SOALAN NO : 13

PEMBERITAHUAN PERTANYAAN LISAN DEWAN RAKYAT
MESYUARAT KEDUA, PENGGAL KEEMPAT,
PARLIMEN KEEMPAT BELAS

PERTANYAAN : LISAN

DARIPADA : DATUK SERI DR. SHAMSUL ANUAR BIN HAJI NASARAH [LENGGONG]

TARIKH : 28 OKTOBER 2021 (KHAMIS)

SOALAN:

Minta **PERDANA MENTERI** menyatakan usaha membanteras pencerobohan siber dan penjualan data peribadi melibatkan pasaran gelap (*dark web*) terutamanya melibatkan data daripada agensi Kerajaan.

SOALAN NO : 13

JAWAPAN:

DIJAWAB OLEH YB DATUK DR. ABD LATIFF BIN AHMAD
MENTERI DI JABATAN PERDANA MENTERI
(TUGAS-TUGAS KHAS)

Tuan Yang di-Pertua,

1. Kerajaan telah mengambil langkah proaktif bagi meningkatkan tahap kesiapsiagaan negara dalam menghadapi ancaman dan serangan siber melalui pembangunan dan pelaksanaan Pelan Pengurusan Krisis Siber Negara (*National Cyber Crisis Management Plan* – NCCMP) pada tahun 2008 lagi.

2. Pelan ini dibangunkan berdasarkan kepada rangka kerja pengurusan risiko menggariskan strategi bagi mengurangkan kesan serangan siber dan tindakbalas yang perlu dilaksanakan oleh agensi Infrastruktur Maklumat Kritikal Negara (*Critical National Information Infrastructure – CNII*) yang terdiri daripada agensi awam dan swasta. Pelan ini seterusnya diterjemahkan kepada Arahan Majlis Keselamatan Negara.

3. Kerajaan juga telah mewujudkan (*National Cyber Coordination and Command Centre* - NC4) yang telah beroperasi pada tahun 2016 bagi memantau dan menangani sebarang insiden dan siber termasuk pencerobohan siber dan penjualan data peribadi melibatkan agensi/organisasi CNII yang merangkumi sektor awam dan swasta.

4. Dengan komitmen tinggi Kerajaan yang telah meletakkan penggunaan teknologi digital dan ICT sebagai pemacu pembangunan negara dan sosio-ekonomi telah turut membuka ruang kepada ancaman siber yang semakin rumit dan sukar diramal. *Dark Web* meningkatkan lagi cabaran untuk menangani ancaman keselamatan siber ini. Aktiviti-aktiviti jenayah yang dahulunya berlaku secara fizikal telah beralih kepada platform *dark web* sebagai saluran penjualan dan pembayaran kerana sukar untuk dikesan.

5. Oleh itu, bagi memperkukuhkan lagi tahap keselamatan siber negara, Kerajaan melalui Agensi Keselamatan Siber Negara, Majlis Keselamatan Negara (NACSA, MKN) telah melancarkan Strategi Keselamatan Siber Malaysia (*Malaysia Cyber Security Strategy* (MCSS)) 2020-2024 pada 12 Oktober 2020 yang menggariskan tindakan strategik bagi menangani ancaman keselamatan siber termasuk pencerobohan siber melalui pendekatan bersepadu meliputi pelbagai aspek keselamatan siber secara holistik dan terselaras. Strategi ini menekankan lima (5) tonggak utama iaitu:

a) aspek tadbir urus;
b) pengurusan dan penyelarasan yang berkesan;
c) peranan agensi yang jelas;
d) peningkatan keupayaan melalui penggunaan teknologi terkini; dan
e) peningkatan kemahiran, pengetahuan dan pendidikan.

6. MCSS juga menggariskan tindakan strategik bagi memperkukuhkan keupayaan negara untuk meramal, mengesan, menghalang dan bertindakbalas kepada ancaman siber melalui pendekatan bersepadu dengan kerjasama yang efektif antara sektor awam dan swasta yang meliputi aspek pengumpulan maklumat risikan siber (*cyber intelligence*) dalam platform *dark web* ini. Melalui inisiatif komprehensif yang digariskan ini, tahap keselamatan lanskap digital negara dapat dipertingkatkan dan memastikan ia dilindungi daripada risiko ancaman siber.

Sekian, terima kasih.