the course of a criminal offense and buying and selling of malware for the purpose of undertaking cybercrime.
- Details of the mandatory reporting regime are yet to be developed but businesses with a turnover of less than $10m can expect to be exempt.

A Private Member's Bill dealing with ransomware (**Bill**) was introduced as *Ransomware Payments Bill 2021*, into the House of Representatives by Tim Watts MP on the 21st of July and as *Ransomware Payments Bill 2021 (*no 2), by Senator the Hon Kristina Keneally to the Senate on 12 August 2021.

The Bill requires the reporting of ransomware payments "as soon as practicable" after they are made. The report must include all that is known about the attacker and details of the attack. Any personal information contained in the notification must not be disclosed.

At the time of writing there is no indication of whether the government favours notification after payment or may be considering mandatory notification when ransomware is identified and/or is associated with a demand for ransom.

## 2. PJCIS Report calls for a rethink on Security of Critical Infrastructure Reform

On 30 September 2021 the Parliamentary Joint Committee on Intelligence and Security (**PJCIS**) released its Advisory Report on the Security Legislation Amendment (Critical Infrastructure) Bill 2020 (**Report**). The Report recommends that the government split the Bill into two Bills:

1. Bill One is recommended to comprise an adjusted version of the existing Bill including expanded ownership and operation and mandatory cyber incident reporting. Adjustments include:

- Excluding risk management programs, declarations of Systems of National Significance and accompanying enhanced cyber security obligations.
- Changes to:
  - the mandatory data incident notification framework.
  - the meanings of cyber security incident and unauthorised access, modification or impairment to ensure that an insider threat is captured.
  - require publication, consolation and presentation to parliament of section 30BBA rules designed for the purposes of proposed section 30BB.
  - the definition of "Offensive cyber action" so that it operates on an inclusive basis.
  - include a definition of "Significant impact", for the purposes of s30BC.
  - include a reasonable timeframe to respond to consolations under proposed section 35AD to allow for the entity to reply before the ministerial authorisation is made.
- Possible changes to National Security Agency immunities listed in Schedule 2 of the Bill if, after review, considered appropriate.
- A mandated review by the PJCIS after 3 years.

2. Bill Two is recommended to include the provisions dealing with:

- Risk management programs, declarations of Systems of National Significance and accompanying enhanced cyber security obligations from the existing Bill.
- Modification and clarification of any definitions or meanings introduced by Bill One identified as requiring modification or clarification during rules development or otherwise. In this context it is It is notable that the Department of HA has not published the submissions or outcome of the Asset Definition Consultation which concluded in May.
- Alignment of the Positive Security Obligations with international standards or practices.
- Where an entity is adversely impacted by a decision under Bill One, a right of reply by the affected entity and consideration of that reply in the final determination.
- Adjustment of the secrecy obligations which apply to declarations of assets as Systems of National Significance. Such declarations only be confidential if the Minister is satisfied on reasonable grounds, that there is a significant risk of harm to Australia's defence or national security as a result of the disclosure of the regulatory status of the asset.
- Adjustment of the protected information provisions to enable the appropriate and lawful exchange of information among oversight and compliance assurance bodies.
- A merits review system of appeal to the security division of the AAT for certain determinations.
- Possible amendment to the types and breadth of immunities afforded to entities under the Schedule 2 of the Bill.

The PJCIS recommended that rules development continue while Bill Two is being prepared and the rules be included in the Explanatory Memorandum for Bill Two. The PJCIS recommended that it be required to review Bill Two once prepared. The Government is considering its response to the PJCIS report. Potential regulated entities are invited to participate in an online discussion regarding next steps on 19 October. You can register here.

**Please contact me if you have any questions regarding the matters discussed in this update. patrick@patrickfair.com 0411361534**