



Protecting Critical Infrastructure and Systems of National Significance

WebEx Town Hall

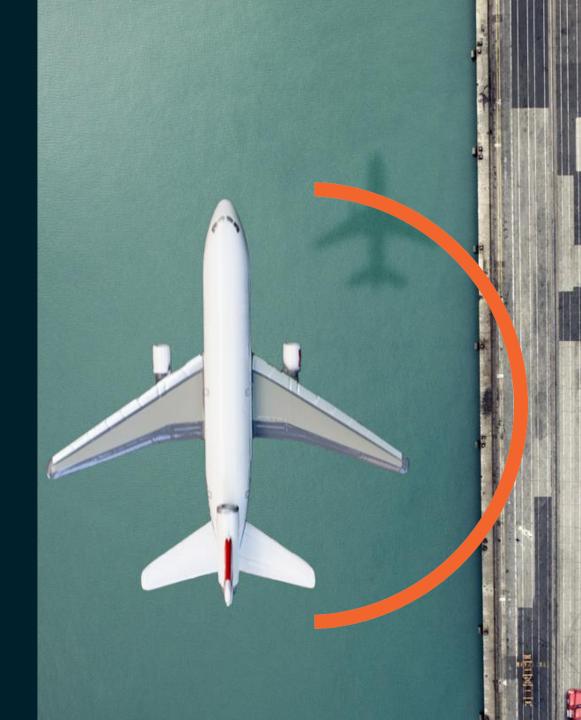






Agenda

- Scope and objectives
- Enhanced Government-Industry Partnership
- Positive Security Obligation
- Enhanced Cyber Security Obligations
- Government Assistance
- Indicative timeline

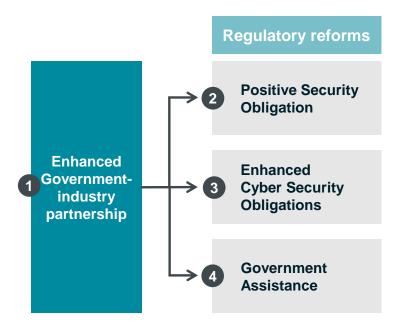


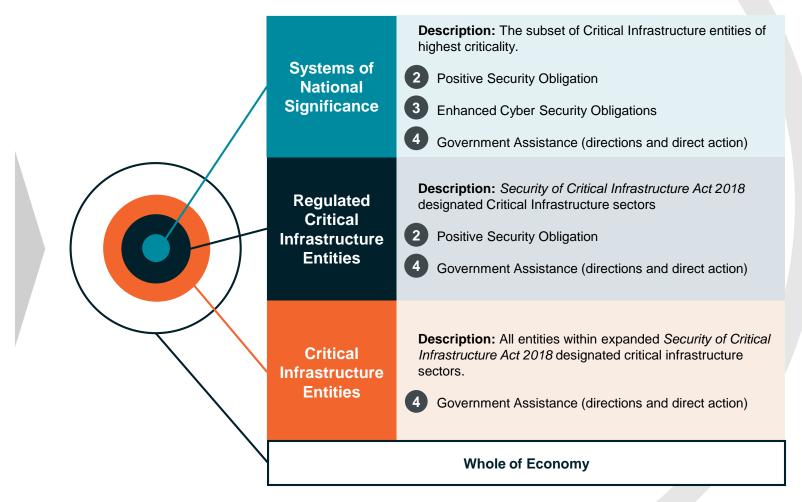




Scope and objectives

Application of initiatives









1. An enhanced voluntary Government-industry partnership will underpin the three regulatory initiatives

All critical infrastructure entities and systems of national significance

Key objectives

- Reinvigorate and expand existing engagement platforms and strategies
- Improve coordination across
 Government to provide classified threat information to entities
- Co-designing best practice guidance
- Multi-year program of workshops, exercises, info-sharing sessions & assessments

Engagement and education

- Co-design best practice guidance for regulatory risk management
- Multi-year engagement program to inform sectoral assessments
- Ensure boards of entities consider security and resilience planning

Vulnerability assessments

- Deliver vulnerability assessments, to:
 - baseline an entity's security maturity against a range of threats and hazards
 - inform risk management plans

Research analysis and evaluation

- Support critical infrastructure modelling (incl. dependencies within and cross-sectoral)
- Identify tech developments and academic insights on regulation, cybersecurity and systems management
- Program life-cycle management and evaluation

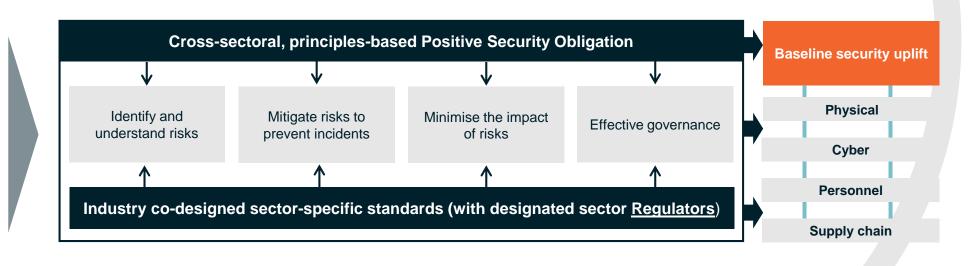




2. Positive Security Obligation to build consistent security and risk management uplift across all critical infrastructure sectors

All regulated critical infrastructure entities and systems of national significance

Set and enforce baseline protections for critical infrastructure Implement sector-specific standards Strengthen sectoral regulatory oversight



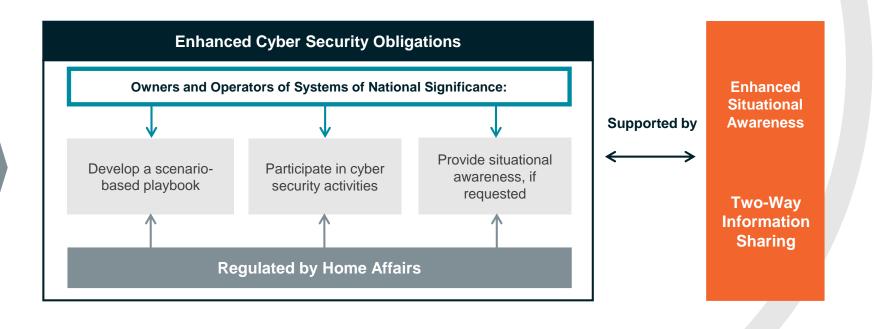




3. Enhanced Cyber Security Obligations to strengthen the resilience of designated Systems of National Significance

All systems of national significance







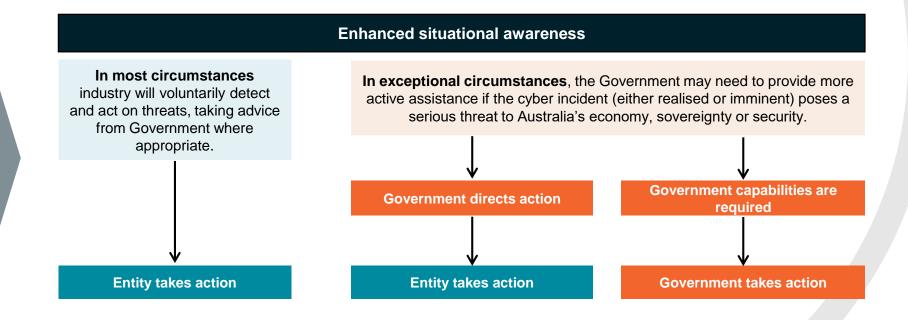


4. Government Assistance to disrupt serious cyber security threats – supported by PSO inputs and enhanced situational awareness

All critical infrastructure entities and systems of national significance

Key objective

To ensure owners and operators are able to receive timely advice and assistance to address and respond to a cyber security attack





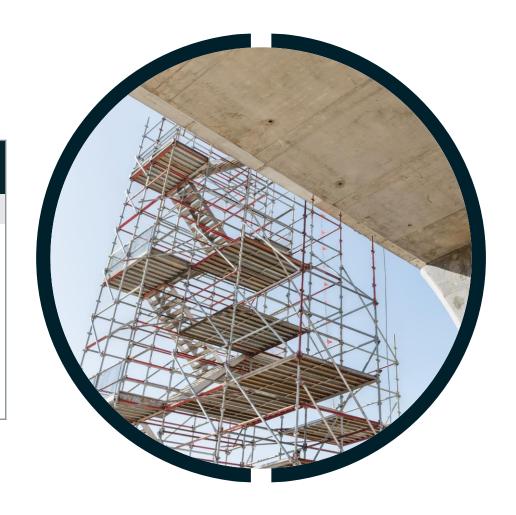


Indicative timeline for consultation

Iterative approach to develop the reforms

Dates	August – September	September – late 2020	Late 2020 - early 2021
Phase	1. Initial consultation	2. Amend legislation	3. Sector design
Activit	Consultation PaperTown HallsWorkshops	Introduce amendments to the Security of Critical Infrastructure Act 2018 to Parliament	Sector workshopsDesign of sector specific standards
Goal	Sector-specific consultation on broad reform framework	Amend Security of Critical Infrastructure Act 2018	Work with industry to design sector-specific standards

Obligations are expected to take effect mid-2021, following the sector-specific co-design.







Keep in touch

Email: ci.reforms@homeaffairs.gov.au

Submissions to the Critical Infrastructure and Systems of National Significance Consultation Paper close on 16 September 2020.

