CAYMAN ISLANDS MONETARY AUTHORITY

PRIVATE SECTOR CONSULTATION

RULE and STATEMENT OF GUIDANCE - CYBERSECURITY

A. Introduction

1. Section 34(1)(a) of the Monetary Authority Law (2018 Revision) ("MAL") states that –

> *After private sector consultation and consultation with the Minister charged with responsibility for Financial Services, the Authority may -*
>
> *(a) issue or amend rules or statements of principle or guidance concerning the conduct of licensees and their officers and employees, and any other persons to whom and to the extent that the regulatory laws may apply;*

2. Requirements specific to the private sector consultation are outlined in section 4(1) of the MAL as follows:

> *When this Law requires private sector consultation in relation to a proposed measure –*
>
> *(a) the Authority shall give to each private sector association a draft of the proposed measure, together with –*
>
> *i. an explanation of the purpose of the proposed measure;*
> *ii. an explanation of the Authority's reasons for believing that the proposed measure is compatible with the Authority's functions and duties under section 6;*
> *iii. an explanation of the extent to which a corresponding measure has been adopted in a country or territory outside the Islands;*
> *iv. an estimate of any significant costs of the proposed measure, together with an analysis of the benefits that will arise if the proposed measure is adopted; and*
> *v. notice that representations about the proposed measure may be made to the Authority within a period specified in the notice (not being less than thirty days or such shorter period as may be permitted by subsection (3)); and*
>
> *(b) before proceeding with the proposed measure, the Authority shall have regard to any representations made by the private sector associations,*

and shall give a written response, which shall be copied to all the private sector associations.

3. The Cayman Islands Monetary Authority ("Authority" or "CIMA") seeks consultation and comments from the private sector associations concerning the following:

   a. Rule – Cybersecurity; and

   b. Statement of Guidance ("SoG") – Cybersecurity.

4. The new Rule and SoG are attached Appendices A and B, respectively.

B. Background

5. Globally, there have been increasing cyber-threats and attacks over the years leading to serious high-profile data breaches (e.g. Paradise and Panama papers). The Cayman Islands is not immune to these threats and attacks given the interconnected and cross-border nature of financial services, information technology ("IT") and cybersecurity risks. A number of international organisations (including global standard setters relating to the financial services sectors) have released cybersecurity specific information or guidance over the years.

6. The Authority issued several Supervisory Circulars in 2016 highlighting the importance of data security and advising of CIMA's approach when assessing licensees' cybersecurity frameworks. The Authority also issued an alert to Financial Service Providers advising of the Business Email Compromise Schemes[1]. Following the issuance of the first Circular, some industry stakeholders had questions seeking further details surrounding the Authority's expectations relating to cybersecurity, highlighting the need for more specific guidance.

7. Currently, CIMA has an SoG on Use of the Internet that offers some level of guidance surrounding the use of the Internet and how licensees should be addressing the issues and risks specifically posed by business conducted via the Internet. Also, several of the Authority's regulatory measures contain some elements concerning IT security related matters in connection with corporate governance, internal controls, business continuity and operational risks. That said, there is no one measure specific to cybersecurity or that captures cybersecurity in a more focused way.

8. The Authority does not wish to limit the use of technology given the benefits of innovation, competitive advantages as well as greater efficiency, effectiveness and productivity (Fintech[2]). However, the Authority is aware of the risks associated with the use of technology and the need for suitable cybersecurity frameworks to address these risks. That said, the decision to

---

[1] The FBI defines Business Email Compromise (BEC) as a sophisticated scam targeting businesses working with foreign suppliers and businesses that regularly perform wire transfer payments.

[2] Suptech refers to technologies used by supervisory agencies. (Source: https://www.bis.org/fsi/publ/insights9.pdf)

develop a Rule and SoG was made in order to establish certain legally binding obligations on regulated entities relating to cybersecurity as well as provide further non-prescriptive guidance on how they can best approach cybersecurity to ensure a robust framework is in place that is appropriate for their business and level of risk.

C. Purpose of Proposed Measure and Consistency with the Authority's Functions

9. Section 6(1) of the MAL provides that the principal responsibilities of the Authority include its regulatory functions, inter alia, "to regulate and supervise financial services business carried on in or from within the Islands …"

10. Section 6(3) of the MAL provides that in performing its regulatory functions, the Authority shall, inter alia:

    a. endeavour to promote and enhance market confidence and the reputation of the Islands as a financial centre;
    b. recognise the international character of financial services and markets and the necessity of maintaining the competitive position of the Islands, vis a vis both consumers and suppliers of financial services, while conforming to internationally applied standards insofar as they are relevant and appropriate to the circumstances of the Islands;
    c. recognise the principle that a burden or restriction which is imposed on a person or activity should be proportionate to the benefits, considered in general terms; and
    d. recognise the desirability of facilitating innovation in financial services business.

11. The proposed Rule SOG will ultimately further the regulatory function of the Authority in line with Sections 6(1) and 6(3) of the MAL, as stated above and further allow regulated entities to operate in a manner that is in the best interest of the public and their clients as is provided for in the Authority's regulatory laws via their enforcement provisions. The new regulatory measures also facilitate 6(3)(d) of the MAL as they are sufficiently flexible to allow regulated entities to consider the use new technology in a prudent way. The intention with the proposed Rule and SoG is not to create a "local standard" or to recommend one standard over another, however the Rule and SoG do consider the National Institute of Standards and Technology (NIST) standard as well as elements from some of the other recognised standards, as appropriate.

12. Simultaneously, the Authority intends to repeal the SoG on Use of the Internet as the new measures are determined to appropriately capture the significant elements of the said SoG or are captured in other currently issued measures. The proposed Rule and Guidance cover such elements as:

    - Cybersecurity framework and review of said framework
    - Risk management/strategy
    - IT systems controls and Use of Internet
    - Employee Selection, Training and Awareness

- Outsourcing arrangements
- Data protection
- Accountability (Governing Body and Senior management)
- Intra-Group arrangements
- Notification requirements (Authority and Clients)

13. A transitional period of six months has been offered to give regulated entities sufficient time to develop appropriate policies and procedures or to revise current ones in order to effectively implement the Rule and SoG.

14. Fundamentally, the new SOG will help ensure that (1) all regulated entities that fall within the proposed measures' scope have developed proportionate cybersecurity frameworks that reflect their needs, the needs of their clients and their risk tolerance as well as ensure Governing bodies are fully aware of their responsibility with respect to cybersecurity, (2) Clients of regulated entities are better protected in terms of the level of confidentiality, integrity and availability of their information, and (3) the jurisdiction's reputation as a financial centre is upheld.

D. Implementation in Other Jurisdictions

15. A review of certain jurisdictions, namely the Bahamas, Bermuda, Canada, Guernsey, Hong Kong, Jersey, Singapore, United Kingdom ("UK") was completed to consider their approach to cybersecurity, particularly in relation to the supervisory/regulatory approach of their financial services regulators. The below information should not be relied upon as a complete report of the various jurisdictions' efforts relating to cybersecurity.

16. Globally, according to the World Bank, some countries have already established national cybersecurity strategies with specific government agencies named that have responsibility for deciding minimum standards and for responding to cyber incidents. The Toronto Centre noted that "most jurisdictions address cybersecurity as a subset of broader technology risks, which in itself is a subset of operational risk" which was also observed in the research conducted by CIMA.

Bahamas

17. The Government of the Bahamas enacted the Computer Misuse Act (2003), the Data Protection Act (2003) and the Electronic Communication and Transactions Act (2006). The Royal Bahamas Police Force formulated a specific Cyber Security Unit.

18. The Securities Commission of The Bahamas' website does not appear to have issued any specific cybersecurity guidance. The Central Bank of the Bahamas has issued several guidelines relating to electronic banking, corporate governance, internal controls, business continuity, outsourcing of material functions and operational risk management. Notably, it also issued specific technology risk management ("TRM") guidelines (not legally binding). These TRM guidelines are quite extensive covering such areas as governance, expectations relating to a TRM framework, outsourcing risks, audit planning.

Bermuda

19. In 2015, the Bermuda Premier formally established a Cabinet Cybersecurity Committee under the chairmanship of the Minister of Economic Development. The Government of Bermuda issues cybersecurity advisories on such areas as ransomware and computer viruses and other current or potential threats. The Personal Information Protection Act 2016 is in effect which Bermuda deems to have equivalent effect to the General Data Protection Regulation ("GDPR") in the EU. A Bermuda Cybersecurity Strategy draft has been prepared in collaboration with the Commonwealth Telecommunications Organisation and was consulted on in 2018.

20. With respect to the Bermuda Monetary Authority ("BMA"), a "cybersecurity" legislation and Rule pertaining to digital asset business have been published. However, there does not appear to any specific legislation or measures developed or issued relating to cybersecurity across the BMA's regulated sectors. Several sector specific measures cover general risk management and corporate governance.

Canada

21. From a country standpoint, Canada has an established national cybersecurity strategy. Canada updated its consumer privacy laws similar to the General Data Protection Regulation (GDPR) in the European Union by revising its Personal Information Protection and Electronic Documents Act to focus on user consent and transparency. The Office of the Superintendent of Financial Institutions' ("OSFI") 2017-2018 annual report noted that it is "rethinking its role in the management of cyber-risk by financial institutions" given the Government of Canada's creation of its Canadian Cyber Security Centre.

22. OSFI currently has Guidelines on Operational Risk Management (2016) which include the Cyber Security Self-Assessment Guidance (2013) listed as related guidance. This Assessment Guidance encourages federally regulated financial institutions ("FRFIs") to conduct self-assessments on their current level of preparedness, and to develop and maintain effective cyber security practices using the provided template or some similar assessment tool. The self-assessment covers questions on resources, control assessment, threat and vulnerability risk management, cybersecurity incident management, policies, oversight and audits amongst others. OSFI also published its 'Technology and Cybersecurity Incident Reporting Advisory', which applies to all FRFIs starting from March 31, 2019.

23. The Canadian Securities Administrators[3] ("CSA") issued notices with respect to general expectations for market participants in respect of their cybersecurity frameworks while reminding Market Participants that they should take appropriate protective measures to safeguard themselves and their clients or stakeholders, including employee education, use of best practices, third party vulnerability and security tests and assessments and regular review of cybersecurity risk controls.

[3] CSA is comprised of Canada's 13 provincial and territorial securities regulators that are responsible for investor protection and market integrity in their respective jurisdictions

Guernsey

24. The Guernsey Financial Services Commission ("GFSC") issued cybersecurity guidance in 2016 with links to the UK's Centre for the Protection of National Infrastructure. In 2018, the GFSC set out to undertake a thematic review of cyber/information security across supervised firms. The outcomes of this thematic will form the basis for further amendment to the GFSC's existing guidance. In the meantime, the GFSC strongly supports firms considering guidance published by the UK National Cyber Security Centre ("NCSC"), including the "10 Steps to Cyber Security" (which provides guidance on why protecting information is a board-level responsibility and provides details on how organisations can protect themselves in cyberspace) and the recently released "Board toolkit: five questions for your Board's agenda". Links to these, and other recommended resources for company Boards, are provided on the GFSC's website. Lastly, cybersecurity advisories are issued on GFSC's website (https://www.gfsc.gg/news/category/warnings).

Hong Kong

25. The Government of Hong Kong has taken a very comprehensive national approach to cybersecurity and IT risks. Among other things it maintains a cybersecurity portal that provides guidelines and cyber security tool information for general users, small and medium-sized enterprises (SMEs) and schools to conduct health checks on computers, mobile devices and websites, and gives practical advice to guard against cyber-attacks. It also issues the latest technology crime alerts. In additional to the cybersecurity portal and technology crime alerts the Government provides guidance and information relating to e-commerce, information security for SMEs, security alerts and advisories, anti-spam, digital certificates, wireless security tips and the Government's IT security policy and guidelines.

26. Specific to the Hong Kong Monetary Authority ("HKMA"), the 'Cyber Fortification Initiative' program was launched in 2016. The program consists of three key pillars aiming to improve the cyber resilience of authorized institutions:

    a. Cyber Resilience Assessment Framework Professional Development Programme
    b. Professional Development Programme
    c. Cyber Intelligence Sharing Platform

27. Finally, in 2016, the HKMA also issued a Guide to Enhanced Competency Framework on Cybersecurity for banks.

Jersey

28. The Protection Authority (Jersey) Law 2018 and the Data Protection (Jersey) Law 2018 are in effect. A national Cybersecurity Strategy was published in February 2017 that has five pillars:

    a. **Pillar 1:** Government
    b. **Pillar 2:** Critical National Infrastructure
    c. **Pillar 3:** Businesses
    d. **Pillar 4:** Legislation and international engagement
    e. Pillar 5: Citizens

29. The Government's website offers information on such areas as how to stay safe online, among other things. An optional Cyber Security Information

Sharing Partnership registration process is noted on the Government's website.

30. Specific to the Jersey Financial Services Commission ("JFSC"), a cybersecurity survey was conducted in 2017 to get a better idea of how cybersecurity risks are being managed by firms and to inform future regulatory activity in this area; provide useful feedback to industry; and provide useful information to industry on the types of incidents and threats being dealt with by firms.

31. The JFSC's website provides general information on cyber-risk and how to mitigate it as well as general information regulatory obligations, how to report threats/breaches and information sharing relating to threats.

32. Registered persons in Jersey are encouraged to consider which cybersecurity related standard, or combination of standards, is most relevant to them and be aware that the standards may be updated from time to time. Warnings/alerts are issued on the JFSC's website relating to known threats. Nothing specific was noted in legislation nor does there appear to be a specific cybersecurity measure issued by the JFSC. However, a "Dear CEO" letter sent out in 2016 advising that Principle 3 of the Codes of Practice would cover such risks as cyber security risks and therefore registered persons must follow the relevant Codes.

Singapore

33. Singapore has a national cybersecurity strategy in place and the Cyber Security Agency of Singapore has worked closely with 'Sector Leads'[4] to identify the Critical Information Infrastructure (CII) supporting the provision of essential services across 11 critical sectors. The critical sectors include Banking and Finance. Services relating to banking and finance are:

- Banking services, including cash withdrawal and deposits, corporate lending, treasury management, and payment services
- Payments clearing and settlement services
- Securities trading, clearing, settlement and depository services
- Derivatives trading, clearing and settlement services
- Services relating to maintenance of monetary and financial stability
- Currency issuance
- Services relating to cash management and payments for the Government

34. The Banking and Finance sector offers guidance to help address cyber-threats and incidents. The Cybersecurity Act does not prevent Sector Leads from setting more stringent cybersecurity requirements under their sectoral regulations to cater to the cybersecurity needs of the sector. In such cases, the sectoral regulations would take precedence over the Cybersecurity Act.

35. The Singapore Computer Emergency Response Team (SingCERT) responds to cyber security incident for its Singapore constituent. It was set up to facilitate the detection, resolution and prevention of cyber security related incidents on the Internet.

[4] Government lead agencies in charge of each sector (e.g. MAS)

36. Specific to the financial services regulator, the Monetary Authority of Singapore ("MAS") launched a S$30 million Cybersecurity Capabilities Grant to strengthen the cyber resilience of the financial sector in Singapore and help financial institutions develop local talent in cybersecurity. With respect to providing guidance, the MAS issued TRM guidelines in 2013, as well as a notice on TRM. The TRM guidelines cover similar elements as those noted by the Central Bank of the Bahamas, including such areas as cybersecurity framework, Board of Directors and senior management oversight, outsourcing risks, systems reliability, availability and recoverability, access control, and IT audits among other things.

37. The MAS also issued circulars in 2015 on 'Technology Risk and Cyber Security Training for Board' and 'Early Detection of Cyber Intrusions'.

United Kingdom

38. The UK, like other jurisdictions, has also taken a country-wide approach to cybersecurity. The Department for Digital, Culture, Media & Sport (DCMS) determined that there is a need for regulation to secure personal data in the public's interest in order to protect citizens from crime and other harm. The Government aimed to achieve this through its implementation of the GDPR.

39. Specific to financial services, the Financial Conduct Authority ("FCA") issued various guidance on risk management and information relating to cybersecurity matters (e.g. ransomware). The Bank of England established the CBEST framework to test firms' cyber-resilience by CBEST accredited penetration test companies (intelligence led penetration testing). The UK financial authorities (HM Treasury, the Bank of England and the FCA) established a single mechanism to coordinate a response to incidents that have affected, or have the potential to affect, the financial sector. The incident-response mechanism also includes the National Cyber Security Centre and, when appropriate, the National Crime Agency.

E. Significant Costs and Benefits

40. The table below shows the estimated costs (including possible risks if the measures are not revised) and benefits relating to the revised measures.

Table 2 – Estimated Costs and Benefits of Proposed Measures

	Costs	Benefits
CIMA	1. The Authority will incur the usual administrative costs associated with conducting industry consultation, publication, amending CIMA's supervisory manuals and staff training. 2. These costs are not deemed to be overly burdensome and represent usual costs of the	1. Enhance and support supervisory framework and regulatory processes, in particular on-site inspections. 2. Further enhance the Authority's risk- based approach to its supervision as it will assess regulated entities' compliance with the SoG in a proportionate manner relative to their nature,

	Costs	Benefits
	Authority carrying out its mandate.	scale and complexity. The Rule excludes certain entities while noting requirements for the development of appropriate cybersecurity frameworks and accountability requirements necessary to ensure regulated entities' buy-in. 3. Provides focused guidance on cybersecurity across sectors encourages adoption of sound and suitable cybersecurity risk management frameworks by regulated entities thereby decreasing breaches and enforcement actions by CIMA. 4. CIMA's effort to fulfil its mandate of ensuring a stable financial sector and investor protection is enhanced resulting in reduced the time spent assessing breaches and corrective actions.
Cayman Islands	1. To be fully effective there could be some expenditure (not necessary for the Rule and SOG to operate) to raise awareness of consumers: ○ press releases ○ presentations ○ educational workshops 2. Notwithstanding, no significant cost to the jurisdiction as a whole with the new Rule and SoG. Without these measures, the country may be faced with reputational risk and loss of financial services business if significant breaches occur here as a result of a lack of a cybersecurity framework.	1. Raises the jurisdiction's profile as an international financial centre. 2. A more consistent approach to cybersecurity relating to the financial services industry will promote economic stability and a financial market that is less susceptible to data breaches, service disruption as well as potential fraud. 3. Increases protection for clients of regulated entities relating to data breaches, availability of information and services and the integrity of information. 4. Lessens the reputational risk relating to the use of technology and related cost to the jurisdiction thereby ensuring the jurisdiction remains an attractive domicile to clients and entities wishing to carry on business here. Helps prevent a reputational crisis such as that

	Costs	Benefits
		experienced as a result of the breaches like the Panama papers. 5. Improves results of future assessments by international standard setters.
Regulated Entities	1. Regulated entities may have to invest in upgrading their IT systems and there may be a relatively steep learning curve for some entities that do not currently consider cybersecurity as part of their risk management. 2. Relatively minor costs relating to the development of appropriate policies and procedures for those regulated entities that do not already have a framework in place or revisions to existing policies and procedures for those that do. 3. Minor training and awareness costs to ensure all staff are properly assessing, monitoring, and managing cyber-risks and threats. 4. Possible cost associated with the appointment of appropriate senior person to implement, manage and monitor cybersecurity (where applicable).	1. Reduces risks relating to cybersecurity and the use of technology including, for instance, reputational, legal and operational risks. 2. Increases certainty relating to on-site inspections and CIMA's expectations. 3. Encourages Governing body buy-in relating to cybersecurity and consequently ensures increased investment in mitigation and monitoring efforts that are appropriate to the regulated entity's risks.

F. <u>Comments and Consultation</u>

41. The Authority seeks consultation through written comments and representations from the private sector associations concerning the:-

- Rule – Cybersecurity
- Statement of Guidance – Cybersecurity

42. The Authority must receive representations by 1700hrs on **Thursday, November 28, 2019.**

43. Comments and representations must be addressed to

The Managing Director
Cayman Islands Monetary Authority
P.O. Box 10052
80e Shedden Road
Elizabethan Square
Grand Cayman KY1-1001
Cayman Islands
Tel: 345-949-7089
Fax: 345-946-5611
Email:
Consultation@cima.ky
and copied to Kourtneigh-Michelle.Nicholson@cima.ky

44. The Authority shall have due regard to any representation made by the private sector associations and industry stakeholders. The Authority shall provide a written response collating the feedback received and the Authority's position on this feedback. This response shall be copied to all relevant private sector associations only.
