For discussion on
6 May 2025

Legislative Council Panel on Security

Proposal to Create Directorate Posts in the Office of the Commissioner of Critical Infrastructure (Computer-system Security)

PURPOSE

This paper seeks Members' support for the creation of three directorate posts in the Office of the Commissioner of Critical Infrastructure (Computer-system Security) ("Commissioner's Office") of the Security Bureau ("SB") to implement the Protection of Critical Infrastructures (Computer Systems) Ordinance ("the Ordinance").

BACKGROUND

Policy Objective

2. To protect the computer systems of critical infrastructures ("CIs") in Hong Kong and minimize the chance of essential services being disrupted or compromised due to cyberattacks, the Legislative Council ("LegCo") passed the Ordinance on 19 March 2025. The Ordinance imposes three categories of statutory obligations on designated operators of CIs ("CI Operators"), namely Category 1 organizational obligations, Category 2 preventive obligations, and Category 3 incident reporting and response obligations[1]. This is to ensure that CI Operators have put in place appropriate measures to protect their computer systems and minimize the chance of essential services

[1] Category 1 organizational obligations include maintaining an address and office in Hong Kong; reporting operator change; setting up a computer-system security management unit supervised by a dedicated supervisor.
Category 2 preventive obligations include reporting material change in respect of Critical Computer Systems ("CCSs"); preparing and implementing a computer-system security management plan; conducting computer-system security risk assessments; and conducting computer-system security audits.
Category 3 incident reporting and response obligations include participating in computer-system security drills; preparing an emergency response plan; and reporting security incidents in respect of CCSs within a designated timeframe.

being disrupted or compromised due to cyberattacks, thereby maintaining the normal functioning of the Hong Kong society and the normal life of the people.

3. The SB plans to table the Commencement Notice at LegCo in July 2025 to appoint 1 January 2026 as the date for the Ordinance to come into effect. The Commissioner's Office will be formally set up under the SB on the same date to implement the Ordinance.

PROPOSAL

4. We propose to create the following three directorate posts in the SB to lead the Commissioner's Office –

(a) a new one-rank grade for the post of the Commissioner of Critical Infrastructure (Computer-system Security) ("the Commissioner") and one permanent directorate/non-civil service post (D3);

(b) one supernumerary time-limited post[2] of Chief Systems Manager ("CSM")(D1), designated as Deputy Commissioner (Compliance) ("DC(Com)") for three years; and

(c) one time-limited post of Chief Superintendent of Police ("CSP") (Police Pay Scale ("PPS") 55 or D1-equivalent), designated as Deputy Commissioner (Operations) ("DC(Ops)") for three years.

5. The Commissioner's Office will have a total establishment of 32 staff. In addition to the three proposed directorate posts, it will comprise 11 police officers seconded from the Hong Kong Police Force, 12 computer system professionals, two legal professionals and four administrative / clerical staff. Out of the 32 staff, 21 will be deployed through internal resources. The proposed organization chart of the Commissioner's Office is at **Annex 1**.

JUSTIFICATIONS

(i) To create a new one-rank grade and a permanent directorate post/non-civil service post (D3)

6. The Commissioner leading the Commissioner's Office plays a very important role in maintaining the computer-system security of CIs in Hong

[2] The civil service establishment includes posts on the permanent establishment and those on the non-permanent establishment (i.e. time-limited posts). Time-limited directorate posts are referred to as "supernumerary directorate posts", which are time-limited posts on the non-permanent establishment. It does not mean they are not counted towards the establishment.

Kong. The Commissioner must possess excellent cybersecurity expertise, international exposure, law enforcement experience and strategic management capability. At the technical level, the Commissioner needs to be familiar with cybersecurity standards and the operations of CIs in order to accurately identify CI Operators and develop Codes of Practice ("CoPs"). The Commissioner also needs to keep abreast of the latest international threat trends and protective measures, so as to ensure that the regulatory framework is in line with global standards. At the management level, the Commissioner needs to co-ordinate inter-departmental efforts, establish an efficient notification mechanism, and make prompt decisions and co-ordinate contingency actions in the event of an incident. In addition, the Commissioner needs to possess a high degree of political sensitivity and communication skills to clearly communicate compliance requirements to CI Operators, which are predominantly large enterprises, while balancing regulatory stringency with the practical needs of the industry, and enhancing the overall network resilience through regular drills and compliance investigations. The Commissioner's leadership has a direct bearing on the effectiveness of enforcement of the Commissioner's Office, which is closely related to the safety of Hong Kong's CIs and social stability.

7. In this regard, the leadership and representation of a senior directorate officer is of paramount importance. We consider it necessary to create a new one-rank grade and a permanent post/non-civil service post at D3 rank to take up the role of the Commissioner under the Ordinance and lead the Commissioner's Office with expertise in computer-system security, extensive management experience and good communication and co-ordination skills.

8. We note that there are other posts of "Commissioner" in other bureaux of the Government. They are ranked at around D2 to D8, depending on the scope of work and the level of responsibilities. We consider that the Commissioner's appointment at D3 has balanced the need for authority and responsibility with the prudent use of resources. The proposed job description of the Commissioner is at **Annex 2**.

9. Section 69 of the Ordinance provides that the Secretary for Security may give the Commissioner such directions relating to the performance of his functions under the Ordinance as the Secretary considers appropriate. The Commissioner will be accountable to the Secretary for Security through his immediate supervisor, the Permanent Secretary for Security. The Permanent Secretary for Security is mainly responsible for assisting the Secretary in formulating and implementing security policies, co-ordinating the work of the disciplined services under his purview (including the Police, Immigration Department, Customs and Excise Department, Fire Services

Department, Correctional Services Department and Government Flying Service), monitoring and supervising matters relating to public order and security, national security, counter-terrorism, immigration control and emergency response, as well as explaining relevant policies to the LegCo and the public. The Permanent Secretary for Security is also required to oversee the operation of the Bureau and the allocation of resources to ensure the effective implementation of various security measures. The organization chart of the SB after the establishment of the Commissioner's Office is at **Annex 3**.

10. The specific tasks to be undertaken by the Commissioner's Office under the leadership of the Commissioner are detailed below.

Identify CIs and designate CI Operators and Critical Computer Systems ("CCSs")

11. CIs are the linchpin of society and economy and are crucial to the normal functioning of society. They are closely related to the lives of citizens. It is important to maintain the effective and efficient functioning of the CCSs of these infrastructures. Upon the commencement of the Ordinance, the Commissioner's Office will be responsible for identifying these CIs and, based on the extent of reliance on computer systems for the core functions of these infrastructures, the sensitivity of the data and the management control, etc., designate the CI Operators and the CCSs to be subject to the regulation of the Ordinance for effective protection.

12. Each of the above steps, from the identification of CIs to the designation of CI Operators and CCSs, involves close communication with CI Operators. They include requesting the submission of the system structure and information, and providing the CI Operators with sufficient opportunities to make representations and explanations. It must be a prudent and credible process to ensure that all CI Operators will be identified and regulated under the Ordinance without omission, so as to enhance the overall computer-system security. Therefore, the Commissioner and the Deputy Commissioners leading the Commissioner's Office taking forward the above work must have good connection and comprehensive understanding of the CI Operators and computer systems in different industries, provide guidance and supervision in the process, and ultimately make judgment and designation to ensure that the designation is in compliance with the requirements of the Ordinance and is credible.

Issue CoPs

13. The Ordinance sets out the framework of the new regime and the statutory obligations of CI Operators. It also empowers the Commissioner to draw up CoPs to set out recommended standards based on the statutory requirements, covering areas such as security management, risk assessment, incident reporting, etc., to assist CI Operators in complying with the requirements of the Ordinance at the administrative level. In view of the rapid technological advancement, the Commissioner's Office will update the CoPs in a timely manner to keep up with the latest technology and international standards, and consult relevant stakeholders as appropriate to ensure that the CoPs are up to the latest standards while meeting the needs of the industry.

Monitor compliance of the Ordinance

14. The Commissioner's Office will regularly check the compliance of CI Operators with the statutory obligations stipulated in the Ordinance and assist CI Operators to enhance their protection capability through the formulation of recommended technical standards, approval of security management plans, regular drills, etc., and issue written directions to CI Operators in a timely manner to require them to rectify the non-compliance of statutory obligations when detected.

15. The process of these checks and monitoring of the rectification process by the CI Operator are critical. This would ensure that the CI Operators have a proper management structure in place to implement the necessary measures to protect their CCSs, and to promptly respond to and restore the affected system in the event of an attack on their computer systems.

Investigation and responding to threats and incidents

16. Nowadays, information on the internet sees no boundaries and the operation of CIs increasingly relies on computer systems. The Commissioner's Office must respond to any attack that interrupted CCSs promptly and timely, as any delay may have a chain effect, spreading to CI Operators in other sectors, or even affecting the whole society, seriously jeopardizing the public interest in terms of the economy, people's livelihood, and public safety, etc.

17. The Commissioner's Office will investigate the cause of incidents (including through questioning and obtaining documents from CI Operators, or applying for a warrant from a Magistrate to enter premises for investigation, etc.) in order to remedy the damage, recover the system and prevent further damage or incident. Therefore, the Commissioner leading

the Commissioner's Office must have the judgment to assess each violation and incident, provide guidance and authorize his staff to take necessary measures within a short period of time to ensure effective cooperation with the CI Operator in defending against attacks and recovering the system.

Co-ordinating with Designated Authorities under the Ordinance and Bureaux/Departments

18. To fully implement the Ordinance, the Commissioner's Office will need to work closely with the Monetary Authority, which is responsible for regulating the banking and financial services sector, and the Communications Authority, which is responsible for regulating the communications and broadcasting sector (i.e. the Designated Authorities under the Ordinance), as well as the Hong Kong Police Force, the Digital Policy Office ("DPO"), and the Office of the Privacy Commissioner for Personal Data, etc., with a view to co-ordinating the development of the CoPs for the respective sectors, the handling and investigation of cross-sectoral computer-system security incidents, etc. Therefore, the co-ordination role of the Commissioner's Office is extremely important. It needs to hold regular inter-departmental meetings and establish a notification mechanism with the relevant government departments and regulatory bodies to ensure that there is effective co-ordination among the relevant departments in enforcing the Ordinance, and that various types of cybersecurity risks can be addressed in a timely manner.

Perform other functions that are imposed on the Commissioner under the Ordinance or any other Ordinance

19. Apart from the above major functions, the Ordinance also empowers the Commissioner to investigate offences. If the Commissioner's Office finds that there is a breach of statutory obligations, such as failure to submit a notice or report, failure to implement a security management plan, contravention of the Commissioner's Office's written directions, or any other contravention of the Commissioner's power to investigate an incident etc., the Commissioner's Office is also required to investigate offences under the Ordinance and assist in the handling of related criminal prosecutions to ensure effective enforcement of the Ordinance and to maintain the deterrent effect of the Ordinance.

(ii) To create two time-limited directorate posts of DC(Com) and DC(Ops)

20. As set out above, the Ordinance regulates the infrastructure that are critical to the continued provision of essential services or the maintenance of critical social and economic activities in Hong Kong. It is important that the CCSs of these facilities function properly and effectively. The Commissioner's Office will bear the major responsibility for the implementation of this brand new piece of legislation, including handling highly sensitive information, formulating CoPs, monitoring compliance with the Ordinance, investigating and responding to security threats and incident response, etc. It is therefore necessary to have other directorate officers to support to the Commissioner in overseeing the work of the Commissioner's Office. The two proposed Deputy Commissioners will work in tandem. The DC(Com) will be responsible for setting up the regulatory framework, vetting and assessing potential CI Operators, formulating and regularly reviewing CoPs, and overseeing compliance inspections and review of reports by CI Operators to ensure compliance with the requirements of the Ordinance. The DC(Ops) will be responsible for leading response and investigation of computer-system security incidents and following up on non-compliance. The two Deputy Commissioners will support the Commissioner in both institutional oversight and implementation to ensure the effective operation of the cybersecurity protection framework for CIs during the initial implementation of the Ordinance.

21. At the initial stage of the commencement of the Ordinance, the Commissioner's Office will need to put in place a brand new mechanism to identify and assess each organization that may be designated as a CI Operator, examine the importance of its computer systems to its core functions in order to determine whether it should be designated and regulated in accordance with the Ordinance. In this regard, we consider it necessary to create two directorate posts on a time-limited basis in the first three years of the establishment of the Commissioner's Office, namely -

(a) DC(Com) (D1); and

(b) DC (Ops) (PPS 55 or D1 equivalent),

to support the Commissioner in overseeing the work of the Commissioner's Office. We will examine the feasibility of having the Commissioner or the non-directorate working staff to absorb the duties of the two time-limited posts after the Ordinance has been implemented for a period of time and is operating on track.

DC(Com)

22. The proposed DC(Com) post will mainly be responsible for assisting the Commissioner in identifying and designating CI Operators and their CCSs, formulating and reviewing from time to time the CoPs, and monitoring the compliance of CI Operators with the obligations relating to organization and prevention of threats and incidents under the Ordinance, including reviewing and assessing the notifications required to be made by the CI Operators under the relevant statutory obligations, e.g. change of office address, change of operator, change of the head of the computer-system security management unit, material change of CCSs, etc. DC(Com) will also review and assess the plans and reports submitted by CI Operators, including the computer-system security management plan, the reports of computer-system security risk assessment and computer-system security audits, etc.

23. As the operational requirements and cyber risks faced by CIs vary across sectors, to ensure that the CoPs cater for the specificities of each sector and to keep pace with technological advancement, DC(Com) will assist the Commissioner in maintaining communication with CI Operators to ensure that the Commissioner's Office has a comprehensive, accurate and up-to-date understanding of the operations of each sector. DC(Com) will also be responsible for the management of the computer systems and IT services of the Commissioner's Office (including the confidential file sharing system with CI Operators, etc.), as well as the administration of the Office.

24. The job description for this proposed post is at **Annex 4**. Given that this role requires the incumbent to possess professional knowledge and experience in cybersecurity while also playing a role of a leader, we recommend filling the post with a CSM (D1) with relevant experience in computer-system security from DPO.

DC(Ops)

25. The proposed DC(Ops) post will primarily assist the Commissioner in regulating CI Operators' compliance with incident reporting and response obligations. This includes reviewing and assessing emergency plans submitted by CI Operators, conducting regular computer-system security drills, and receiving incident reports from CI Operators. DC(Ops) will support the Commissioner in monitoring cyber threats, responding to cybersecurity incidents, recovering the attacked system, plugging the loopholes and preventing the incident from spreading. Additionally,

DC(Ops) will be responsible for external liaison, fostering close collaboration with relevant stakeholders, including the Designated Authorities, relevant government policy bureaux/departments, and professional bodies. The role also involves investigating and following up on breaches of statutory duties, assisting in the initiation of criminal prosecutions where necessary, and performing other functions assigned to the Commissioner under the Ordinance or other legislation.

26. The proposed job description for this post is at **Annex 5**. Given that the role requires the incumbent to respond to incidents swiftly, proactively investigate suspected non-compliance, and engage with senior management of predominantly large-scale enterprises, it should be taken up by an officer with enforcement and investigation experience and trained in these aspects. In this regard, we recommend filling the post with a CSP (at PPS 55 or D1-equivalent).

ALTERNATIVES CONSIDERED

27. The Commissioner's Office will need to enforce a new piece of legislation and put in place an entirely new and comprehensive system. The Ordinance covers a number of essential service sectors and other infrastructures that sustain critical social and economic activities. It involves the designation of CI Operators, which are predominantly large enterprises, the formulation of CoPs and compliance monitoring, handling of contingencies, investigation of breaches and incidents, etc. It is highly specialized as it requires a dynamic understanding of the development and trend of international computer security and cyber risk management. In addition, the implementation of the new legislation requires close cooperation with CI Operators and quick response to emerging cyber threats, which requires the full-time commitment of a dedicated team to ensure the efficiency and professionalism of the regulatory work. The SB has critically reviewed its existing manpower. At present, the directorate staff in the Bureau are mainly from the Administrative Officer and Executive Officer grades, who are responsible for the housekeeping of the disciplined and auxiliary services, handling Legislative Council business and overseeing a wide range of policy matters relating to law and order, immigration, etc. They are not equipped with technical expertise and experience in relation to computer-system security. It is not feasible for them to take up the duties of the Commissioner and the two Deputy Commissioners on top of their respective portfolios. A summary of the duties of the existing directorate staff in the SB is at **Annex 6**.

28. We have also considered creating only the post of Commissioner to head the Commissioner's Office. Taking into account the need for the Commissioner to lead, formulate policies and coordinate the Commissioner's Office in handling a large number of designated CI Operators and formulating guidelines such as CoPs during the initial implementation of the Ordinance, there is a practical need to create two Deputy Commissioner posts to share out the workload in the face of diversified demands from different infrastructures and the rapidly changing cyber threats.

29. We have also explored the possibility of having officers from the Police and the DPO to serve as the Deputy Commissioners as well. However, the existing CSP handling cybersecurity (i.e. CSP of the Cyber Security and Technology Crime Bureau) is not only responsible for cybersecurity-related matters, but also specializes in technology crime investigation, computer forensics and technology crime prevention. The relevant staff of the DPO are also responsible for overseeing and enforcing policies and measures relating to the management and security of Government IT projects. The option of having officers from the Police and the DPO to serve as Deputy Commissioners concurrently is not feasible in view of the need for a dedicated team to take up the relevant work on a full-time basis after the implementation of the Ordinance.

30. If the proposed posts were not approved, the SB will not be able to implement the Ordinance effectively.

FINANCIAL AND ESTABLISHMENT IMPLICATIONS

31. The total notional annual salary cost at mid-point salary ("NAMS") of the proposed creation of one permanent post of Commissioner (D3), one time-limited post of CSM (D1) and one time-limited post of CSP (PPS 55 or D1-equivalent) is $7,123,020. The full annual average staff cost, including salaries and staff on-cost, is estimated to be $10,058,000. The detailed breakdown is as follows—

Post	Number of Post	NAMS($)	Full annual average staff cost ($)
Commissioner	1	2,878,620	3,891,000
CSM (3-year time-limited)	1	2,088,840	3,043,000
CSP (3-year time-limited)	1	2,155,560	3,124,000
Total	**3**	**7,123,020**	**10,058,000**

32. The SB has earmarked the necessary provision in the 2025-26 Estimates and will reflect the resource requirements in the Estimates of the subsequent years concerned.

33. The Government has implemented the zero-growth policy in the civil service establishment since 2021-22 with the overall establishment controlled at a level not exceeding that as at end-March 2021. It is anticipated that by the end of the 2025-26 financial year, the civil service establishment (including the one permanent directorate post / non-civil service position and two time-limited directorate posts proposed to be created in this paper) will have reduced to about 193 000 posts.

Progress of implementing the Ordinance

34. To prepare for the formal establishment of the Commissioner's Office and the implementation of the Ordinance, the SB has, since May this year, arranged for its staff (accounting for about half of the total establishment of the Commissioner's Office) to commence various preliminary tasks, including drafting the CoP, approaching organizations that may be designated as CI Operators and conducting preliminary communication, and formulating the workflow of the Commissioner's Office.

VIEWS SOUGHT

35. Members are invited to comment on the proposal. Subject to Members' views, we will submit the proposal to the Establishment Subcommittee for consideration before seeking the approval of the Finance Committee.

Security Bureau
April 2025

Annex 1

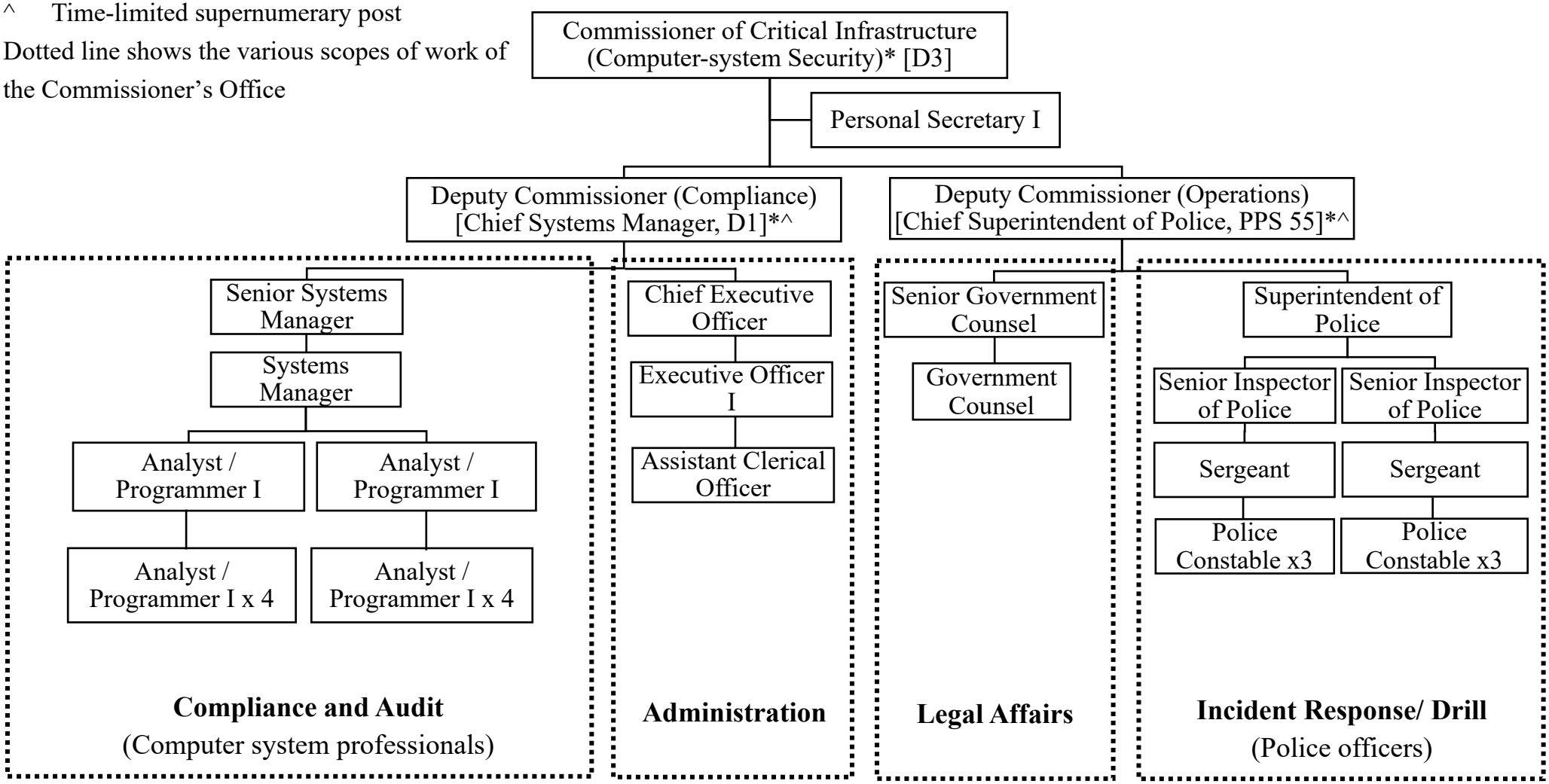
Proposed Organization Chart of the Commissioner's Office

Legend:

* Directorate Post

^ Time-limited supernumerary post

Dotted line shows the various scopes of work of the Commissioner's Office



Annex 2

Proposed Job Description of

the Commissioner of Critical Infrastructure

(Computer-system Security)

Post Title: Commissioner of Critical Infrastructure (Computer-system Security)

Rank: Commissioner of Critical Infrastructure (Computer-system Security)
(One-rank grade post at D3/ Non-civil service post at a rank equivalent to D3)

Responsible to: Permanent Secretary for Security

Main Duties and Responsibilities -

(a) to formulate an overall strategy and provide strategic advice to the Secretary for Security on the monitoring of the computer-system security of critical infrastructures ("CIs");

(b) to oversee the implementation of and compliance with the Protection of Critical Infrastructures (Computer Systems) Ordinance ("the Ordinance");

(c) to develop the mechanism and criteria for identifying CIs and designating CI Operators and critical computer systems;

(d) to spearhead the development of the Codes of Practice to provide professional guidance to CI Operators of various sectors while balancing security requirements with business operational needs;

(e) to set up a comprehensive regulatory framework, and to oversee the compliance checking mechanism of the Ordinance to ensure that the safeguards for CIs are in line with the international standards;

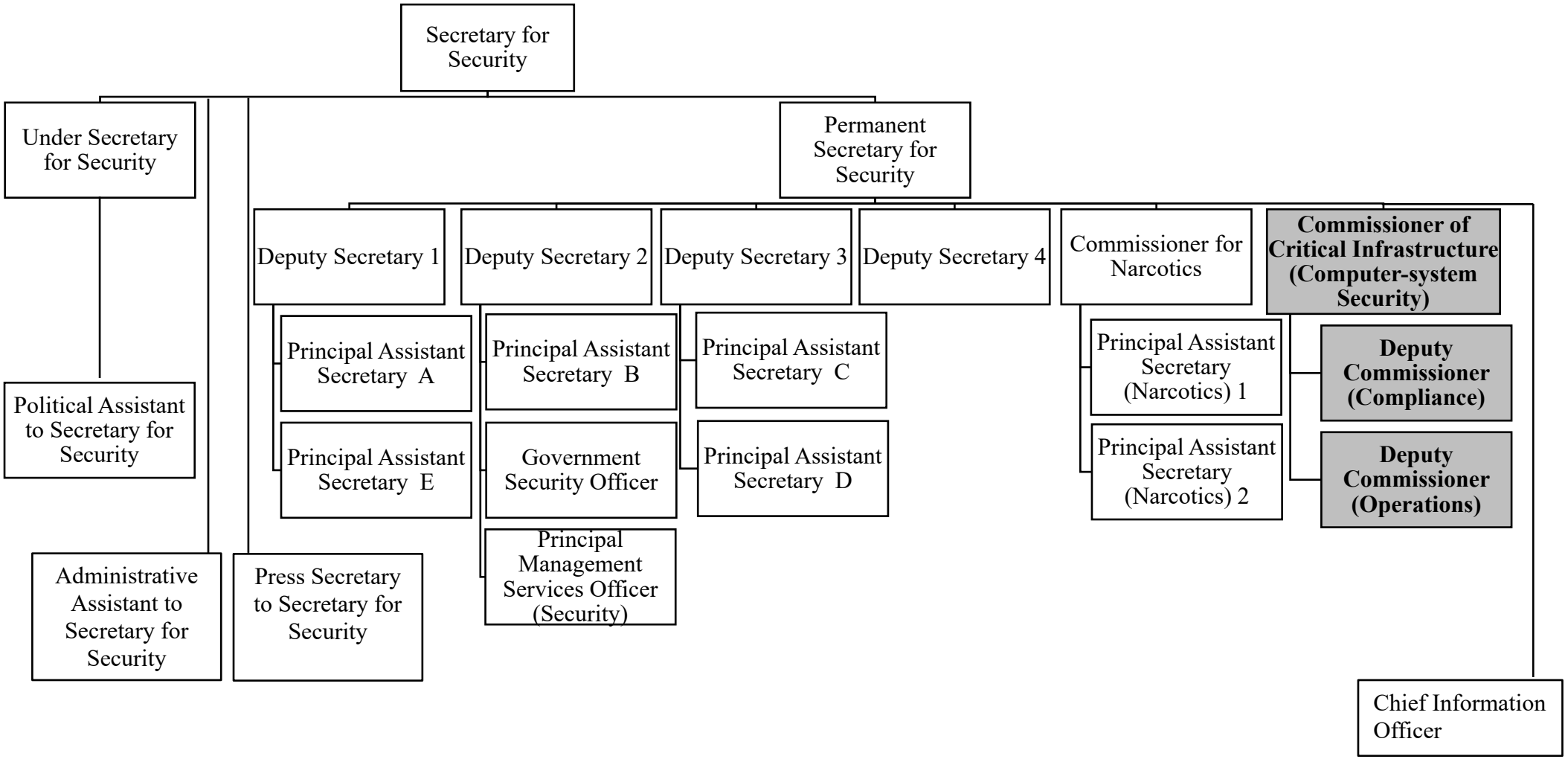
(f) to lead an inter-departmental contingency mechanism in co-ordinating investigation and response to critical computer-system security threats and incidents;

(g) to act as the key co-ordinator in facilitating co-ordination with the Designated Authorities under the Ordinance (i.e. the Hong Kong Monetary Authority and the Communications Authority) and Government bureaux/departments for the implementation of the Ordinance and promotion of policy synergy;

(h) to lead the operation of the Commissioner's Office and build up an efficient team of professional staff; and

(i) to carry out any other duties as may be assigned by the Security Bureau under the Ordinance.

Proposed Organisation Chart of the Security Bureau



Legend：

Posts proposed to be created are marked in grey.

Annex 4

Proposed Job Description of
the Deputy Commissioner of Critical Infrastructure
(Computer-system Security)(Compliance)

Post Title: Deputy Commissioner of Critical Infrastructure (Computer-system Security)(Compliance)

Rank: Chief Systems Manager (D1)

Responsible to: Commissioner of Critical Infrastructure (Computer-system Security)

Main Duties and Responsibilities –

(a) Assist in developing the mechanism and criteria for identifying critical infrastructures ("CIs") and designating CI Operators and critical computer systems;

(b) Establish a rigorous regulatory mechanism to monitor CI Operators' compliance with obligations relating to organization and prevention of threats and incidents, including reviewing and assessing notifications, plans, and reports submitted by CI Operators to ensure protective measures meet required standards;

(c) Coordinate the formulation and updating of Codes of Practice, engaging with industry stakeholders to establish appropriate computer-system security standards for CIs;

(d) Oversee the operation of the Commissioner's Office's information technology systems to ensure effective support for decision making;

(e) Manage relevant office administrative matters; and

(f) Perform any other duties assigned by the Commissioner of Critical Infrastructure (Computer-system Security) under the Ordinance.

Annex 5

Proposed Job Description of
the Deputy Commissioner of Critical Infrastructure
(Computer-system Security)(Operations)

Post Title:	Deputy Commissioner of Critical Infrastructure (Computer-system Security)(Operations)
Rank:	Chief Superintendent of Police (PPS 55/D1-equivalent)
Responsible to:	Commissioner of Critical Infrastructure (Computer-system Security)

Main Duties and Responsibilities –

(a) Regulate operators of critical infrastructure ("CI Operators")'s compliance with incident reporting and response obligations, including reviewing and assessing emergency plans submitted by CI Operators and receiving incident reports from CI Operators;

(b) Coordinate computer-system security exercises to enhance the overall protection and response capabilities of critical infrastructure;

(c) Lead investigations into CI Operators' non-compliance, leveraging professional law enforcement expertise to ensure effective enforcement;

(d) Monitor cyber threats to address computer-system security threats and incidents, integrating the latest international threat intelligence to direct immediate response measures and safeguard critical computer systems and public interests;

(e) Handle external liaison matters to foster close collaboration with relevant stakeholders;

(f) Represent Hong Kong in international cybersecurity law enforcement cooperation, establishing strategic partnerships with cybersecurity agencies in other jurisdictions to facilitate cross-border intelligence sharing; and

(g) Perform any other duties assigned by the Commissioner of Critical Infrastructure (Computer-system Security) under the Ordinance.

Annex 6

Job Descriptions of Posts and Officers of Directorate Grades in the Security Bureau

Deputy Secretary for Security 1

Deputy Secretary for Security 1 ("DS(S)1") is assisted by the Principal Assistant Secretary for Security A ("PAS(S)A") and the Principal Assistant Secretary for Security E (PAS(S)E). DS(S)1 is mainly responsible for the formulation and implementation of policies and legislation relating to internal security, public safety, public order, fight crime matters and border of Hong Kong.

- **PAS(S)A**

  As the head of A Division of the Security Bureau ("SB"), PAS(S)A assists DS(S)1 in liaising with the Chinese People's Liberation Army Hong Kong Garrison, in handling mutual legal assistance matters on criminal cases between Hong Kong and other jurisdictions, and in formulating and implementing policies relating to the border and the Frontier Closed Area. PAS(S)A is also responsible for supervising the policies, legislation and resources relating to the Government Flying Service ("GFS") and the policies and legislation relating to anti-terrorism measures. In addition, PAS(S)A assists the Security and Guarding Services Industry Authority in developing policies on the regulation of the security and guarding services industry and oversees the administration of the licensing regime, and is responsible for overseeing the operation of the police complaints system.

- **PAS(S)E**

  As the head of E Division of the SB, PAS(S)E assists DS(S)1 in formulating and implementing policies and legislation relating to internal security, public safety, public order, and in supervising the policies, legislation and resources relating to the Hong Kong Police Force and the Hong Kong Auxiliary Police Force. In addition, as the Secretary of the Fight Crime Committee, PAS(S)E is responsible for liaising and consulting with other bureaux/departments on law and order issues, and provides clerical support for the Appeal Board on Public Meetings and Processions.

Deputy Secretary for Security 2

Deputy Secretary for Security 2 ("DS(S)2") is assisted by the Principal Assistant Secretary for Security B ("PAS(S)B"), the Government Security Officer ("GSO") and the Principal Management Services Officer (Security) ("PMSO(S)"). DS(S)2 is mainly responsible for resources allocation and management in respect of the SB programme areas, and the formulation and implementation of policies relating to fire and rescue services, correctional services, aviation security and emergency response management, and government security matters.

- **PAS(S)B**

  As the head of B Division of the SB, PAS(S)B assists DS(S)2 in formulating and implementing policies and legislation and managing resources relating to the Correctional Services Department, the Fire Services Department and aviation security; and in developing and taking forward penal policies including arrangements for the transfer of sentenced persons, commutation arrangements, and matters relating to statutory bodies for sentence reviews and post-release supervision of prisoners. PAS(S)B is also responsible for supervising matters relating to correctional facilities, the regulatory frameworks of fire safety and dangerous goods, the Hong Kong Aviation Security Programme and aviation security services of the Hong Kong International Airport.

- **GSO**

  As the head of the Emergency Support Unit of the SB, GSO assists DS(S)2 in the management of government security matters, and in the formulation and implementation of contingency plans relating to natural disasters, search and rescue operations as well as other emergencies (including those occurring outside Hong Kong and involving Hong Kong residents). GSO is also responsible for emergency response management, formulation of operational strategies and planning against terrorism, and development of policies relating to Daya Bay contingency response management. In addition, GSO is responsible for supervising the policies, legislation and resources relating to the Civil Aid Service ("CAS") and the Auxiliary Medical Service ("AMS").

- **PMSO(S)**

  As the head of the Resource Management Unit, the Bureau Administration Unit, the Statistics Unit and the Information Technology Management Unit of the SB, PMSO(S) assists DS(S)2 in Bureau administration as well as the allocation and management of resources for the SB and its departments. PMSO(S) is also responsible for supporting the Statistics Unit, formulating and implementing policies on quarters for staff of disciplined services, and supervising the management of information in relation to the SB, the GFS, the CAS, the AMS and the Secretariat of the Commissioner on Interception of Communications and Surveillance.

Deputy Secretary for Security 3

Deputy Secretary for Security 3 ("DS(S)3") is assisted by the Principal Assistant Secretary for Security C ("PAS(S)C") and the Principal Assistant Secretary for Security D ("PAS(S)D"). DS(S)3 is mainly responsible for the formulation and implementation of policies relating to immigration control, stay, right of abode and nationality, and visa arrangements.

- **PAS(S)C**

  As the head of C Division of the SB, PAS(S)C assists DS(S)3 in handling right of abode and nationality matters, and in formulating and implementing policies relating to immigration control over the entry of Mainland, Taiwan and Macao residents and foreigners into Hong Kong and visa arrangements. PAS(S)C is also responsible for formulating and implementing policies/strategies relating to the combat of trafficking in persons, the processing of non-refoulement claims, and the provision of humanitarian assistance to and the detention and removal of non-refoulement claimants. In addition, PAS(S)C provides secretariat services for statutory review requests and petition cases relating to immigration matters.

- **PAS(S)D**

  As the head of D Division of the SB, PAS(S)D assists DS(S)3 in formulating and implementing policies and legislation and managing resources relating to the establishment and operation of immigration control points, and in co-operating with the Mainland on related

matters. PAS(S)D is also responsible for formulating and implementing policies/strategies relating to the registration of persons, births, deaths and marriages, the information systems of the Immigration Department ("ImmD"), the provision of publicly-funded legal assistance for non-refoulement claimants, and the handling of removal, deportation and detention cases. In addition, PAS(S)D is responsible for supervising the operation of the Torture Claims Appeal Board, housekeeping matters of the Immigration Tribunal, the Registration of Persons Tribunal, the HKSAR Passports Appeal Board and the Civil Celebrant of Marriages Appointment Appeal Board, matters relating to the Outbound Travel Alert System and assistance to Hong Kong residents in distress or detained outside Hong Kong, and the legislation and resources relating to the ImmD.

Commissioner for Narcotics

The Commissioner for Narcotics ("C for N") is the head of the Narcotics Division ("ND") and is assisted by the Principal Assistant Secretary (Narcotics) 1 ("PAS(N)1") and the Principal Assistant Secretary (Narcotics) 2 ("PAS(N)2"). The C for N is mainly responsible for formulating and implementing policies and legislation and managing resources relating to anti-drugs matters, co-ordinating and implementing anti-drugs preventive education and publicity, and supervising policies of the Customs and Excise Department (work under the purview of the SB).

- **PAS(N)1**

  As the head of Team 1 of the ND, PAS(N)1 assists C for N in co-ordinating and implementing anti-drugs preventive education and publicity, and mobilising the community to support and participate in anti-drugs efforts, and is responsible for the legislation on general anti-drugs matters. PAS(N)1 also oversees the work of the Secretariat of the Action Committee Against Narcotics and the Secretariat of the Beat Drugs Fund Association, and supervises the policies, legislation and resources of the Customs and Excise Department (work under the purview of the SB). In addition, PAS(N)1 is responsible for formulating and implementing policies

and legislating on anti-money laundering and counter-terrorist financing for designated non-financial businesses and professions.

- **PAS(N)2**
  As the head of Team 2 of the ND, PAS(N)2 assists the C for N in formulating and implementing drug treatment and rehabilitation policies, in co-ordinating services across policy bureaux/ departments/non-governmental organisations, and in formulating policies on anti-drugs prevention education (including the Healthy School Programme with a drug testing component) and their operation in schools. PAS(N)2 is also responsible for the legislation work on bringing new drugs and substances under control and the external liaison and international co-operation relating to anti-drugs matters. In addition, PAS(N)2 assists residential-based drug addiction treatment centres in meeting statutory licensing conditions, and handles other drug testing-related matters and drug-related survey/research work.

- **Administrative Assistant to Secretary for Security**
  The main duties of the Administrative Assistant to Secretary for Security is to provide administrative assistance to the Secretary for Security.