THE CYBERSECURITY (AMENDMENT) BILL AT-A-GLANCE:

The Government has proposed changes to the **Cybersecurity Act 2018** to ensure that our legislative framework is kept up to date. What are these key changes?

CRITICAL INFORMATION INFRASTRUCTURE (CII)

What they are:

- Critical computer systems that are necessary for the delivery of essential services in Singapore (e.g. water supply, power generation, banking services)
- Cyber incidents affecting CII can cause disruptions to our essential services, and put our national security and survival at risk

Proposed Bill will:

- **Expand the list of cyber incidents that CII owners need to report on**, such as incidents that affect computers managed by a supplier that are interconnected or communicate with the CII
- **Update the laws so that CSA can better safeguard and protect CII systems**, even as CII owners embrace new technologies and business models (e.g. the use of cloud computing and outsourcing)
- **Enable CSA to have better situational awareness** and proactively alert other CII sectors to curb the spread of similar attacks

SYSTEMS OF TEMPORARY CYBERSECURITY CONCERN (STCC)

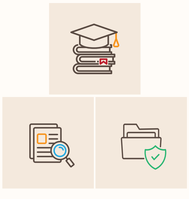
What they are:

- Systems that could be critical to Singapore and at high risk of cyberattacks for a limited period (e.g. system for vaccine distribution during a pandemic)

Proposed Bill will:

- **Impose strict cybersecurity obligations on owners of STCCs** similar to what is required of CII owners
- **Require STCC owners to report prescribed cybersecurity incidents to CSA**
- **Allow CSA to regulate STCCs when needed** as it is crucial to protect these important systems in a timely manner

ENTITIES OF SPECIAL CYBERSECURITY INTEREST (ESCI)



What they are:

- Entities that hold sensitive information or perform a function of national interest
- Cyber incidents affecting ESCI can cause significant detrimental effect on the defence, foreign relations, economy, public health, public safety, or public order of Singapore

FOUNDATIONAL DIGITAL INFRASTRUCTURE (FDI)

What they are:

- Providers of digital infrastructure services that are foundational to our economy or way of life, such as cloud service providers and data centre operators
- Disruptions arising from a cyberattack could have widespread impact on the economy and our way of life

Proposed Bill will:

- **Allow CSA to issue or approve codes of practices or standards of performance** to set a baseline level of cybersecurity for ESCI and FDI
- **Require ESCI and FDI to report prescribed cybersecurity incidents to CSA**, augmenting CSA's situational awareness of cyber incidents affecting these entities
- **Impose obligations on ESCI and FDI in a risk-based manner** as compared to CII and STCC

CSA SINGAPORE