Isu berhubung tahap kesediaan Negara dalam menghadapi serangan Siber yang berskala besar ini secara umumnya adalah di bawah kawal selia Majlis Keselamatan Negara (MKN) melalui pelaksanaan Dasar Keselamatan Siber Negara (NCSP) dan pembangunan Pelan Pengurusan Krisis Siber Negara.

Berkenaan ancaman siber kepada sektor kewangan dan khususnya sektor perbankan pula, **Bank Negara Malaysia (BNM)** telah menubuhkan *Internet Banking Task Force* pada tahun 2004 bagi membangunkan amalan terbaik (best practices) untuk kegunaan industri perbankan dan bekerjasama dengan agensi-agensi yang berkait untuk menangani insiden keselamatan siber.

Di kesempatan ini, saya ingin menyentuh sedikit mengenai sektor informasi dan komunikasi di mana **Kementerian Sains, Teknologi dan Inovasi (MOSTI) melalui CyberSecurity Malaysia (CSM)** pula menyediakan bantuan teknikal dalam mengendalikan insiden siber. CSM juga melaksanakan program latihan kepada agensi CNII sektor awam dan swasta bagi meningkatkan kemahiran dan kecekapan dalam menangani insiden siber.

Manakala **Kementerian Komunikasi dan Multimedia Malaysia (KKMM)** melalui Pusat Keselamatan Rangkaian (SNSC) di bawah seliaan SKMM pula merupakan peneraju bagi sektor informasi dan komunikasi sentiasa menjalankan pemantuan keselamatan rangkaian negara secara berterusan bagi melindungi infrastruktur kritikal komunikasi dan maklumat negara.

SOALAN NO: 8

Sepanjang bulan Januari ke bulan September 2015, SKMM telah mengesan dan mengendalikan sejumlah 29525 kes insiden keselamatan siber.

JENIS KES INSIDEN	JUMLAH
DEFACEMENT	**2786**
PHISHING INCIDENT	**1045**
INSTRUSION INCIDENT	**29**
MALWARES DETECTION	**25665**
JUMLAH KES	**29525**

5