NO SOALAN :16

PEMBERITAHUAN PERTANYAAN

DEWAN RAKYAT, MALAYSIA

DARIPADA	:	**Y.B. TUAN MOHD RAFIZI BIN RAMLI (PANDAN)**
PERTANYAAN	:	**LISAN**
TARIKH	:	**30.10.2014**

Y.B. TUAN MOHD RAFIZI BIN RAMLI [PANDAN] minta **MENTERI KEWANGAN** menyatakan apakah kriteria yang digunakan untuk melantik Bridge Partners Hong Kong menguruskan dana USD$2.3 bilion milik 1MDB dan bayaran tahunan yang dibayar kepada firma itu.

JAWAPAN

Tuan Yang Dipertua,

Pemilihan pengurus dana yang menguruskan dana milik 1MDB adalah dipilih berdasarkan kriteria-kriteria seperti keteguhan firma

tersebut, reputasi dan pengalaman pelaburan yang dimiliki, kawasan bidang kuasa ianya diperbadankan (*incorporated jurisdiction*), peraturan-peraturan yang wajib dipatuhi (*accompanying regulation*), pematuhan terhadap IFRS dan daya saing pasaran dengan fi yang dikenakan.

1MDB memastikan fi dan perbelanjaan adalah dinyatakan dengan betul di dalam penyata kewangan yang telah diaudit. Apa-apa maklumat lain yang telah dinyatakan di dalam penyata kewangan adalah milik persendirian (*proprietry*) syarikat.

NO SOALAN :17

PEMBERITAHUAN PERTANYAAN

DEWAN RAKYAT, MALAYSIA

DARIPADA	:	**Y.B. DATO' SERI ONG KA CHUAN (TANJONG MALIM)**
PERTANYAAN	:	**LISAN**
TARIKH	:	**30.10.2014**

Y.B. DATO' SERI ONG KA CHUAN [TANJONG MALIM] minta **MENTERI KEWANGAN** menyatakan apakah langkah yang berkesan yang telah diambil oleh Kerajaan untuk mengawal-selia institusi-institusi kewangan di negara ini terhadap ancaman siber supaya sistem kewangan dalam negara ini selamat dan terjamin.

JAWAPAN

Tuan Yang di-Pertua,

Bagi mengawal selia institusi-institusi kewangan daripada ancaman

siber, Kerajaan melalui Bank Negara Malaysia (BNM) telah menyediakan rangka kerja yang lengkap untuk mengekang masalah ini antaranya:

i. Mewujudkan fungsi pemantauan berterusan berdasarkan profil risiko institusi perbankan dan pengeluaran garis panduan / pekeliling yang perlu dipatuhi oleh institusi perbankan seperti *Circular on Preparedness Against Distributed Denial of Service Attack, Circular on Managing Inherent Risk of Internet Banking Kiosks, Circular on Prior Notification by Licensed Institutions for External System Interfaces, Guidelines on Management of IT Environment (GPIS1)* dan *Guidelines on e-Banking Services;*
ii. Menyediakan sistem peranti rangkaian keselamatan seperti *firewall* dan *Intrusion Detection and Prevention System* di setiap rangkaian ICT;
iii. Memastikan sistem operasi dan aplikasi, pelayan peranti (*hardware server*) serta peranti rangkaian adalah selamat dan bebas daripada ancaman;
iv. Memastikan sistem operasi dan peranti rangkaian ICT sentiasa dikemaskini melalui pengurusan *patch* secara berkala;

v. Menyediakan rekabentuk sistem rangkaian tiga lapis (*three-tier architecture*) dengan mengasingkan zon-zon capaian umum dan sensitif;

vi. Melaksanakan proses penyulitan (*encryption*) ke atas maklumat sensitif;

vii. Menyediakan prasarana rangkaian ICT yang berdaya tahan dengan rekabentuk dan konfigurasi yang berkesan (*no single point of failure*);

viii. Melanggan perkhidmatan pencegahan serangan *Distributed Denial of Service (DDoS);*

ix. Menjalankan ujian penembusan / pencerobohan terhadap sistem rangkaian institusi perbankan secara berkala;

x. Menyediakan sistem pemantauan (*surveillance monitoring system*) yang dapat mengesan dan menganalisis corak rangkaian trafik yang tidak normal dan mencurigakan untuk tindakan susulan;

xi. Mewujudkan rangkaian pemantauan dan risikan ancaman global *(Global Threat Intelligence*);

xii. Menubuhkan pasukan bertindak, *Cyber Emergency Response Team (CERT);* dan

xiii. Menyertai Latihan Tahunan Siber *(Cyber Drill)* yang dikendalikan oleh Majlis Keselamatan Negara.

Selain itu, BNM turut mewujudkan mekanisme kerjasama dan kolaborasi antara institusi perbankan dengan agensi serta sektor yang berkaitan seperti Penubuhan Pasukan Petugas Perbankan Internet *(Internet Banking Task Force)* yang dianggotai oleh BNM, institusi perbankan, Suruhanjaya Komunikasi dan Multimedia (SKMM), Polis Di Raja Malaysia (PDRM) dan Cybersecurity. Setakat ini, belum ada ancaman siber yang telah berjaya melumpuhkan operasi sistem rangkaian ICT institusi perbankan mahupun sistem perbankan Internet di Malaysia. Walaupun terdapat kes-kes penipuan tertentu yang melibatkan perbankan Internet, ianya adalah disebabkan kelemahan pihak pengguna yang mudah terpedaya dengan pelbagai teknik penipuan *(social engineering)* akibat daripada kesedaran yang rendah tentang amalan perbankan secara selamat.

Sebagai langkah berjaga-jaga, institusi perbankan sentiasa diingatkan supaya mempertingkatkan sistem kawalan infrastruktur ICT dan kesiapsiagaan serta kemahiran kakitangan masing-masing bagi menghadapi dan menangani ancaman siber ini.