2019-2020-2021

THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

HOUSE OF REPRESENTATIVES

Ransomware Payments Bill 2021

EXPLANATORY MEMORANDUM

TABLE OF CONTENTS

GLOSSARY

The following abbreviations and terms are used in this Explanatory Memorandum:

Abbreviation	Definition
ACSC	Australian Cyber Security Centre, part of the Australian Signals Directorate
ASD	Australian Signals Directorate
The Bill	Ransomware Payments Bill 2021
IT	Information Technology

GENERAL OUTLINE

Ransomware is malicious software used to deny access to an organisation's IT systems and/or to threaten the release of private data unless a ransom is paid. It is the 'highest cyber threat' facing Australian businesses according to the Australian Cyber Security Centre (ACSC).

The last 12 months have seen attacks on JBS Foods which paralysed a company that employs 11,000 Australians across 47 sites; on Nine Entertainment which disrupted the network's ability to broadcast; and on the Colonial pipeline in the United States leading to widespread fuel shortages in the that country.

This is a stand-alone Bill to establish a mandatory reporting requirement for Commonwealth entities, State or Territory agencies, corporations, and partnerships who make ransomware payments in response to a ransomware attack.

The Bill will require entities who make a ransomware payment to notify the ACSC of key details of the attack, the attacker, and the payment. This information will be held by the ACSC and used to:

- Share de-identified information to the private sector through the ACSC threat-sharing platform.
- Collect and share information that may be used by law enforcement.
- Collect and share information to inform policy making and to track the effectiveness of policy responses.

Ransomware is a jobs and investment destroyer when the Australian economy can least afford it. Analysts suggest that the cost to the Australian economy of ransomware attacks in 2019 alone was in the order of $1 billion.

This Bill provides an important foundation for a comprehensive national ransomware strategy, which is needed to deal with the onslaught of ransomware attacks on Australian organisations.

Part 1 — Preliminary

The purpose of this Part is to create a definition of ransomware and set out the persons and entities to which the Bill applies.

Section 4 defines a ransomware attack as when an unauthorised person accesses, modifies, or impairs data and demands payment to repair or undo damage or prevent the publication or exfiltration of data. The definition of "unauthorised access, modification, or impairment" is as per section 476.2 of the *Criminal Code Act 1995* (Cth).

Section 5 applies the reporting requirement to ransomware attacks against all Australian organisations, excluding small businesses, sole traders, and unincorporated entities, and charities. The Bill is intended to apply to all Commonwealth entities (corporate and non-corporate), all State and Territory agencies, and specified private sector entities. The purpose of excluding small businesses is to limit compliance costs and to ensure that ACSC has access to high-quality actionable intelligence from the mandatory disclosures. "Small business entities" with an aggregate turnover of less than $10 million will be excluded from the scheme. This is the same meaning as in the *Income Tax Assessment Act 1997* (Cth).

Part 2 — Notification of ransomware payments

The purpose of this Part is to create a mandatory notification scheme for reporting ransomware payments, administered by the ACSC.

Section 8 establishes the mandatory notification requirement and sets out the information that must be provided by an entity to the ACSC. If an entity makes a ransomware payment, they must provide ACSC with their details, the details of the attacker and information about the attack to that extent that it is known. Information about the attack includes cryptocurrency wallet details, the amount of the payment, and indicators of compromise. Failure to notify the ACSC attracts a penalty.

Section 9 establishes the purposes for which the ACSC may use this information, which includes disclosing de-identified information for the purpose of informing the public and private sector about the current threat environment and disclosing information to Commonwealth, State, or Territory agencies for the purpose of law enforcement.

This section also protects entities who make disclosures by making it an offence to disclose personal information except for use by law enforcement.

Part 3 — Miscellaneous

The purpose of this Part is to give effect to the penalty provision for non-compliance established in Section 8.

Section 12 provides the Director-General of ASD with the power to delegate his or her functions under the Bill.

FINANCIAL IMPACT STATEMENT

ASD will meet the ongoing costs of administering the measures in this Bill within existing resources.

REGULATION IMPACT STATEMENT

A Regulation Impact Statement (RIS) was not required for the items in this Bill and a RIS was not prepared.

STATEMENT OF COMPATABILITY WITH HUMAN RIGHTS

The Bill engages the right to privacy and reputation by requiring entities who chose to make a ransomware payment to notify the ASCS and provide details of the ransomware attack and payment.

The cost of ransomware to the Australian economy in 2019 was estimated to be over $1 billion. Industry and cyber-security experts support the introduction of mandatory reporting scheme which will assist private entities and the public sector to better understand and respond to this threat.

The extent to which the Bill limits this right is mitigated by the requirement that ACSC de-identify this information and through the inclusion of penalties for misuse of the collected information.

The Bill is compatible with human rights because to the extent it may limit the right to privacy and reputation, those limitations are reasonable, necessary, and proportionate.