SOALAN NO : 15

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

PERTANYAAN : LISAN

DARIPADA : YB DATUK DR. HASAN BIN BAHROM
[TAMPIN]

TARIKH : 13 NOVEMBER 2019 (RABU)

SOALAN

Minta **PERDANA MENTERI** menyatakan adakah Kementerian telah bersiap sedia dalam menghadapi serangan siber terhadap Malaysia, kerana pada era sekarang, keganasan siber boleh memberikan kesan yang buruk kepada imej dan pembangunan negara jika kita tidak bersedia menghadapinya. Dan apakah usaha-usaha Kementerian dalam memberi keyakinan kepada rakyat dalam kesiap siagaan negara terhadap apa-apa bentuk serangan siber sekalipun.

JAWAPAN

Tuan Yang Di-Pertua,

1. Kerajaan telah mengambil langkah proaktif dan perlindungan kepada agensi-agensi Infrastruktur Maklumat Kritikal Negara (*Critical National Information Infrastructure* (CNII)) daripada ancaman dan serangan siber melalui inisiatif di bawah Dasar Keselamatan Siber Negara (*National Cyber Security Policy* (NCSP)) dan Pelan Pengurusan Krisis Siber Negara (*National Cyber Crisis Management Plan* (NCCMP)).

2. Pelan ini dibangunkan berdasarkan rangka kerja pengurusan risiko dan telah diterjemahkan ke dalam dua (2) dokumen iaitu **Arahan Majlis Keselamatan Negara (MKN) No. 24 : Dasar dan Mekanisme Pengurusan Krisis Siber Negara** dan **Prosedur Tindakbalas Komunikasi dan Penyelarasan Krisis Siber Negara**.

3. Antara program kesiapsiagaan yang dilaksanakan sejak tahun 2008 adalah Latih Amal Krisis Siber Negara (X-Maya) yang bertujuan untuk menguji dan membiasakan agensi CNII dengan mekanisme pengendalian insiden siber dan meningkatkan tahap keupayaan serta kesediaan agensi bagi menghadapi sebarang ancaman siber. Pada tahun ini, NACSA dengan kerjasama pihak International Telecommunication Union (ITU) dan Kementerian Komunikasi dan Multimedia Malaysia telah menganjurkan Latih Amal Siber di peringkat Asia Pacific dan Commonwealth of Independent States (CIS) pada 23-27 September 2019 untuk menguji tahap kemampuan pengendali-pengendali insiden keselamatan siber di rantau ini.

4. Bagi melaksanakan pemantauan tahap keselamatan siber negara, Kerajaan telah membangunkan *National Cyber Coordination and Command Centre* (NC4) yang menghubungkan agensi-agensi kritikal negara dan pusat-pusat pemantauan siber yang dikenalpasti.

5. Selain itu, Kerajaan juga telah menetapkan keperluan dan baseline keselamatan siber yang perlu kepada agensi-agensi CNII melalui pelaksanaan Pensijilan MS ISO/IEC 27001 Sistem Pengurusan Keselamatan Maklumat (*Information Security Management System* (ISMS)) untuk agensi-agensi CNII melalui keputusan Jemaah Menteri pada 24 Februari 2010. Pensijilan ini menetapkan keperluan pematuhan melalui satu pendekatan yang sistematik dalam pengurusan maklumat bagi menjamin keselamatan maklumat termasuk polisi, proses, prosedur dan fungsi perkakasan serta perisian berkaitan. Seperti juga pensijilan MS ISO yang lain, agensi-agensi CNII yang telah mendapat pensijilan tersebut perlu melalui pengauditan semula setiap dua (2) hingga (3) tahun bagi mengekalkan pensijlan tersebut.

SOALAN NO : 15

6. Kerajaan juga akan melaksanakan usaha agresif memantau dan mengambil tindakan proaktif bagi mengukuhkan infrastruktur ICT negara berdasarkan pelan tindakan Strategi Keselamatan Siber Negara (2020-2024) yang akan dilancarkan kelak.

7. Selain itu, kerajaan melalui Agensi Keselamatan Siber Negara (NACSA) telah dan sedang mengambil inisiatif meningkatkan sesi libat urus bersama rakyat untuk meningkatkan kesedaran rakyat terhadap ancaman keselamatan siber. Dalam sesi ini, NACSA berkongsi dengan masyarakat terhadap inisiatif-inisiatif yang telah dan sedang dilaksanakan oleh Kerajaan sebagai usaha untuk meningkatkan keyakinan kepada rakyat dalam kesiapsiagaan negara terhadap apa-apa bentuk serangan siber.

Sekian, terima kasih.