SOALAN NO : 7

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

PERTANYAAN : LISAN

DARIPADA : TUAN HAJI WAN HASSAN BIN MOHD RAMLI
[DUNGUN]

TARIKH : 28 OKTOBER 2021 (KHAMIS)

SOALAN

Minta **PERDANA MENTERI** menyatakan perancangan Kementerian dalam memastikan perlindungan daripada serangan siber dari dalam dan luar serta tidak akan menggugat keselamatan infrastruktur digital negara kita pada waktu ini.

JAWAPAN

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

Tuan Yang di-Pertua,

1. Saya mohon untuk menjawab soalan ini bersekali dengan **soalan No.13 daripada YB Lenggong dalam aturan urusan mesyuarat pada hari dan No.36 daripada YB Muar pada 16 November 2021** ini kerana membawa maksud yang sama.

2. Kita sama-sama sedia maklum bahawa isu keselamatan siber merupakan isu keselamatan negara. Selain itu, keselamatan siber juga merupakan aspek yang penting bagi mewujudkan keyakinan (*trust*) kepada persekitaran ekonomi yang berlandaskan Internet dan digital. Kita

sedia maklum isu jenayah siber yang juga merupakan isu keselamatan siber telah mengakibatkan kerugian ratusan juta ringgit setiap tahun.

3. Kerajaan telah melaksanakan pelbagai inisiatif dalam memastikan perlindungan daripada memastikan perlindungan negara daripada serangan siber dari dalam dan luar serta terutamanya melindungi keselamatan infrastruktur digital negara kita melalui Pelan Pengurusan Krisis Siber Negara (*National Cyber Crisis Management Plan* – NCCMP) yang telah dibangunkan pada tahun 2008 lagi.

4. 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), dengan izin selepas ini saya akan menyebut CNII, yang terdiri daripada agensi awam dan swasta. Pelan ini seterusnya diterjemahkan kepada Arahan Majlis Keselamatan Negara No. 24 : Dasar dan Mekanisme Pengurusan Krisis Negara dan Prosedur Tindakbalas Komunikasi dan Penyelarasan Krisis Siber Negara.

5. Kerajaan juga telah mewujudkan Pusat penyelarasan dan Kawalan Siber Negara dengan izin (*National Cyber Coordination and Command Centre* - NC4), selepas ini saya akan menyebut NC4, yang telah beroperasi pada tahun 2016 bagi memantau dan menangani sebarang insiden dan ancaman siber dari dalam dan luar melibatkan agensi/organisasi CNII yang merangkumi sektor awam dan swasta.

6. Bagi memperkukuhkan lagi tahap keselamatan siber negara bagi mewujudkan persekitaran siber yang berdaya tahan dan lestari, Kerajaan melalui Agensi Keselamatan Siber Negara dengan izin (National Cyber Security Agency (NACSA)) di bawah Majlis Keselamatan Negara (MKN) telah melancarkan Strategi Keselamatan Siber Malaysia dengan izin (*Malaysia Cyber Security* Strategy) selepas ini saya akan menyebut MCSS (MCSS)) 2020-2024, pada 12 Oktober 2020 yang menggariskan tindakan strategik bagi menangani ancaman tersebut melalui pendekatan bersepadu meliputi pelbagai aspek keselamatan siber secara holistik dan terselaras. Strategi ini menekankan lima (5) tonggak utama iaitu:

i. aspek tadbir urus;
ii. pengurusan dan penyelarasan yang berkesan;
iii. peranan agensi yang jelas;
iv. peningkatan keupayaan melalui penggunaan teknologi terkini; dan
v. peningkatan kemahiran, pengetahuan dan pendidikan.

7. Dalam mempertingkatkan perlindungan daripada serangan siber dari dalam dan luar negara, pelaksanaan MCSS akan turut menumpukan kepada peningkatan keupayaan NC4 yang akan turut memperluaskan *visibility* pemantauan dengan merangkaikan kepada semua pusat pemantauan di dalam negara termasuk pusat pemantauan yang dikendalikan oleh syarikat swasta, mewujudkan *Sectoral Cyber Command Centre* (melalui sistem NC4) dan sistem pemantauan rapi terhadap sistem kritikal negara. Sistem NC4 juga akan dilengkapi dengan sistem pengurusan insiden yang lebih berkesan bagi meningkat pengurusan insiden siber melibatkan Pasukan Tindakbalas Kecemasan Komputer dengan izin (*Computer Emergency Response Team* (CERT)) diperingkat ketua sektor dan agensi CNII.

8. Melalui inisiatif komprehensif yang digariskan ini, Kerajaan dapat mengetahui situasi keselamatan siber semasa dan tahap kesiapsiagaan negara dalam memastikan ia dilindungi daripada risiko ancaman siber daripada dalam dan luar negara. Pelaksanaan MCSS juga digariskan sebagai strategi yang akan dirujuk dalam RMKe-12 2021-2025 aspek pengukuhan keselamatan siber dalam Strategi A1: Menyediakan Persekitaran Yang Menyokong Pertumbuhan Ekonomi Digital.

Sekian, terima kasih.