Computer Misuse (Amendment) Bill

Bill No. 36/2012.

Read the first time on 12th November 2012.

A BILL

i n t i t u l e d

An Act to amend the Computer Misuse Act (Chapter 50A of the 2007 Revised Edition) and to make consequential amendments to certain other written laws.

Be it enacted by the President with the advice and consent of the Parliament of Singapore, as follows:

Short title and commencement

1. This Act may be cited as the Computer Misuse (Amendment) Act 2012 and shall come into operation on such date as the Minister may, by notification in the *Gazette*, appoint.

Amendment of long title

2. The long title to the Computer Misuse Act (referred to in this Act as the principal Act) is amended by inserting, immediately after the word "modification", the words ", to require or authorise the taking of measures to ensure cybersecurity,".

Amendment of section 1

3. Section 1 of the principal Act is amended by inserting, immediately after the words "Computer Misuse", the words "and Cybersecurity".

Repeal and re-enactment of section 15A

4. Section 15A of the principal Act is repealed and the following section substituted therefor:

"**Cybersecurity measures and requirements**

15A.—(1) Where the Minister is satisfied that it is necessary for the purposes of preventing, detecting or countering any threat to the national security, essential services or defence of Singapore or foreign relations of Singapore, the Minister may, by a certificate under his hand, authorise or direct any person or organisation specified in the certificate (referred to in this section as the specified person) to take such measures or comply with such requirements as may be necessary to prevent, detect or counter any threat to a computer or computer service or any class of computers or computer services.

(2) The measures and requirements referred to in subsection (1) may include, without limitation —

(*a*) the exercise by the specified person of the powers referred to in sections 39(1)(*a*) and (*b*) and (2)(*a*) and (*b*)

and 40(2)(*a*), (*b*) and (*c*) of the Criminal Procedure Code (Cap. 68);

(*b*) requiring or authorising the specified person to direct another person to provide any information that is necessary to identify, detect or counter any such threat, including —

(i) information relating to the design, configuration or operation of any computer, computer program or computer service; and

(ii) information relating to the security of any computer, computer program or computer service;

(*c*) providing to the Minister or a public officer authorised by him any information (including real-time information) obtained from any computer controlled or operated by the specified person, or obtained by the specified person from another person pursuant to a measure or requirement under paragraph (*b*), that is necessary to identify, detect or counter any such threat, including —

(i) information relating to the design, configuration or operation of any computer, computer program or computer service; and

(ii) information relating to the security of any computer, computer program or computer service; and

(*d*) providing to the Minister or a public officer authorised by him a report of a breach or an attempted breach of security of a description specified in the certificate under subsection (1), relating to any computer controlled or operated by the specified person.

(3) Any measure or requirement referred to in subsection (1), and any direction given by a specified person for the purpose of taking any such measure or complying with any such requirement —

(*a*) shall not confer any right to the production of, or of access to, information subject to legal privilege; and

(*b*) subject to paragraph (*a*), shall have effect notwithstanding any obligation or limitation imposed or right, privilege or immunity conferred by or under any law, contract or rules of professional conduct, including any restriction on the disclosure of information imposed by law, contract or rules of professional conduct.

(4) A specified person who, without reasonable excuse, fails to take any measure or comply with any requirement directed by the Minister under subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 10 years or to both.

(5) Any person who, without reasonable excuse —

(*a*) obstructs a specified person in the taking of any measure or in complying with any requirement under subsection (1); or

(*b*) fails to comply with any direction given by a specified person for the purpose of the specified person taking any such measure or complying with any such requirement,

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 10 years or to both.

(6) No civil or criminal liability shall be incurred by —

(*a*) a specified person for doing or omitting to do any act if the specified person had done or omitted to do the act in good faith and for the purpose of or as a result of taking any measure or complying with any requirement under subsection (1); or

(*b*) a person for doing or omitting to do any act if the person had done or omitted to do the act in good faith and for the purpose of or as a result of complying with a direction given by a specified person for the purpose of taking any such measure or complying with any such requirement.

(7) The following persons shall not be treated as being in breach of any restriction upon the disclosure of information imposed by law, contract or rules of professional conduct:

(*a*) a specified person who, in good faith, obtains any information for the purpose of taking any measure under subsection (1) or complying with any requirement under that subsection, or who discloses any information to the Minister or a public officer authorised by the Minister, in compliance with any requirement under that subsection;

(*b*) a person who, in good faith, obtains any information, or discloses any information to a specified person, in compliance with a direction given by the specified person for the purpose of taking any measure under subsection (1) or complying with any requirement under that subsection.

(8) The following persons, namely:

(*a*) a specified person to whom a person has provided information in compliance with a direction given by the specified person for the purpose of taking any measure under subsection (1) or complying with any requirement under that subsection;

(*b*) a person to whom a specified person provides information in compliance with any requirement under subsection (1),

shall not use or disclose the information, except —

(i) with the written permission of the person from whom the information was obtained or, where the information is the confidential information of a third person, with the written permission of the third person;

(ii) for the purpose of preventing, detecting or countering a threat to a computer, computer service or class of computers or computer services;

(iii) to disclose to any police officer or other law enforcement authority any information which discloses the commission of an offence under this Act or any other written law; or

(iv) in compliance with a requirement of a court or the provisions of this Act or any other written law.

(9) Any person who contravenes subsection (8) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 12 months or to both.

(10) Where an offence is disclosed in the course of or pursuant to the exercise of any power under this section —

(*a*) no information for that offence shall be admitted in evidence in any civil or criminal proceedings; and

(*b*) no witness in any civil or criminal proceedings shall be obliged —

(i) to disclose the name, address or other particulars of any informer who has given information with respect to that offence; or

(ii) to answer any question if the answer would lead, or would tend to lead, to the discovery of the name, address or other particulars of the informer.

(11) If any book, document, data or computer output which is admitted in evidence or liable to inspection in any civil or criminal proceedings contains any entry in which any informer is named or described or which may lead to his discovery, the court shall cause those entries to be concealed from view or to be obliterated so far as may be necessary to protect the informer from discovery.

(12) In subsection (1), "essential services" means —

(*a*) services directly related to communications infrastructure, banking and finance, public utilities, public transportation, land transport infrastructure, aviation, shipping, or public key infrastructure; or

(*b*) emergency services such as police, civil defence or health services.".

Consequential amendments to other written laws

5. The provisions of the Acts specified in the first column of the Schedule are amended in the manner set out in the second column thereof.

THE SCHEDULE

Section 5

CONSEQUENTIAL AMENDMENTS TO OTHER WRITTEN LAWS

First column	*Second column*
1. Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Chapter 65A, 2000 Ed.)	
Second Schedule, Part III	Insert, immediately after the words "Computer Misuse" immediately above item 210, the words "and Cybersecurity".
2. Criminal Procedure Code (Chapter 68, 2012 Ed.)	
(*a*) Section 2(1)	Insert, immediately after the words "Computer Misuse" in the definition of "computer", the words "and Cybersecurity".
(*b*) Second Schedule	Insert, immediately after the words "Computer Misuse" in item 4, the words "and Cybersecurity".
3. Goods and Services Tax Act (Chapter 117A, 2005 Ed.)	
Section 2(1)	Insert, immediately after the words "Computer Misuse" in the definitions of "computer" and "computer output", the words "and Cybersecurity".

THE SCHEDULE — *continued*

First column	*Second column*
4. Income Tax Act (Chapter 134, 2008 Ed.)	
Section 65B(4)	Insert, immediately after the words "Computer Misuse", the words "and Cybersecurity".
5. Manufacture of Optical Discs Act (Chapter 170C, 2005 Ed.)	
Section 20(4)	Insert, immediately after the words "Computer Misuse", the words "and Cybersecurity".
6. Private Lotteries Act (Chapter 250, 2012 Ed.)	
Section 13(5)	Insert, immediately after the words "Computer Misuse" in the definitions of "computer" and "computer output", the words "and Cybersecurity".
7. Strategic Goods (Control) Act (Chapter 300, 2003 Ed.)	
Section 2(1)	Insert, immediately after the words "Computer Misuse" in the definition of "computer", the words "and Cybersecurity".

EXPLANATORY STATEMENT

This Bill seeks to amend the Computer Misuse Act (Cap. 50A) to enable the Government to take more effective and timely measures to prevent, detect and counter cyber attacks that may threaten national security, essential services, defence or the foreign relations of Singapore. It does this by expanding the scope of the existing section 15A. Currently, section 15A allows the Minister to authorise persons to take measures to prevent or counter threats against a computer or computer service if the Minister is satisfied that this is necessary for preventing or

countering a threat to the national security, essential services, defence of Singapore or the foreign relations of Singapore.

The Bill also makes consequential amendments to certain other written laws.

Clause 1 relates to the short title and commencement.

Clause 2 amends the long title to the Act to include cybersecurity.

Clause 3 changes the short title of the Act in section 1 from Computer Misuse Act to the Computer Misuse and Cybersecurity Act.

Clause 4 repeals and re-enacts section 15A.

The new section 15A expands the scope of the existing section 15A in the following ways:

(*a*) by enabling the Minister to not only authorise but also direct a person or an organisation (the specified person) to take certain measures and comply with certain requirements, which may include a measure or requirement that is necessary for detecting a threat against a computer or computer service (new subsection (1));

(*b*) by specifying that the measures and requirements that the Minister may authorise or direct include one of requiring the specified person to direct another person to disclose information that is necessary to identify, detect or counter any such threat, providing to the Minister or a public officer authorised by him information necessary to prevent, detect or counter cyber threats; as well as furnishing a report concerning a breach or an attempted breach of cybersecurity (new subsection (2));

(*c*) by providing that any such measure or requirement overrides any obligation or limitation imposed or right, privilege or immunity conferred by any law, contract or rules of professional conduct, but not legal privilege (new subsection (3));

(*d*) by criminalising non-compliance by a specified person with a measure or requirement directed by the Minister, the obstruction of a specified person in taking such measure or complying with such requirement, and non-compliance with a direction by a specified person given pursuant to such measure or requirement (new subsections (4) and (5));

(*e*) by conferring various immunities for acts done pursuant to such measure or requirement (new subsections (6) and (7));

(*f*) by imposing a duty to protect any information obtained pursuant to such measure or requirement (new subsections (8) and (9));

(*g*) by modifying the definition of "essential services". Currently, it covers services directly related to communications infrastructure, banking and finance, public utilities, public transportation, or public key infrastructure

(i.e. systems providing electronic trust services), as well as emergency services like police, civil defence and medical services. It now includes services directly related to land transport infrastructure, aviation, shipping, and other health services besides medical services (new subsection (12)).

Clause 5 makes consequential amendments to certain other written laws as a result of the change to the short title of the Act.

EXPENDITURE OF PUBLIC MONEY

This Bill will not involve the Government in any extra financial expenditure.