立法會

Legislative Council

LC Paper No. LS74/2024

Paper for the House Committee Meeting
on 13 December 2024

Legal Service Division Report on
Protection of Critical Infrastructures (Computer Systems) Bill

I. SUMMARY

1.	**The Bill**	The Bill seeks to: (a) protect the security of the computer systems of Hong Kong's critical infrastructures; (b) regulate the operators of such infrastructures; (c) provide for the investigation into, and response to, computer-system security threats and incidents in respect of such computer systems; and (d) provide for related matters.
2.	**Public Consultation**	According to the Administration, relevant stakeholders have been engaged since 2023. Consultation on the legislative proposals was conducted from 2 July to 1 August 2024. Almost all the views received expressed support for the legislative proposals or offered constructive suggestions. A briefing and engagement sessions were also held with key stakeholders.
3.	**Consultation with LegCo Panel**	The Panel on Security was consulted on the legislative proposals at its meeting on 2 July 2024 and a paper on the consultation report was issued to Panel members on 2 October 2024. Members generally supported the legislative proposals but expressed various concerns.
4.	**Conclusion**	The Legal Service Division is scrutinizing the legal and drafting aspects of the Bill. As the Bill seeks to introduce a new statutory regime with a view to protecting the security of the computer systems of critical infrastructures of Hong Kong, Members may consider forming a Bills Committee to study the Bill in detail.

II. REPORT

The date of First Reading of the Bill is 11 December 2024. Members may refer to the Legislative Council ("LegCo") Brief (File Ref.: SBCR 1/3231/2022 Pt. 5) issued by the Security Bureau on 4 December 2024 for further details.

Object of the Bill

2. The Bill seeks to:

(a) protect the security of the computer systems of Hong Kong's critical infrastructures ("CIs");

(b) regulate the operators of such infrastructures;

(c) provide for the investigation into, and response to, computer-system security threats and incidents in respect of such computer systems; and

(d) provide for related matters.

Background

3. At present, there is no dedicated legislation to protect the security of the computer systems of CIs of Hong Kong. According to paragraph 2 of the LegCo Brief, nowadays the operation of CIs has become more dependent on the Internet, computer systems, telecommunications infrastructures, smart devices, etc. Their computer systems are also increasingly vulnerable to attacks with serious consequences affecting the entire society. The Bill is thus introduced to establish a new statutory regulatory regime to require operators of CIs to protect their computer systems, enhance their capabilities to respond to attacks, and report to the regulatory authority in the event of security incidents in respect of computer systems. Key provisions of the Bill are summarized in the ensuing paragraphs.

Provisions of the Bill

Proposed meaning of "critical infrastructure" etc.

4. Part 1 of the Bill seeks to provide for definitions on terms such as "critical infrastructure", which is proposed to mean any infrastructure that is essential to the continuous provision in Hong Kong of an essential service in a specified sector (i.e. energy, information technology, banking and financial services, air transport, land transport, maritime transport, health services, and telecommunications and broadcasting services as specified in Schedule 1 to the Bill) ("Type 1 CI"), or any other infrastructure the damage, loss of functionality or data leakage of which may hinder or otherwise substantially affect the maintenance of critical societal or economic activities in Hong Kong ("Type 2 CI").

Proposed functions and powers of the regulating authorities

5. Part 2 (clauses 3 to 10) of the Bill seeks to provide for the establishment of the regulating authorities. The Chief Executive would be empowered to appoint a

Commissioner of CI (Computer-system Security) ("Commissioner") (clause 3). The Commissioner, together with the "designated authorities" specified in column 2 of Part 2 of Schedule 2 to the Bill (i.e. the Monetary Authority and the Communications Authority), would be the "regulating authorities" for the purposes of the Bill (clause 5).

6. The proposed functions of the regulating authorities include identifying CIs, designating CI operators, designating critical computer systems, and issuing codes of practice (clauses 4 and 6). Part 3 of the Bill seeks to provide that:

(a) a regulating authority could ascertain whether an infrastructure is a specified CI for the authority by considering factors such as the kind of service provided by the infrastructure and the implications of damage being caused to the infrastructure (clause 11);

(b) the Commissioner could, by written notice, designate an organization that operates a specified CI as a CI operator, having considered factors such as how dependent the core function[1] of the CI concerned is on computer systems, and the sensitivity of the digital data controlled by the organization in respect of the infrastructure (clause 12); and

(c) a regulating authority could, by written notice to a CI operator, designate a computer system (whether under the control of the CI operator or not) that is (i) accessible by the operator in or from Hong Kong; and (ii) essential to the core function of a CI operated by the operator, as a critical computer system for the infrastructure, having considered factors such as the role of the subject system in respect of the core function of the CI concerned (clause 13).

7. For the purpose of identifying CIs, designating CI operators or designating critical computer systems, the regulating authorities would be empowered to require an organization operating (or appearing to have control over) an infrastructure, or a CI operator to provide any information the authorities reasonably consider necessary for ascertaining whether the infrastructure is a specified CI, whether to designate the organization as a CI operator, or whether to designate a computer system as a critical computer system. The Commissioner could require a CI operator to provide any information the Commissioner reasonably considers necessary to better understand the critical computer systems of the CI (clauses 14 to 17). Clause 18 of the Bill proposes that it would be an offence if an organization without reasonable excuse fails to comply with any of the requirements to provide information under clauses 14(2), 15(3), 16(2) or 17(3), and would be liable (i) on summary conviction to a fine of HK$3,000,000 (HK$300,000 for a non-CI operator) and in the case of a continuing offence, to a further fine of HK$60,000 (HK$30,000 for a non-CI operator) for every day during which the offence continues; or (ii) on conviction on indictment to a fine of HK$5,000,000 (HK$500,000 for a non-CI operator) and in the case of a continuing offence, to a further fine of HK$100,000 (HK$50,000 for a non-CI operator) for every day during which the offence continues.

---

[1] Clause 2(1) of the Bill seeks to provide that in relation to Type 1 CI, "core function" would mean the provision of the essential service concerned. For Type 2 CI, "core function" would mean any function of the infrastructure that is essential to the maintenance of critical societal or economic activities in Hong Kong.

Proposed obligations of critical infrastructure operators

8. Part 4 (clauses 19 to 28) of the Bill proposes to impose the following obligations on CI operators:

(a) in relation to the organization of CI operators: (i) maintaining an office in Hong Kong; (ii) notifying the regulating authority of operator changes; and (iii) setting up and maintaining computer-system security management unit (clauses 19 to 21) ("category 1 obligations");

(b) in relation to the prevention of threats and incidents: (i) notifying the regulating authority of material changes to certain computer systems; (ii) submitting and implementing computer-system security management plans (see Schedule 3 to the Bill for further details); (iii) conducting computer-system security risk assessments (see Schedule 4 to the Bill for further details); and (iv) arranging to carry out computer-system security audits (see Schedule 5 to the Bill for further details) (clauses 22 to 25) ("category 2 obligations"); and

(c) in relation to incident reporting and response: (i) participating in computer-system security drills; (ii) submitting and implementing emergency response plans; and (iii) notifying the Commissioner of computer-system security incidents within the time specified in Schedule 6 to the Bill (clauses 26 to 28) ("category 3 obligations").

9. It would be an offence if a CI operator fails to comply with any of the above three categories of obligations. For example, clauses 26(4) and 28(6) of the Bill propose that a CI operator who fails to comply with the requirement to participate in a computer-system security drill or to notify the Commissioner of a computer-system security incident would commit an offence, and would be liable on summary conviction to a fine of HK$3,000,000 or on conviction on indictment to a fine of HK$5,000,000.

10. The Bill proposes to empower the Commissioner to direct (in writing) a CI operator to do (or refrain from doing) an act in relation to the compliance with all the above three categories of obligations. It would be an offence if the CI operator fails to comply with such direction and would be liable: (i) on summary conviction to a fine of HK$3,000,000 and in the case of a continuing offence, to a further fine of HK$60,000 for every day during which the offence continues; or (ii) on conviction on indictment to a fine of HK$5,000,000 and in the case of a continuing offence, to a further fine of HK$100,000 for every day during which the offence continues (clause 7).

Proposed powers of authorized officers to make inquiries and conduct investigations in relation to computer-system security threats etc.

11. Part 5 (clauses 29 to 42) of the Bill proposes that for example, if the Commissioner reasonably suspects that an event that has an actual adverse effect on the computer-system security of a critical computer system of a CI has occurred, or a computer-system security threat has occurred in respect of a critical computer system of a CI, the Commissioner could direct an authorized officer to make inquiries for the purpose of identifying what caused the event, or to carry out an investigation into (and to respond to) the computer-system security threat for the purposes of identifying what caused the threat (clauses 29 and 34).

12. It is proposed that a range of enforcement powers would be granted to authorized officers including:

(a) requiring a CI operator to e.g. produce documents that the officer has reasonable grounds to believe to be relevant to the inquiries or investigations ("Relevant Documents") and give an explanation in relation to the Relevant Documents (clauses 30 and 35);

(b) entering premises to e.g. search for Relevant Documents, if the specified conditions are met (clauses 31, 32, 38, 39 and 40); and

(c) requiring an investigated CI operator e.g. not to use the investigated system if the Commissioner is satisfied that the specified conditions are met, and applying for a warrant from a magistrate to impose a requirement on an organization having (or appearing to have) control over the investigated system to e.g. preserve the state of the system (clauses 36 and 37).

Proposed powers of regulating authorities to investigate offences

13. Part 6 (clauses 43 to 46) of the Bill seeks to provide for investigation powers of the regulating authorities in respect of the proposed offences under the Bill. Clause 43 of the Bill proposes that if a regulating authority (e.g. the Commissioner) reasonably suspects that an offence under the Bill has been committed, the Commissioner could direct an authorized officer to carry out an investigation into the offence and, for this purpose, to require an organization to e.g. answer in writing a written question relating to any matter under investigation. Clause 46 of the Bill proposes that an authorized officer could apply to a magistrate for a warrant authorizing the officer e.g. to enter the premises or to access and inspect an electronic device if the specified conditions are met.

Proposed appeal mechanism

14. Part 7 (clauses 47 to 49) of the Bill seeks to establish an appeal mechanism. Clause 48 of the Bill proposes that an organization aggrieved by any decision made by a regulating authority could lodge an appeal against such decision. Clause 49 of the Bill further proposes that an appeal board appointed for an appeal may e.g. confirm, vary, or reverse any decision to which the appeal relates and such decision would be final. Schedule 7 to the Bill seeks to provide for further details concerning appeals.

Miscellaneous matters

15. Part 8 (clauses 50 to 70) of the Bill seeks to provide for miscellaneous matters, which include:

(a) the proposed power of the Commissioner to exempt a CI operator from any of the three categories of obligations under Part 4 of the Bill by written notice (which would not be subsidiary legislation and thus not subject to LegCo's scrutiny) (clause 55);

(b) providing for the protection of informers who have given information with respect to an investigation under Part 5 or 6 of the Bill (clause 59);

(c) empowering the Secretary for Security ("Secretary") to make regulations (which would be subsidiary legislation subject to the negative vetting procedure of LegCo pursuant to section 34 of the Interpretation and General

Clauses Ordinance (Cap. 1)) for the better carrying out of the provisions of the Bill (clause 69); and

(d) empowering the Secretary, by notice published in the Gazette, to amend any of the Schedules to the Bill (such notice would be subsidiary legislation subject to the negative vetting procedure of LegCo pursuant to section 34 of Cap. 1) (clause 70).

Commencement

16. The Bill, if passed, would come into operation on a day to be appointed by the Secretary by notice published in the Gazette.

Public Consultation

17. According to paragraphs 34 and 35 of the LegCo Brief, relevant stakeholders (including organizations that may be designated as CI operators and computer-system security service providers) have been engaged since 2023. Consultation on the legislative proposals was conducted from 2 July to 1 August 2024. Almost all the views received expressed support for the legislative proposals or offered constructive suggestions. The Administration also held a briefing session for major chambers of commerce and all stakeholders on the consultation report on 1 November 2024, and arranged engagement sessions with selected key potential CI operators before the introduction of the Bill.

Consultation with LegCo Panel

18. As advised by the Clerk to the Panel on Security, the Panel was consulted on the legislative proposals at its meeting on 2 July 2024 and a paper on the consultation report was issued to Panel members for information on 2 October 2024. Members generally supported the legislative proposals, but also raised various concerns such as the technology neutrality of the regulatory regime, potential liabilities of third-party service providers of designated CI operators (and their staff), deterrent effect of the penalties for the proposed offences, standards of the various proposed statutory obligations, and availability of competent computer security personnel in the market.

Conclusion

19. The Legal Service Division is scrutinizing the legal and drafting aspects of the Bill. As the Bill seeks to introduce a new statutory regime with a view to protecting the security of the computer systems of CIs of Hong Kong, Members may consider forming a Bills Committee to study the Bill in detail.

Prepared by

Joyce CHAN
Senior Assistant Legal Adviser
Legislative Council Secretariat
12 December 2024