Critical Infrastructure Laws in Australia

Dr Bruce Tonkin, Chief Operating Officer, .au Domain Administration Limited (auDA)

ccTLD News Session #2 – Thursday, 1 October 2020

.au DOMAIN ADMINISTRATION LTD

Australian Cybersecurity strategy

Vision:
A more secure online world for Australians, their business and the essential services upon which we all depend

Actions by governments	Actions by business	Actions by the community
Key Themes: • Protect critical infrastructure, essential services and households • Combat cyber crime, including on the dark web • Protect Government data and networks • Share threat information • Strengthen cyber security partnerships • Support business to meet cyber security standards • Enhance cyber security capabilities	Key Themes: • Improve baseline security for critical infrastructure • Uplift the cyber security of SMEs • Provide secure products and services • Grow a skilled workforce • Take steps to block malicious activity at scale	Key Themes: • Access and apply guidance and information on cyber security • Make informed purchasing decisions • Make informed purchasing decisions • Report Cyber crime • Access help and support when needed

Critical infrastructure definition

- Australia's Government's Critical Infrastructure Resilience Strategy currently defines critical infrastructure as:

  'those physical facilities, supply chains, information technologies and communication networks, which if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation, or affect Australia's ability to conduct national defence and ensure national security.'

  - *For further information see:* *https://cicentre.gov.au/*

.au DOMAIN ADMINISTRATION LTD

Security of Critical Infrastructure Act (2018)

- Currently covers critical assets in:

  - Electricity

  - Port

  - Water

  - Gas

  - An ability for the Government to declare an asset as critical

- 2020 discussion paper, is proposing to include:

  - Banking and finance

  - Communications

  - Data and the Cloud

  - Defence Industry

  - Education, research and innovation

  - Energy

  - Food and grocery

  - Health

  - Space

  - Transport

.au DOMAIN ADMINISTRATION LTD

Classes of critical infrastructure entities
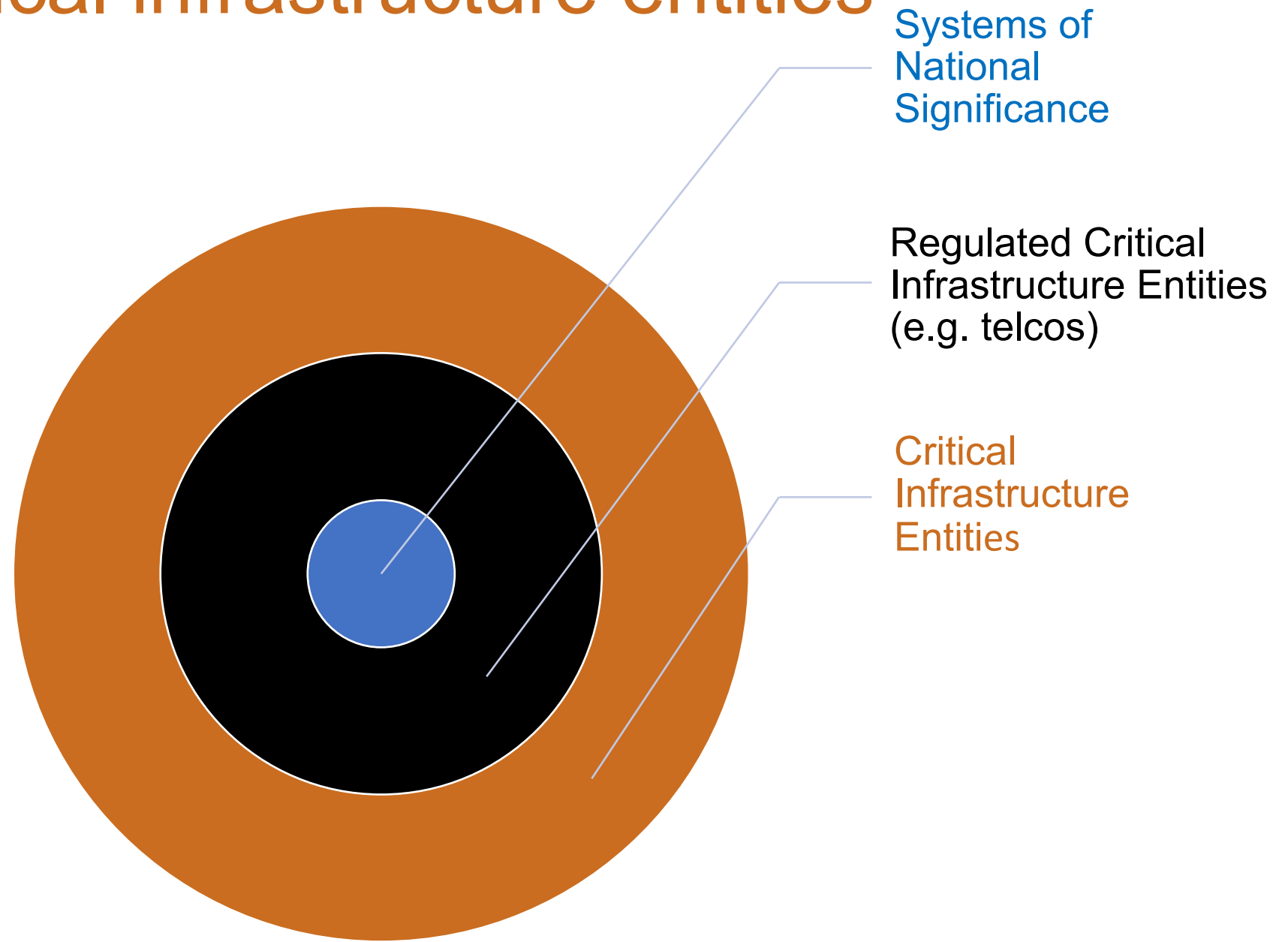
Systems of National Significance

Regulated Critical Infrastructure Entities (e.g. telcos)

Critical Infrastructure Entities

5

Systems of National Significance

In considering whether an asset is of national significance, the Government will consider:

- **Interdependency with other functions**

  - including: the potential for a domino effect if the function were compromised; and vulnerabilities within and between systems and networks.

- **The consequence of compromise to the entity**

  - including: immediate threat to life; sensitivity of data; and broader impacts on economy, security, sovereignty and the well-being of Australians.

.au DOMAIN ADMINISTRATION LTD

Positive Security Obligations

For regulated critical infrastructure entities:

Principles-based outcomes

1. Identify and understand risks ✓
2. Mitigate risks to prevent incidents ✓
3. Minimise the impact of realised incidents ✓
4. Effective Governance ✓

Security Obligations

- Physical security ✓
- Cyber security ✓
- Personnel security ✓
- Supply chain security ✓

Enhanced Cyber Security Obligations

- For Systems of National Significance

- Situational awareness ✓
- Participation in preparatory activities
    - Cyber security activities ✓
    - Playbook ✓

.au DOMAIN ADMINISTRATION LTD

Government "direct action"

Enhanced situational awareness		
In most circumstances Industry will detect and act on threats	Where there is an imminent or realised threat, Government may direct protective action and collaboration	**In a declared emergency:** Government can assist industry to protect critical infrastructure and mitigate the impact of a cyber attack
⬇ ⬇ ⬇ ⬇ ⬇ Entity takes action	Imminent/realised threat detected ⬇ Government direction ⬇ Entity takes action	⬇ ⬇ ⬇ Declared Emergency ⬇ Government takes action

Source: https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf