

立法會
Legislative Council

LC Paper No. CB(2)773/2025(04)

Ref : CB2/PL/SE

Panel on Security

Meeting on 6 May 2025

**Background brief on the establishment of the Office of the Commissioner
of Critical Infrastructure (Computer-system Security)**

Purpose

This paper provides background information on the establishment of the Office of the Commissioner of Critical Infrastructure (Computer-system Security) (“the Commissioner”) for the implementation of the Protection of Critical Infrastructures (Computer Systems) Ordinance (Ord. No. 4 of 2025) (“the Ordinance”), and gives an account of Members’ past discussions on the subject.

Background

Protection of Critical Infrastructures (Computer Systems) Ordinance

2. The Ordinance was published in the Gazette on 28 March 2025 after the Protection of Critical Infrastructures (Computer Systems) Bill (“the Bill”) was passed by the Legislative Council (“LegCo”) on 19 March 2025.¹ It **imposes three categories of statutory obligations** (details in [Appendix 1](#)) **on designated operators of specified critical infrastructures (“CIs”)**² to ensure the putting in

¹ The Ordinance as published in the Gazette is accessible at <https://www.legco.gov.hk/yr2025/english/ord/2025ord004-e.pdf>. It will come into operation on a day to be appointed by the Secretary for Security by notice published in the Gazette.

² Pursuant to section 2 of the Ordinance, CI means (a) any infrastructure that is essential to the continuous provision in Hong Kong of an essential service in a sector specified in Schedule 1 to the Ordinance; or (b) 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. Eight sectors are currently specified in Schedule 1 to the Ordinance, namely energy; information technology; banking and financial services; air transport; land transport; maritime transport; healthcare services; and telecommunications and broadcasting services.

place of appropriate measures to protect their computer systems and minimize the chance of essential services being disrupted or compromised due to cyberattacks and other incidents, thereby maintaining the normal functioning of the Hong Kong society and the normal life of the people.

3. Pursuant to section 3 of the Ordinance, the Chief Executive may, for the purpose of the Ordinance, appoint a person to be the Commissioner. The Commissioner is to be appointed **for a term of not more than five years, but is eligible for reappointment**. The Commissioner is entitled to be **paid the remuneration and allowance determined by the Secretary for Security**. The **Commissioner** and the **designated authorities** (“DAs”)³ as specified in the Ordinance are the **regulating authorities**. The functions of regulating authorities include identifying CIs, designating CI operators, designating critical computer systems, as well as monitoring and supervising the compliance of CI operators under their regulation with the relevant statutory obligations. Details of the statutory functions of the Commissioner and DAs are set out in [Appendix 2](#).

Establishment of the Commissioner’s Office

4. According to the Administration, drawing on the practices in Mainland China, Macao, Australia, the European Union, Singapore, the United Kingdom and the United States, **a Commissioner’s Office**, headed by the Commissioner with the aid of directorate officers from the Digital Policy Office (“DPO”) and the Hong Kong Police Force (“HKPF”), **will be set up under the Security Bureau** for implementing the statutory regulatory regime. The Administration’s target is to **establish the Commissioner’s Office within one year after the passage of the Bill** and to **designate CI operators in phases within six months after the establishment of the Commissioner’s Office**.

Members’ views and concerns

5. Given the extensive scope and complexity of the Commissioner’s work portfolio, Members expressed concern about **the filling of the post of the Commissioner**, as well as **the establishment of the Commissioner’s Office**.

³ Currently, the Monetary Authority and the Communications Authority are specified in column 2 of Part 2 of Schedule 2 to the Ordinance as DAs for the purpose of the Ordinance. The Monetary Authority is responsible for regulating those organizations of the banking and financial services sector as specified in column 4 of Part 2 of the above Schedule, whereas the Communications Authority is responsible for regulating those organizations of the communications and broadcasting sector as specified in column 4 of Part 2 of the above Schedule.

The Administration advised that the Commissioner's Office would have an overall establishment of about 30 to 40 personnel, comprising the Commissioner, two directorate officers from DPO and HKPF, as well as non-directorate personnel to provide policy, administrative, liaison and clerical support, etc. The Commissioner post would be filled through open recruitment. With due regard to the principles of streamlining manpower and maximising the use of existing resources, two-thirds of the staff members of the Commissioner's Office would be deployed through existing resources, including personnel seconded from DPO and HKPF.

6. Members held the view that **proper coordination should be made between the Commissioner and DAs** to ensure that the two could perform their respective functions through the division of work concerning the monitoring and supervision of the relevant statutory obligations. They sought the Administration's elaboration with examples on the circumstances under which the Commissioner would exercise the power conferred by section 54 of the Ordinance to perform functions in respect of CIs and CI operators regulated by DAs if necessary.

7. The Administration advised that the Commissioner would not intervene in the work and decisions of DAs unless necessary, and would maintain close communication with DAs to ensure consistency of compliance standards. Section 54 of the Ordinance was to provide flexibility for the Commissioner to exercise the catch-all power under exceptional and special circumstances that it was necessary to timely protect critical computer systems of CIs and in the public interest, say in situations of extreme urgency where time did not permit the issuance of directions via DA; and where DA was unable to operate as usual due to special circumstances.

Relevant papers

8. A list of relevant papers available on the LegCo website is in [Appendix 3](#).

Obligations of critical infrastructure operators

Category	Obligations (see Part 4 of the Protection of Critical Infrastructures (Computer Systems) Ordinance)
<p><u>Category 1</u></p> <p>Obligations relating to organization of critical infrastructure operators</p>	<p>(a) maintaining an office in Hong Kong</p> <p>(b) notifying the relevant regulating authority of operator change</p> <p>(c) setting up and maintaining computer-system security management unit</p>
<p><u>Category 2</u></p> <p>Obligations relating to prevention of computer-system security threats and computer-system security incidents</p>	<p>(a) notifying the relevant regulating authority of material changes to certain computer systems</p> <p>(b) submitting and implementing computer-system security management plans</p> <p>(c) conducting computer-system security risk assessments</p> <p>(d) arranging to carry out computer-system security audits</p>
<p><u>Category 3</u></p> <p>Obligations relating to incident reporting and response</p>	<p>(a) participating in computer-system security drills</p> <p>(b) submitting and implementing emergency response plans</p> <p>(c) notifying computer-system security incidents</p>

**Functions of the Commissioner of Critical Infrastructure
(Computer-system Security) and the designated authorities**

<p align="center">Functions of the Commissioner of Critical Infrastructure (Computer-system Security)</p> <p align="center">(see Section 4 of the Protection of Critical Infrastructures (Computer Systems) Ordinance)</p>	<p align="center">Functions of the designated authorities</p> <p align="center">(see Section 6 of the Protection of Critical Infrastructures (Computer Systems) Ordinance)</p>
<ul style="list-style-type: none"> ● to identify critical infrastructures and designate critical infrastructure operators (“CI operators”) and critical computer systems 	<ul style="list-style-type: none"> ● to identify critical infrastructures regulated by the authority (“subject infrastructures”) and designate CI operators and critical computer systems for such infrastructures
<ul style="list-style-type: none"> ● to issue, revise and maintain codes of practice in respect of category 1 obligations, category 2 obligations and category 3 obligations of CI operators 	<ul style="list-style-type: none"> ● to issue, revise and maintain codes of practice in respect of category 1 obligations and category 2 obligations of CI operators regulated by the authority (“subject operators”)
<ul style="list-style-type: none"> ● to monitor and supervise compliance with the provisions of the Ordinance 	<ul style="list-style-type: none"> ● to monitor and supervise compliance with category 1 obligations and category 2 obligations
<ul style="list-style-type: none"> ● to regulate CI operators with regard to the computer-system security of the critical computer systems of critical infrastructures 	<ul style="list-style-type: none"> ● to regulate subject operators with regard to the computer-system security of the critical computer systems of subject infrastructures to the extent that such regulation relates to category 1 obligations and category 2 obligations
<ul style="list-style-type: none"> ● to monitor, investigate and respond to computer-system security threats and computer-system security incidents in respect of the critical computer systems of critical infrastructures 	
<ul style="list-style-type: none"> ● to coordinate the implementation of the Ordinance with designated authorities and government departments 	<ul style="list-style-type: none"> ● to facilitate the Commissioner’s performance of the Commissioner’s functions under the Ordinance
<ul style="list-style-type: none"> ● to perform any other functions imposed or conferred on the Commissioner under the Ordinance or any other Ordinance 	<ul style="list-style-type: none"> ● to perform any other functions imposed or conferred on the authority under the Ordinance.

List of relevant papers on the establishment of the Office of the Commissioner of Critical Infrastructure (Computer-system Security)

Committee	Date of meeting	Paper
Panel on Security	2 July 2024	Agenda item III: Proposed legislative framework to enhance protection of the computer systems of critical infrastructure Minutes of meeting
	2 October 2024*	Information paper on "Consultation report on proposed legislative framework to enhance protection of the computer systems of critical infrastructures" provided by the Administration
Bills Committee on Protection of Critical Infrastructures (Computer Systems) Bill	13 March 2025*	Report of the Bills Committee
Finance Committee	11 April 2025	Administration's replies to Members' initial written questions raised in the examination of the Estimates of Expenditure 2025-2026 (Reply serial nos.: SB002, SB007, SB024 and SB025)

* Issue date