First published in the Government *Gazette*, Electronic Edition, on 30 August 2018 at 5 pm.

No. S 519

CYBERSECURITY ACT 2018
(ACT 9 OF 2018)

CYBERSECURITY (CRITICAL INFORMATION INFRASTRUCTURE) REGULATIONS 2018

ARRANGEMENT OF REGULATIONS

In exercise of the powers conferred by sections 17(10) and 48 of the Cybersecurity Act 2018, Mr S Iswaran, who is charged with the responsibility for the portfolio of the Prime Minister as regards cybersecurity, makes the following Regulations:

PART 1

PRELIMINARY

Citation and commencement

1. These Regulations are the Cybersecurity (Critical Information Infrastructure) Regulations 2018 and come into operation on 31 August 2018.

Definitions

2. In these Regulations, unless the context otherwise requires —

"Appeals Secretary" means the Appeals Secretary appointed under regulation 17(1);

"appellant" means an owner of a critical information infrastructure who makes an appeal to the Minister under section 17(1) of the Act;

"working day" means any day except a Saturday, Sunday or public holiday.

PART 2

PROVIDING INFORMATION TO COMMISSIONER

Information to ascertain if computer, etc., fulfils criteria of critical information infrastructure

3.—(1) For the purposes of subsection 2 of section 8 of the Act, a notice to provide relevant information to the Commissioner under that subsection must be given in writing in the form set out on the Internet website at https://www.csa.gov.sg.

(2) The Commissioner may by notice under section 8(2) of the Act require a person who appears to be exercising control over a computer or computer system, to provide to the Commissioner the following information relating to that computer or computer system as is relevant for the purpose of ascertaining whether the computer or computer system fulfils the criteria of a critical information infrastructure:

(*a*) name and location of the computer or computer system;

(*b*) the function that the computer or computer system is employed to serve;

(*c*) the type of essential service, if applicable, that the computer or computer system has a role in making available in Singapore, and the role performed by the computer or computer system;

(*d*) the person or persons, or other computer or computer systems, that the computer or computer system mentioned in the notice serves;

(*e*) information relating to the design of the computer or computer system, including the parameters and key components of the computer system, as specified in the notice;

(*f*) the name, address, contact and business registration number (if applicable) of the person to whom the notice is given;

(*g*) if the person to whom the notice is given is not the owner of the computer or computer system, the name, address, contact and business registration number (if applicable) of the owner;

(*h*) such other information as the Commissioner may require in order to ascertain whether the computer or computer system fulfils the criteria of a critical information infrastructure.

Information relating to critical information infrastructure

4.—(1) For the purposes of subsection (1) of section 10 of the Act, a notice to the owner of a critical information infrastructure to furnish information required under that subsection must be given in writing in the form set out on the Internet website at https://www.csa.gov.sg.

(2) The Commissioner may by notice under section 10(1) of the Act require the owner of the critical information infrastructure to provide to the Commissioner —

(*a*) the following information on the design, configuration and security of the critical information infrastructure:

(i) a network diagram depicting every key component and interconnection in the critical information infrastructure, and any external connection and dependency that the critical information infrastructure may have;

(ii) for every key component in the critical information infrastructure, the following details:

(A) its name and description;

(B) its physical location;

(C) any operating system and version;

(D) any key software and version;

(E) its internet protocol address and any open port, if the component is internet facing;

(F) the name and address of the operator, if the owner is not the operator;

(iii) the types of data processed on or stored in the critical information infrastructure;

(iv) the name and contact of every individual having overall responsibility for the cybersecurity of the critical information infrastructure;

(*b*) the following information on the design, configuration and security of any other computer or computer system under the owner's control that is interconnected with or that communicates with the critical information infrastructure:

(i) the name and description of that other computer or computer system;

(ii) the physical location of that other computer or computer system;

(iii) the name and address of its operator, if the owner is not the operator;

(iv) a description of any function provided by that other computer or computer system;

(v) the types of data exchanged with the critical information infrastructure;

(vi) the operating system and version;

(vii) the key software and version;

(viii) how that other computer or computer system is interconnected with or communicates with the critical information infrastructure, including the communication protocol of that other computer or computer system with the critical information infrastructure;

(*c*) the name of any outsourced service provider supporting the critical information infrastructure, and the nature of the outsourced service; and

(*d*) such other information as the Commissioner may require in order to ascertain the level of cybersecurity of the critical information infrastructure.

Report of cybersecurity incident in respect of critical information infrastructure, etc.

5.—(1) For the purposes of section 14(1) of the Act, where a cybersecurity incident mentioned in section 14(1)(*a*), (*b*) or (*c*) of the Act occurs, the owner of a critical information infrastructure must notify the Commissioner of the occurrence of the cybersecurity incident in the following form and manner:

(*a*) by submitting the following details in the manner specified in paragraph (2), within 2 hours after becoming aware of the occurrence:

(i) the critical information infrastructure affected;

(ii) the name and contact number of the owner of the critical information infrastructure;

(iii) the nature of the cybersecurity incident, whether it was in respect of the critical information infrastructure or an interconnected computer or computer system, and when and how it occurred;

(iv) the resulting effect that has been observed, including how the critical information infrastructure or any interconnected computer or computer system has been affected;

(v) the name, designation, organisation and contact number of the individual submitting the notification;

(*b*) by providing to the fullest extent practicable the following supplementary details in writing in the form set out on the Internet website at https://www.csa.gov.sg within 14 days after the submission mentioned in sub-paragraph (*a*):

(i) the cause of the cybersecurity incident;

(ii) its impact on the critical information infrastructure, or any interconnected computer or computer system;

(iii) what remedial measures have been taken.

(2) The details mentioned in paragraph (1)(*a*) must be submitted —

(*a*) by calling the telephone number specified by the Commissioner; or

(*b*) if the owner is unable to submit the details in the manner set out in sub-paragraph (*a*) within a reasonable time —

(i) by text message to the telephone number specified by the Commissioner; or

(ii) in writing, in the form set out on the Internet website at https://www.csa.gov.sg, to the electronic address specified by the Commissioner.

(3) For the purposes of section 14(1)(*a*) and (*b*) of the Act, the following are prescribed cybersecurity incidents in respect of a critical information infrastructure or an interconnected computer or computer system:

(*a*) any unauthorised hacking of the critical information infrastructure or the interconnected computer or computer system to gain unauthorised access to or control of the critical information infrastructure or interconnected computer or computer system;

(*b*) any installation or execution of unauthorised software, or computer code, of a malicious nature on the critical information infrastructure or the interconnected computer or computer system;

(*c*) any man-in-the-middle attack, session hijack or other unauthorised interception by means of a computer or computer system of communication between the critical information infrastructure or the interconnected computer or computer system, and an authorised user of the critical information infrastructure or the interconnected computer or computer system, as the case may be;

(*d*) any denial of service attack or other unauthorised act or acts carried out through a computer or computer system that adversely affects the availability or operability of the critical information infrastructure or the interconnected computer or computer system.

(4) In paragraph (3) —

"interception", in relation to a communication to or from a critical information infrastructure or an interconnected computer or computer system, includes —

(*a*) listening to or recording of the communication; and

(*b*) acquiring the substance, meaning or purport of that communication;

"interconnected computer or computer system" means any computer or computer system under the owner's control that is interconnected with or that communicates with the critical information infrastructure.

Cybersecurity risk assessment

6.—(1) For the purposes of section 15(1)(*b*) of the Act, a cybersecurity risk assessment of a critical information infrastructure must be conducted in the following form and manner:

(*a*) the assessment must —

(i) identify, as far as is reasonably practicable, every cybersecurity risk to the critical information infrastructure;

(ii) evaluate the likelihood of the occurrence, and the possible consequences, of the materialisation of each identified cybersecurity risk; and

(iii) identify the action that the owner of the critical information infrastructure will take in respect of each identified cybersecurity risk;

(*b*) the report of the assessment must cover the following:

(i) the methodology used in the cybersecurity risk assessment;

(ii) a description of every identified cybersecurity risk to the critical information infrastructure;

(iii) the evaluated likelihood and possible consequences of the materialisation of each identified cybersecurity risk;

(iv) the identified action that the owner of the critical information infrastructure will take in respect of each identified cybersecurity risk.

(2) The first cybersecurity risk assessment of a critical information infrastructure must be completed within 6 months after the date of the notice issued under section 7(1) of the Act or, subject to section 15(1)(*b*) of the Act, such longer period as the Commissioner may allow in a particular case.

(3) In this regulation, "cybersecurity risk", in relation to a critical information infrastructure, means the risk that a vulnerability in the cybersecurity of the critical information infrastructure may be exploited by a cybersecurity threat or incident.

PART 3

APPEAL TO MINISTER

Division 1 — Notice of appeal

Notice of appeal

7.—(1) An appeal to the Minister under section 17(1) of the Act must be made according to this Part.

(2) A notice of appeal must be in writing and must —

(*a*) state the appellant's name and address;

(*b*) state an address in Singapore for the service of documents;

(*c*) provide the information required under section 17(3) of the Act, and as required under paragraph (3), (4) or (5), as applicable;

(*d*) state the relief sought by the appellant; and

(*e*) be signed and dated by a duly authorised officer of the owner of the critical information infrastructure.

(3) A notice of appeal in respect of a decision mentioned in section 17(1)(*a*) of the Act must state the grounds of the owner's belief that the computer or computer system ought not to have been designated under section 7 of the Act.

(4) A notice of appeal in respect of a written direction mentioned in section 17(1)(*b*) of the Act must —

(*a*) identify the written direction the appeal relates to; and

(*b*) specify the part of the direction being appealed against.

(5) A notice of appeal in respect of any provision in any code of practice or standard of performance, or any amendment to a code of practice or standard of performance, mentioned in section 17(1)(*c*) of the Act, must state the provision of the code of practice or standard of performance, or amendment, being appealed against.

(6) An appellant who wishes to make an appeal must —

(*a*) file the notice of appeal with the Appeals Secretary; and

(*b*) serve on the Commissioner a copy of the notice of appeal, and file with the Appeals Secretary a notice of service of the copy of the notice of appeal.

(7) A notice of service mentioned in paragraph (6)(*b*) must be in the form set out on the Internet website at https://www.mci.gov.sg.

Receipt of notice of appeal

8. Upon receiving a notice of appeal, the Appeals Secretary must —

(*a*) inform the appellant that the notice is received and of the date and time that the notice was received;

(*b*) enter the appeal in a list and assign a number to the appeal, which will be the title of the appeal;

(*c*) inform the appellant of the title of the appeal; and

(*d*) forward the notice of appeal to the Minister.

Summary dismissal of appeal

9. The Minister may determine the appeal by confirming the decision, written direction, or provision or amendment of the Commissioner appealed against if —

(*a*) the Minister considers that the notice of appeal discloses no valid ground of appeal;

(*b*) the Minister considers that the appellant is not entitled to appeal; or

(*c*) the Minister is satisfied that the appellant has, without reasonable excuse —

(i) failed to make the appeal within the time specified under section 17(2) of the Act; or

(ii) failed to comply with any direction of the Minister concerning the appeal.

Amendment of notice of appeal

10.—(1) An appellant may only amend a notice of appeal or include additional evidence in support of the notice of appeal if —

(*a*) the Minister permits; or

(*b*) the Minister directs the appellant to amend a notice that the Minister considers to be materially incomplete, unduly lengthy or unclear.

(2) Where the Minister permits or directs an amendment to a notice of appeal or permits the inclusion of additional evidence under paragraph (1), the Minister must give such further or consequential direction as is necessary, including specifying a later date for the Commissioner to file a defence.

(3) The Minister must not permit an amendment unless —

(*a*) the amendment is related to a matter that came to the owner's knowledge after the notice of appeal was filed;

(*b*) at the time the notice of appeal was filed it was not practicable to include, or omit, the subject matter of the amendment in the notice of appeal; or

(*c*) there are exceptional circumstances to do so.

(4) The Minister must not permit any additional evidence to be included unless —

(*a*) it could not have been obtained with reasonable diligence for use at the time the notice of appeal was filed;

(*b*) it would likely have an important influence in determining the outcome of the appeal, though it need not be decisive; and

(*c*) it is apparently credible.

Withdrawal of notice of appeal

11. An appellant may, if the Minister permits, withdraw the appellant's appeal at any time before the Minister determines the appeal.

Division 2 — Response to notice of appeal

Defence

12.—(1) The Commissioner's defence to a notice of appeal must be in writing and —

(*a*) state the Commissioner's name and address;

(*b*) state an address in Singapore for the service of documents;

(*c*) state concisely the facts and arguments upon which the Commissioner will rely;

(*d*) be accompanied by any evidence supporting the defence; and

(*e*) be signed and dated by a duly authorised officer.

(2) The Commissioner must, within 30 days after the date on which the Commissioner receives a copy of the notice of appeal and any accompanying evidence —

(*a*) file a defence with the Appeals Secretary; and

(*b*) serve on the appellant a copy of the defence, and file with the Appeals Secretary a notice of service of the copy of the defence.

(3) A notice of service mentioned in paragraph (2)(*b*) must be in the form set out on the Internet website at https://www.mci.gov.sg.

Amendment of defence

13.—(1) The Commissioner may only amend the defence or include additional evidence to support the defence if —

(*a*) the Minister permits; or

(*b*) the Minister directs the Commissioner to amend a defence that the Minister considers to be materially incomplete, unduly lengthy or unclear.

(2) Where the Minister permits or directs an amendment to a defence or permits the inclusion of additional evidence under paragraph (1), the Minister must give such further or consequential direction as is necessary, including specifying a later date for the appellant to file a reply.

(3) The Minister must not permit an amendment unless —

(*a*) the amendment is related to a matter that came to the Commissioner's knowledge after the defence was filed;

(*b*) at the time the defence was filed it was not practicable to include, or omit, the subject matter of the amendment in the defence; or

(*c*) there are exceptional circumstances to do so.

(4) The Minister must not permit any additional evidence to be included unless —

(*a*) it could not have been obtained with reasonable diligence for use at the time the defence was filed;

(*b*) it would likely have an important influence in determining the outcome of the appeal; and

(*c*) it is apparently credible.

Division 3 — Reply and rejoinder

Reply by appellant

14.—(1) An appellant may submit a reply to the Commissioner's defence, not later than 21 days after the date on which a copy of the defence is served on the appellant —

(*a*) by filing the reply with the Appeals Secretary; and

(*b*) by serving on the Commissioner a copy of the reply, and filing with the Appeals Secretary a notice of service of the copy of the reply.

(2) The appellant's reply must be in writing, and be signed and dated by a duly authorised officer of the owner of the critical information infrastructure, and must —

(*a*) succinctly present the arguments of fact or law in reply to the Commissioner's defence; and

(*b*) be accompanied by any evidence supporting the reply.

(3) A notice of service mentioned in paragraph (1)(*b*) must be in the form set out on the Internet website at https://www.mci.gov.sg.

Rejoinder by Commissioner

15.—(1) If the Minister permits, the Commissioner may submit a rejoinder to the appellant's reply, not later than 21 days after the date that the Minister grants that permission —

(*a*) by filing the rejoinder with the Appeals Secretary; and

(*b*) by serving on the appellant a copy of the rejoinder, and filing with the Appeals Secretary a notice of service of the copy of the rejoinder.

(2) The Commissioner's rejoinder must be in writing, and be signed and dated by a duly authorised officer, and must —

(*a*) succinctly present the arguments of fact or law in response to the appellant's reply; and

(*b*) be accompanied by any evidence supporting the rejoinder.

(3) A notice of service mentioned in paragraph (1)(*b*) must be in the form set out on the Internet website at https://www.mci.gov.sg.

New matter in reply or rejoinder prohibited

16.—(1) Any reply by an appellant to a defence must only address matters raised in the defence, and any rejoinder by the Commissioner to a reply must only address matters raised in the reply.

(2) The Minister may disregard any matter in a reply or a rejoinder that was included in contravention of paragraph (1).

Division 4 — Management of proceedings

Appeals Secretary

17.—(1) The Minister may appoint a public officer as the Appeals Secretary for the purposes of this Part.

(2) The Appeals Secretary provides, in relation to every appeal under section 17 of the Act, administrative and secretariat support —

(*a*) to the Minister; and

(*b*) to any Appeals Advisory Panel established under section 18 of the Act.

(3) The Appeals Secretary must act according to such instructions as the Minister may give from time to time and is, in particular, responsible for —

(*a*) the acceptance, transmission, service and custody of documents according to this Part;

(*b*) the establishment and maintenance of a list of all notices of appeal filed with the Minister; and

(*c*) the keeping of a record of the proceedings of an Appeals Advisory Panel in such form as the chairperson may direct.

Consolidation of appeal

18.—(1) Where 2 or more pending appeals involve the same organisation or the same or similar issues, the Minister may at any time, on the request of any party to such an appeal or on the Minister's initiative, direct that the appeals or any issue raised in the appeals be consolidated or heard together.

(2) Before making a direction under paragraph (1), the Minister must invite all parties to the relevant proceedings to make submissions on whether the direction should be made.

(3) Where any appeal has been consolidated under paragraph (1), the Minister may make such direction as is necessary for the proper administration of those appeals.

Failure to comply with direction or time limits

19.—(1) The Minister may, if the Minister considers that the justice of the case so requires, order that a party to an appeal be debarred from taking further part in the appeal proceedings without the permission of the Minister, if the party has habitually and persistently, and without reasonable ground, failed to comply with —

(*a*) any regulation concerning the appeal; or

(*b*) any direction given by the Minister concerning the appeal.

(2) The Minister may, in consideration of an appeal, disregard any information or document submitted after expiry of the time limit for the submission of such information or document specified under these Regulations or any direction of the Minister.

Irregularities

20.—(1) Any irregularity resulting from a failure to comply with any regulation in this Part before the Minister has determined an appeal does not of itself render the appeal proceedings void.

(2) The Minister may give such direction as the Minister thinks just to cure or waive an irregularity mentioned in paragraph (1) before determining an appeal, if the Minister considers that any person may have been prejudiced by the irregularity.

Calculation of time

21.—(1) Where the time specified by the Minister or any regulation in this Part for doing any act expires on a Saturday, Sunday or public holiday, the act is done in time if done on the next working day.

(2) A period expressed in months ends with the expiry of whichever day in the last month is the same day of the month as the day on which the event or the act or thing after or from which the period is to be calculated happens or is done.

(3) If, in a period expressed in months, the day on which it should expire does not occur in the last month, the period ends with the expiry of the last day of that month.

Extension of time

22.—(1) Subject to paragraph (2), the Minister may on the application of a person, extend the time specified for doing anything under this Part or in any direction made by the Minister under this Part, even if the application for the extension is made after the time specified has expired.

(2) The Minister may only extend the period of time in the following situations, if the Minister is satisfied that it is just to do so because of exceptional circumstances in a particular case:

(*a*) filing a notice of appeal under regulation 7 or defence under regulation 12;

(*b*) amending a notice of appeal under regulation 10 or defence under regulation 13.

PART 4

APPEALS ADVISORY PANEL

Dissolution of Appeals Advisory Panel

23. An Appeals Advisory Panel established in respect of an appeal dissolves when —

(*a*) the Minister determines the appeal; or

(*b*) the appellant withdraws the appeal in accordance with regulation 11.

Made on 30 August 2018.

GABRIEL LIM
Permanent Secretary
(Cybersecurity),
Prime Minister's Office,
Singapore.

[AK02.001.001; AG/LEGIS/SL/70A/2015/2 Vol. 1]