



Feedback to Public Consultation Paper on the Draft Cybersecurity Bill

Feedback on sections of the draft Cybersecurity Bill

| No. | Section of Bill | Feedback |
|-----|---|---|
| 1 | <p><u>Part 5 – Cybersecurity Services Providers</u></p> <p><u>Second Schedule – Section 25 – Licensable Security Services</u></p> <p>There is a distinction made between ‘licensable investigative cybersecurity service’ and ‘non-licensable investigative cybersecurity service’.</p> | <p>What are the criteria for each category and how does one apply for the licenses?</p> |
| 2 | <p><u>Part 1 – Preliminary – Interpretation</u></p> <p>2.—(1) In this Act, unless the context otherwise requires ...</p> <p>“owner of a critical information infrastructure” means a person who –</p> <p>(a) Has effective control over the operations of the critical information infrastructure and has the ability and right to carry out changes to the critical information infrastructure; or</p> <p>(b) is responsible for ensuring the continuous functioning of the critical information infrastructure.</p> | <p>The definition of “owner of a critical information infrastructure” is very broad. Who is the responsible party? An individual, or a company’s senior management or a company’s Board of Directors?</p> <p>We are concerned that without a tighter definition, global companies (also known as multi-nationals or MNCs) will have practical difficulties in identifying the “owner” of CII in a multi-national organization with multiple affiliated corporations and multiple lines of management across many jurisdictions and multiple different businesses and functions within one affiliate.</p> <p>For example, a Singapore corporation owns the hardware of critical information infrastructure and employs a team of employees to operate such critical information infrastructure. In such a case, is the corporation the “owner” or would the team of employees be the “owner” of such critical information infrastructure?</p> <p>Using the same example, suppose now instead of employing its own team, an affiliated corporation within Singapore provides manpower</p> |

| | | |
|---|---|---|
| | | <p>resources to manage and operate the critical information infrastructure of the Singapore corporation, who then will be the “owner” of critical information infrastructure?</p> <p>Taking the example one step further, suppose now, the affiliated corporation is situated outside of Singapore and manages and operates the critical information infrastructure of the Singapore corporation. Who then will be considered the “owner” of the critical information infrastructure?</p> <p>Separately, do the words “effective control” and “responsible for ensuring” extend to management oversight or do they require active control?</p> <p>Clarifying or narrowing the definition of “owner” will bring greater certainty for businesses.</p> <p>Further clarification on the location of data centres and cloud operators and the owner of the data and infrastructure is sought.</p> |
| 3 | <p><u>Part 3 – Critical Information Infrastructure – Designation of critical information infrastructure</u></p> <p>7.—(1) The Commissioner may by a written notice, designate a computer or computer system as a critical information infrastructure for the purposes of this Act, if the Commissioner is satisfied that —</p> <p>(a) the computer or computer system fulfils the criteria of a <u>critical information infrastructure</u>; and</p> <p>(b) the computer or computer system is located wholly or partly in Singapore.</p> | <p>It is important that the Commissioner correctly identifies only information infrastructure that is truly “critical” to national security to be subjected to the requirements of this legislation. This is to avoid placing an unnecessary burden on owners of information infrastructure that are not truly “critical” within the meaning of the Bill.</p> <p>For this reason, the Commissioner should be required to avail himself with all necessary information in determining whether an information infrastructure is indeed a <i>critical information infrastructure</i> (“CII”) (as defined in Section 2 of the Bill).</p> |


| | | |
|---|--|---|
| | | <p>In this regard, we suggest that prior to exercising his powers under Section 7, the Commissioner be required to make due inquiry with the owner to understand the nature of its information infrastructure. Such inquiry should be robust and transparent.</p> <p>Additionally, should the owner have any reasons to disagree that its information infrastructure is a CII, it should be allowed to present its case to the Commissioner before he makes a final determination under this Section 7.</p> <p>Will the designation of CII by the Commissioner be carried out in phases? And if so, what is the CSA's planned timeline for such designations?</p> |
| 4 | <p><u>Part 3 – Critical Information Infrastructure – [Confidentiality provision] – Duties of owner of critical information infrastructure</u></p> <p>10. An owner of a critical information infrastructure has the duty to —</p> <p>(a) provide the Commissioner with information on the technical architecture of the critical information infrastructure;</p> <p>(b) comply with such codes of practice, standards of performance or directions in relation to the critical information infrastructure as may be issued by Commissioner;</p> <p>(c) notify the Commissioner of —</p> <p>(i) any cybersecurity incident that occurs in respect of the critical information infrastructure;</p> | <p>Currently, as it stands, Clause 10 sets out six mandatory compliance areas for CII owners to comply with.</p> <p>We suggest that the Commissioner be granted the discretion to waive compliance where the Commissioner is satisfied that the CII owners have in place alternatives that are the equivalent of and/or supersede the compliance requirements envisaged in this bill. This is in order that businesses can avoid duplication of effort and costs.</p> <p>For section (e), this definition is too broad and further clarification is sought as to what constitutes “regular risk assessments.”</p> |

| | | |
|---|---|--|
| | <p>(ii) any cybersecurity incident that occurs in respect of any computer or computer system under the owner's control that is interconnected with or communicates with the critical information infrastructure; and</p> <p>(iii) any cybersecurity incident of a type as prescribed by notification or as specified by the Commissioner.</p> <p>(d) cause regular audits of the compliance of the critical information infrastructure with the Act, codes of practice and standards of performance to be carried out by an auditor approved or appointed by the Commissioner;</p> <p>(e) carry out regular risk assessments of the critical information infrastructure as required by the Commissioner; and</p> <p>(f) participate in cybersecurity exercises as required by the Commissioner.</p> | |
| 5 | <p><u>Part 3 – Critical Information Infrastructure – Codes of practice or standards of performance</u></p> <p>12.—(1) The Commissioner may, from time to time —</p> <p>(a) issue or approve one or more codes of practice or standards of performance for the regulation of the cybersecurity of critical information infrastructure; or</p> <p>(b) amend or revoke any code of practice or standard of performance issued or approved under paragraph (a).</p> | <p>For major companies with a global footprint, having to comply with multiple cybersecurity regimes across different jurisdictions may lead to undue stifling of productivity and certainly to an increase in business costs. Harmonization between local statutory compliance requirements and a company's global cybersecurity compliance measures would be key in minimizing administration and costs.</p> |

| | | |
|--|--|--|
| | | <p>Moreover, any codes of practice or standards of performance issued by the Commissioner would invariably have varying degrees of impact on different CII owners across the various essential services tabled in Schedule 1 of the Bill. Therefore, it would be vital that CII owners be allowed to participate in the Commissioner’s development and subsequent updates of any such codes of practice or standards of performance. A public consultation process before any changes is recommended.</p> |
| | <p><u>Part 3 – Critical Information Infrastructure – Duty to report cybersecurity incident in respect of critical information infrastructure, etc.</u></p> <p>15.—(1) An owner of a critical information infrastructure must notify the Commissioner in such manner and form as may be prescribed, within the prescribed period after the occurrence of any of the following events:</p> <p>(a) a significant cybersecurity incident in respect of the critical information infrastructure;</p> <p>(b) a significant cybersecurity incident in respect of any computer or computer system under the owner’s control that is interconnected with or communicates with the critical information infrastructure;</p> <p>(c) any other type of cybersecurity incident in respect of the critical information infrastructure that the Minister may prescribe by notification or the Commissioner may specify by written direction.</p> | <p>Firstly, clarification is sought as to what the “prescribed period” is within which notification needs to be made to the Commissioner.</p> <p>Secondly, as Section 15 is a mandatory reporting requirement, it is imperative for CII owners to understand what a “significant” cybersecurity incident is. It needs to be clearly defined.</p> <p>Clear guidance on what and how “significant” is determined would be helpful (whether in this legislation or subsequent guidelines, codes of practice or standards of performance).</p> <p>Cross-referencing to Section 21(1): we note that the term “serious” cybersecurity incidents is used and some qualitative definition of the severity threshold of “serious” is made in Section 21(2). It would be helpful if the Bill uses only one term (either “serious” or “significant”) based on the definition of “serious” in Section 21(1). Alternatively, we suggest that the Bill to provides a clear distinction between what a “serious cybersecurity incidents” is and what a “significant cybersecurity incident” is.</p> |

| | | |
|---|--|---|
| 7 | <p><u>Part 3 – Critical Information Infrastructure – Cybersecurity audits and risk assessments of critical information infrastructure</u></p> <p>16.—(1) An owner of a critical information infrastructure must, at least once every three years —</p> <p>(a) cause an audit, of the compliance of the owner’s critical information infrastructure with respect to the Act, codes of practice and standards of performance, to be carried out by an auditor approved or appointed by the Commissioner; and</p> <p>(b) conduct a cybersecurity risk assessment of the owner’s critical information infrastructure.</p> | <p>As with our comment to Section 10 above, we suggest that instead of making the third-party audit and the conduct of risk assessment as mandatory requirements, the Commissioner be granted the discretion to waive compliance where the CII owner is able to demonstrate to the Commissioner’s satisfaction that it has in place alternatives that are equivalent to and/or supersede the compliance requirements envisaged in the Bill. This is in order that businesses can avoid duplication of effort and costs.</p> <p>We also seek to clarify if the auditor is an internal or an external auditor and if expenses for appointing an auditor are fully under the responsibility of the CII owner.</p> <p>With the audits and risk assessments in place, will there be a new set of auditing standards that companies could take guidance from?</p> |
| 8 | <p><u>Part 4 – Responding to and Prevention of Cybersecurity Incidents – Powers to investigate and prevent serious cybersecurity incidents</u></p> <p>21.—(1) Where information has been received by the Commissioner regarding a cybersecurity threat or a cybersecurity incident... the Commissioner may exercise... the following powers...:</p> <p>...</p> <p>(b) direct, by written notice, any person to carry out such remedial measures, or to cease carrying on such activities, as may be specified, in relation to a computer or computer system that the investigating officer has</p> | <p>The Commissioner’s broad powers under Section 21 can be highly intrusive to any private information infrastructure.</p> <p>In a global business, information infrastructure can be structurally complex and parts of which may reside across multiple geographical off-shore and on-shore locations. There is the concern that any “remedial measures” or installation of any software ordered by the Commissioner, if not managed appropriately, may lead to unforeseen impacts on our systems and business.</p> |

| | | |
|---|--|--|
| | <p>reasonable cause to suspect is or was impacted by a cybersecurity incident, in order to minimize cybersecurity vulnerabilities;</p> <p>(c) require the owner of a computer or computer system to carry out steps to assist with the investigation, including but not limited to —</p> <p>...</p> <p>(iv) allowing the investigating officer to install on the computer or computer system any software program, or interconnect any equipment to the computer or computer system, for the purpose of the investigation.</p> | <p>We suggest that in the exercise of his powers under this Section, the Commissioner engage and work in consultation with CII owners to ensure that any “remedial measures” or software installation ordered will achieve the cybersecurity outcome sought but not lead to any unforeseen adverse impact either to their systems or businesses.</p> |
| 9 | <p><u>Part 5 – Cybersecurity Service Providers – No person to provide licensable non-investigative cybersecurity service without license</u></p> <p>29.—(1) No person may —</p> <p>(a) engage in the business of providing, for reward, any licensable non-investigative cybersecurity service to other persons; or</p> <p>(b) advertise, or in any way hold out, that the person (who is in the business of providing a licensable non-investigative cybersecurity service) provides for reward, or is willing to provide for reward, the licensable non-investigative cybersecurity service,</p> <p>except under and in accordance with a [licensable] non-investigative cybersecurity service provider’s license granted under this Act.</p> | <p>Cross-reference to Section 26. In Section 26, the Bill expressly creates an exception for “a person employed under a contract of service”.</p> <p>For the avoidance of doubt, we suggest that Section 29 similarly expressly create an exception for “a person employed under a contract of service”.</p> <p>Will such exception also cover “bug bounty” and other freelance workers?</p> |

| General Comments | | |
|-------------------------|---|---|
| 10 | CII owners are expected to incur costs to meet the compliance requirements of this Bill. | Does the Government have any plans to provide financial support to CII owners to off-set the associated compliance cost and, if so, what kinds of support will be provided? |
| 11 | It is viewed that the Bill lacks as part Cybersecurity Management for Process Control System. | <p>A proposed Industrial Cybersecurity Standard (ICSS) is attached for consideration.</p>  <p>INDUSTRIAL CYBER SECURITY STANDARE</p> |
| 12. | Operational controls for the Internet of Things (IOT) | The Bill should also define operational controls for IOT infrastructure as a CII given its planned ubiquity and impact on homes, government and businesses. |

INDUSTRIAL CYBER SECURITY STANDARD (ICSS)

July 2017

1. INTRODUCTION

This Industrial Cyber Security Standards (ICSS) provides technical requirements and recommendations for managing the Cyber Security of Process Control System (PCS). The PCS includes both the industrial automation equipment and its network. The Cyber Security management includes the Information Security Management System (ISMS). The ICSS adopt ISO 27001, ISO 27002 and ISA 99/ IEC 62443 international standards. This ICSS is applicable to Process Control System in the Critical Information Infrastructure (CII) facilities and excludes Cyber Security management of Business and Office Networks.

2. RESPONSIBILITY FOR THE ASSETS

To achieve appropriate security of organizational asset, the PCS owner shall clearly identify the assets, including labelling, and maintain register of all PCS and other assets. The inventory register shall be reviewed on a quarterly basis, including physical checks, as part of the quarterly self-assessment.

3. MANAGEMENT OF REMOVABLE MEDIA

The PCS owner shall verify, record and tag all removable media used for accessing the PCS equipment, including the holder of the removable media. Only the CII's Technical Authority shall approve specific personnel to utilize removable media for data transfer from the PCS equipment. Only the CII's Technical Authority shall approve the specific PCS equipment to be enabled for removable media access.

4. PHYSICAL ACCESS

All PCS equipment shall be located in secured areas where physical access control are in place. All authorized personnel accessing the PCS equipment shall wear identification badge / tag at all times.

5. SYSTEM ACCESS

The system access to the PCS shall be password protected. Typically, the PCS should be able to support at least four levels of password protection as follows:

- 5.1 Administrator level enables global engineering access to the PCS equipment and is the highest authorization level. Only personnel authorized by the CII's Technical Authority shall have Administrator access.
- 5.2 Engineering level that enables engineering configuration access to the PCS equipment. Only the PCS owner and personnel authorized by the PCS owner shall have engineering access to the PCS equipment.
- 5.3 Supervisor level that enables settings adjustment to be carried out in the PCS. For DCS Operator Workstations, the Supervisor level is normally accessed by the senior Operations personnel, such as the Operations Shift Supervisor, who requires access to change settings such as alarm settings, etc.
- 5.4 Operator level that enables the PCS equipment to be operated. The Operator level is typically the lowest security access level. For DCS Operator Workstations, the Operator security level does not require password access and access is available for all Panel Operators on 24 hours basis, as the facility is operated round-the-clock, all year round. DCS Operation Workstation password requirement shall be disabled.

Except for the Operator level in DCS Operator Workstations, all PCS equipment requiring password authentication should have the following password management:

- The password policy shall comply with CII's ICT Policy.
- The password shall be changed based on CII's ICT Policy. However, in event any password authentication breach is detected, the password shall be changed immediately.
- The PCS owner shall remove access rights of individuals who are no longer authorized to access.

6. NETWORK ACCESS

All external network access to the PCS equipment, for both CII's business network and external network, shall comply with CII's ICT policies and be approved by the CII's Technical Authority.

7. MALWARE PROTECTION

The PCS equipment shall be protected against the introduction of malware through appropriate system access controls and MOC procedures.

8. BACKUP

System back-up procedures shall be established for all critical PCS equipment. The back-up procedure should typically state the following:

- frequency of back-up
- requirement for testing the back-up on a regular basis on a test equipment and not in an operating PCS equipment.
- physically secured off-site storage of the back-up
- back-up shall be able to restore the PCS equipment, in event of unexpected failure of the PCS equipment, including disaster recovery.

9. MONITORING LOGS

The PCS owner shall regularly monitor the PCS equipment event logs for user activities, exceptions, faults and information security events. All event logs should be documented. The PCS owner shall alert any unusual activities to the CII's Technical Authority.

10. CLOCK SYNCHRONISATION

All the PCS equipment clocks should be automatically synchronized against a centralized system monitoring clock.

11. SOFTWARE

All software installed in the operating PCS equipment in the facility shall be authorized by the CII's Technical Authority. The software and their updates shall be pre-qualified by PCS equipment's vendor for ensuring if full compatibility to existing PCS systems is assured. Updates to the PCS equipment operating system in the CII shall be executed by either PCS equipment vendor or by the PCS owner, as authorized by the CII's Technical Authority.

12. TECHNICAL VULNERABILITY MANAGEMENT

The PCS owner shall seek at least quarterly updates from the critical PCS equipment vendor on the software and hardware vulnerability status. For MS Windows, Linux and UNIX operating platform, the PCS owner shall also obtain vulnerability updates from PCS equipment vendor. The vulnerability status and any system hardware or software updates shall be recorded. All system hardware and software updates and upgrades, such as patch management, anti-virus updates, etc., shall be endorsed by the PCS equipment vendor and approved by the CII's Technical Authority. This includes MS Windows updates and upgrades, including patch management.

Anti-virus software should be configured to automatically scan files accessed by the PCS and configured to log and notify detection of malware infected files. The PCS equipment vendor recommendations shall be adhered when configuring automated anti-virus scans. If automated scans cannot be implemented on a particular PCS equipment due to operational constraints, the PCS owner shall manually conduct the anti-virus scan when the PCS equipment is off-line. Similar shall apply for MS patch management.

13. WIRELESS CONNECTIVITY

There shall be no wireless connectivity to any PCS equipment. Similarly, the use of wireless dongles in any PCS equipment is not permitted.

14. SAFETY NETWORK

The safety network of a Safety Instrumented System (SIS) shall not be connected to the PCS. The SIS safety network shall be in a separate and independent network domain. Access to the SIS shall only be from the dedicated SIS engineering workstation. Remote access to the SIS is not allowed, even from the DMZ. Only non-safety critical information is allowed to be communicated between the SIS and PCS through a dedicated network communication bus at the SIS. All critical information between the SIS and PCS shall be hardwired.

15. VENDOR REQUIREMENTS

All PCS equipment that utilizes Microsoft Windows operating system shall be delivered with up to date anti-virus software and security patches. Vendor shall document all equipment details, including expiry dates of software licenses, if any.

16. PROCEDURES

Operating procedures for all relevant PCS equipment shall be made available for authorized users. For DCS Operator Workstations, the facilities operational procedures and guidelines for Panel Operators are deemed sufficient for the Panel Operators. PCS equipment shall have supplier documentation to ensure safe and reliable operation of the equipment. These documentation shall include:

- Installation and configuration
- Back up procedures
- System error handling, including system restart and recovery procedures
- System monitoring procedures
- Disaster recovery procedures

17. INCIDENT MANAGEMENT

The PCS owner shall log and notify the CII's Technical Authority of all incidents occurring in the PCS equipment. The CII's Technical authority is responsible to classify the incident as Low, Medium, High or Very High risk. All High and Very High risk incidents shall be reported to the CII's Technical Authority and the management.

18. BUSINESS CONTINUITY

The CII's Technical Authority is responsible to identify the business impact of each PCS equipment and to provide the Business Continuity assurance in event of minor or major damage to the PCS equipment.

19. CYBERSECURITY TRAINING & DEVELOPMENT

CII's Technical Authority to enforce PCS equipment vendor to provide Training and Awareness Program.