DEACONS
的近律師行

# Corporate Commercial Client Alert

## China Trade & Investment

4 January 2024

# Highlights of the Administrative Measures for Cybersecurity Incident Reporting (Comment Draft)

Edwarde Webre and Hayley Li

On December 8, 2023, the Cyberspace Administration of China (**CAC**) issued for public comment the Administrative Measures for Cybersecurity Incident Reporting (Comment Draft) (**Measures**). The Measures include two appendices. Appendix 1 is a Guide to the Classification of Cybersecurity Incidents (**Guide**); and Appendix 2 is a Cybersecurity Incident Information Reporting Form (**Form**). The period for commenting on the Measures will end on January 7, 2024.

1. **Applicable subjects**

   The Measures apply to any cyber-operator that develops and operates networks or provides services through networks within the territory of the People's Republic of China. Article 8 of the Measures further requires that any organization or individual that provides services to an operator and becomes aware of a relatively serious, serious or especially serious cybersecurity incident shall remind the operator of the obligation to report the cybersecurity incident and may report the incident if the operator refuses. Article 9 also encourages social organizations and individuals to report relatively serious, serious or especially serious cybersecurity incidents to the cyberspace administration.

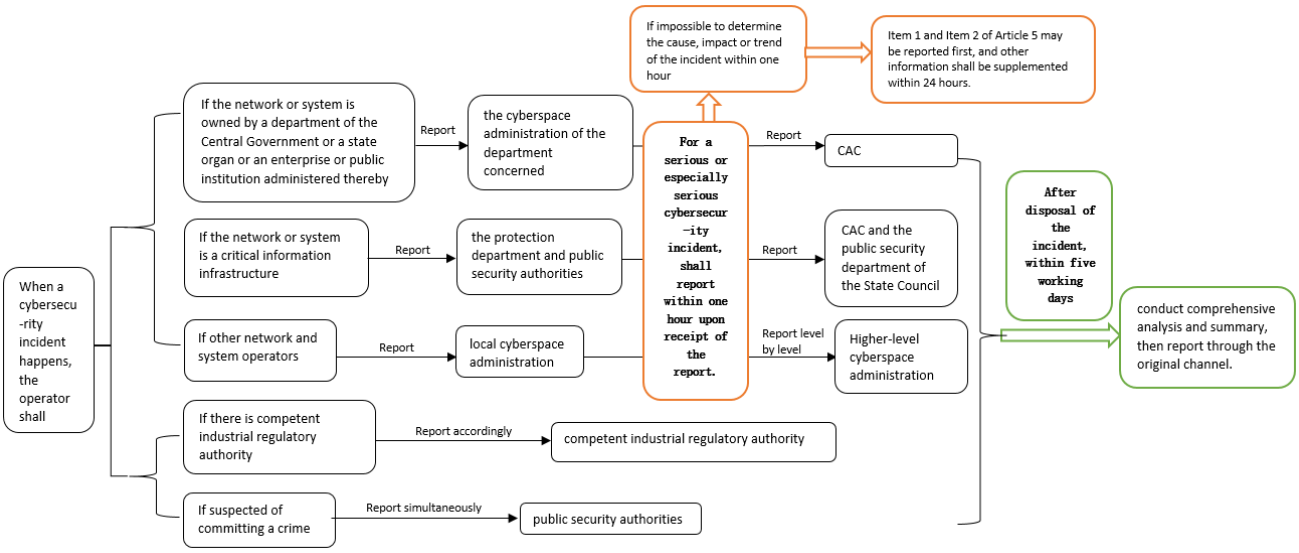
2. **Content of the report**

   According to Article 5 of the Measures and Appendix 2 the Form, the content of the report shall include at least the following items:

   1) basic information of the entity where the incident occurs;
   2) when and where the incident occurred, the type of the incident, function description of the cyberspace system, the impacts and harm caused, the measures that have been taken and their effects;
   3) brief introduction of the development of the incident;
   4) preliminary analysis of the cause of incident;
   5) items required for further investigation;
   6) further measures to be taken and working suggestions;
   7) the status of protection of the incident site, and;
   8) other circumstances that should be reported.

3. **Reporting procedures**

   Upon occurrence of a relatively serious, serious or especially serious cybersecurity incident, the operator shall make its report within one hour. The details of reporting procedures are set out in the chart below.




## 4. Legal liabilities

The Measures specify that any operators failing to report a cybersecurity incident as required shall be punished by the cyberspace administration in accordance with relevant laws and administrative regulations. Meanwhile, the Measures clarify that the operator and relevant responsible individuals shall be subject to severe punishment for delay or omission in reporting, false reporting or concealment of a cybersecurity incident. However, the liability of the operator and relevant responsible individuals may be exempted from punishment or have the level of punishment reduced if reasonable and necessary protective measures have been taken to mitigate the influence of the incident.

## 5. Conclusion

The Measures include two appendices. Appendix 1 the Guide provides guidance to the classification and categorization of cybersecurity incidents, demonstrating how to distinguish between especially serious, serious, relatively serious and general cybersecurity incidents. Appendix 2 the Form provides templates for the specific content of the cybersecurity incident report.

The Measures are still in comment draft form. Deacons will pay close attention to the status of legislation on cybersecurity incident reporting and provide updates on changes that may impact your business. Please contact us for tailored measures and practical advice regarding cybersecurity incident reporting.

## Want to know more?


Cynthia Chung
Partner
cynthia.chung@deacons.com
+852 2825 9297

Machiuanna Chu
Partner
machiuanna.chu@deacons.com
+852 2825 9630

Elsie Chan
Partner
elsie.chan@deacons.com
+852 2825 9604

Helen Liao
Partner
helen.liao@deacons.com
+852 2825 9779

Mark Stevens
Partner
mark.stevens@deacons.com
+852 2825 5192

Edwarde Webre
Consultant
edwarde.webre@deacons.com
+852 2825 9730