

**PEMBERITAHUAN PERTANYAAN DEWAN RAKYAT**

**PERTANYAAN : BUKAN LISAN**  
**DARIPADA : DATO' SRI DR. HAJI IRMOHIZAM BIN HAJI IBRAHIM**  
**[ KUALA SELANGOR – BN UMNO ]**  
**SOALAN : 207**

**Dato' Sri Dr. Haji Irmohizam bin Haji Ibrahim [Kuala Selangor] minta PERDANA MENTERI menyatakan apakah strategi paling berkesan untuk menghalang berlakunya pencerobohan asing yang menggunakan teknologi maklumat dan komunikasi (ICT) untuk mendapatkan maklumat pertahanan awam atau keselamatan negara.**

**JAWAPAN:**            **YB. DATO' SERI DR. SHAHIDAN BIN KASSIM**  
**MENTERI DI JABATAN PERDANA MENTERI**

Tuan Yang Di-Pertua,

Perkembangan teknologi maklumat dan komunikasi (ICT), internet dan teknologi mudah alih telah mempengaruhi senario ancaman keselamatan siber termasuk pencerobohan asing apabila ia menjadi semakin kompleks dan mencabar untuk ditangani. Dalam hubungan ini, Kerajaan telah mengambil langkah proaktif bagi melindungi Infrastruktur Maklumat Kritikal Negara (CNII) melalui penggubalan Dasar Keselamatan Siber Negara.

Dasar ini memfokuskan kepada penggunaan teknologi yang selamat ke arah penggunaan dan pengeluaran teknologi tempatan bagi mengurangkan kebergantungan kepada teknologi-teknologi luar. Dasar ini turut menekankan aspek pembangunan keupayaan dalam bidang keselamatan siber, penyelidikan dan pembangunan serta inisiatif-inisiatif kesiapsiagaan dalam menghadapi ancaman siber. Bagi menghadapi ancaman ini, Kerajaan akan sentiasa meningkatkan tahap keselamatan sistem komunikasi negara selari dengan perkembangan teknologi semasa. Bagi menangani isu ketirisan dan kecurian maklumat, beberapa inisiatif di bawah Dasar Keselamatan Siber Negara sedang dan akan dilaksanakan. Antara inisiatif yang dilaksanakan termasuk:

- i. Pelaksanaan Pensijilan MS ISO 27001: Sistem Pengurusan Keselamatan Maklumat (Information Security Management System) yang menetapkan satu

pendekatan yang sistematik dalam pengurusan maklumat bagi menjamin keselamatan maklumat termasuk polisi, proses, prosedur dan fungsi perkakasan dan perisian berkaitan;

- ii. Pembangunan Rangka Kerja dan Rangka Dasar Perlindungan Ketirisan Maklumat Elektronik yang menetapkan kaedah pengurusan maklumat elektronik kerajaan serta organisasi kritikal negara; dan
- iii. Penggubalan Dasar Kriptografi Negara yang menggariskan kaedah dan pendekatan strategik dalam aspek penggunaan kriptografi, penghasilan Produk Kriptografi Terpercaya (Trusted Cryptography Product) serta penyelidikan dan pembangunan bagi melindungi maklumat kerajaan dan agensi-agensi kritikal.

Sekian, terima kasih.