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. Enhanced Government-industry partnership
   - Regulatory reforms
     2. Positive Security Obligation
     3. Enhanced Cyber Security Obligations
     4. Government Assistance

2. Systems of National Significance
   - Description: The subset of Critical Infrastructure entities of highest criticality.
   - Positive Security Obligation
   - Enhanced Cyber Security Obligations
   - Government Assistance (directions and direct action)

3. Regulated Critical Infrastructure Entities
   - Description: Security of Critical Infrastructure Act 2018 designated Critical Infrastructure sectors
   - Positive Security Obligation
   - Government Assistance (directions and direct action)

4. Critical Infrastructure Entities
   - Description: All entities within expanded Security of Critical Infrastructure Act 2018 designated critical infrastructure sectors.
   - Government Assistance (directions and direct action)

Whole of Economy

Protecting Critical Infrastructure and Systems of National Significance
1. An enhanced voluntary Government-industry partnership will underpin the three regulatory initiatives

All critical infrastructure entities and systems of national significance

**Key objectives**

1. Reinvigorate and expand existing engagement platforms and strategies
2. Improve coordination across Government to provide classified threat information to entities
3. Co-designing best practice guidance
4. 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

Key objectives

1. Set and enforce baseline protections for critical infrastructure
2. Implement sector-specific standards
3. Strengthen sectoral regulatory oversight
3. Enhanced Cyber Security Obligations to strengthen the resilience of designated Systems of National Significance

All systems of national significance

Key objectives

1. Co-develop scenario based ‘playbook’ setting out response arrangements
2. Build near real-time threat picture
3. Build the cyber resilience of Systems of National Significance

Enhanced Cyber Security Obligations

Owners and Operators of Systems of National Significance:

- Develop a scenario-based playbook
- Participate in cyber security activities
- Provide situational awareness, if requested

Regulated by Home Affairs

Supported by

Enhanced Situational Awareness

Two-Way Information Sharing

Protecting Critical Infrastructure and 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

---

**Enhanced situational awareness**

- **In most circumstances**, industry will voluntarily detect and act on threats, taking advice from Government where appropriate.
- **In exceptional circumstances**, the Government may need to provide more active assistance if the cyber incident (either realised or imminent) poses a serious threat to Australia’s economy, sovereignty or security.

**Entity takes action**

- **Government directs action**
- **Government capabilities are required**

**Entity takes action**

- **Government takes action**
## Indicative timeline for consultation

### Iterative approach to develop the reforms

<table>
<thead>
<tr>
<th>Dates</th>
<th>Phase</th>
<th>Activities</th>
<th>Goal</th>
</tr>
</thead>
<tbody>
<tr>
<td>August – September</td>
<td>1. Initial consultation</td>
<td>• Consultation Paper</td>
<td>Sector-specific consultation on broad reform framework</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Town Halls</td>
<td>Amend Security of Critical Infrastructure Act 2018</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Workshops</td>
<td>Act 2018 to Parliament</td>
</tr>
<tr>
<td>Late 2020 - early 2021</td>
<td>3. Sector design</td>
<td>• Sector workshops</td>
<td>Work with industry to design sector-specific standards</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Design of sector specific standards</td>
<td></td>
</tr>
</tbody>
</table>

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.
Protecting Critical Infrastructure and Systems of National Significance