Australian Government
Department of Home Affairs

CRITICAL INFRASTRUCTURE SECURITY CENTRE

Addendum to the proposed amendments to enhance the Critical Infrastructure Risk Management Program Rules (CIRMP Rules)

Physical 1: Physical security plan

The Consultation Paper on the Proposed amendments to enhance the Critical Infrastructure Risk Management Program Rules (CIRMP Rules) did not specify a measure under physical and natural hazards. In response to preliminary feedback received, the Department is proposing to introduce a requirement to develop and maintain a physical security plan as part of the enhanced CIRMP.

The issue

The threats facing critical infrastructure are increasingly diverse and complex, and traverse all-hazards. Physical threats to critical infrastructure, which could materialise as physical theft of components or operational information, vandalism, or sabotage can have significant consequences, including major disruption to essential services, increased operational costs, and serious safety risks for the offender, employees and the general public. By not including physical security uplift, resourcing for physical security may not be sufficient, resulting in increased physical security risk.

What we propose

The Department is proposing responsible entities develop and maintain a Physical Security Plan.

It is proposed the physical security plan will require the responsible entity to, as far as it is reasonably practicable to do so, develop and maintain a process or system to:

- Implement protective security measures that apply to the whole asset or organisation, and incident response plans to address breaches in such security arrangements.
- Identify the nature of the site the critical asset is located on, including ownership and tenancy, and how such arrangements could impair the availability of the asset. This could also include potential collateral exposure posed by nearby attractive targets and other critical infrastructure assets.
- Implement physical access controls, which involves managing privileged access, implementing appropriate perimeter access controls (like fences, and security barriers), and implementing and maintaining appropriate surveillance and security alarm systems, such that critical components and critical systems are subject to continuous monitoring.
    - This includes identification of physical access controls to the critical infrastructure asset, sensitive areas within the asset that hold business critical data, or areas that contain critical systems and critical components, and identification of business hours and out-of-hours access controls, such as such as CCTV, alarms, secure doors, and sensors.
- In line with existing requirements, test security arrangements for the asset are effective and appropriate to detect, delay, deter, respond to and recover from a breach in the arrangements.

The proposed physical security plan is intended to be in addition to existing requirements under the CIRMP Rules. Together, the existing CIRMP requirements and proposed enhanced arrangements would comprise the Physical Security Plan.

This approach is informed by the Protective Security Policy Framework (PSPF) Facility Security Plan principles[1]. The PSPF is an understood framework for critical infrastructure assets, and the protective security standard for Commonwealth Government entities. It is also a benchmark some industry participants have identified as the basis of their organisational physical security posture. Established physical security and resilience standards and frameworks have been considered, however, the Department considers adopting the principles of the PSPF to be a less prescriptive and cost-effective means of achieving physical security uplift.

A comparison between the PSFP facility security plan and the proposed CIRMP physical security plan can be found at the bottom of this document.

The Department is proposing compliance by 30 June 2028, which will require responsible entities to attest to compliance in the July to September 2028 reporting period. Given the extended periods for compliance, there will be a requirement to have a documented plan within the CIRMP detailing how compliance will be accomplished in attestation periods leading up to the 2028 attestation period.

Policy design questions

- Does your organisation have a physical security plan, or equivalent controls in place?
- Would a physical security plan requirement improve security posture or duplicate existing controls?
- What practical limitations do you foresee for your organisation if required to implement a physical security plan?

[1] PSPF Release 2025 pg. 132

PSPF facility security plan and proposed CIRMP physical security plan comparison

PSPF Facility Security Plan principles:		CIRMP Physical Security Plan to include:
Location and nature of the site	✓	Assess the nature of the site the critical asset is located on, and the material risks that could arise – which could include FOCI risks, unauthorised access, or how such arrangements could impair the availability of the asset. This includes an assessment of potential collateral exposure posed by nearby attractive targets, other critical infrastructure assets, and other tenants in multi-tenant locations.
Ownership or tenancy of the site (sole or shared, including multiple entities sharing the same space)	✓	
Collateral exposure, such as the presence nearby of other 'attractive targets'	✓	
Other resources that will be on the site	✓	
Access to the site for authorised personnel and the public (if necessary) and preventing access as required	✓	Access control requirements, which involves managing privileged access to the asset and sensitive internal areas, implementing appropriate perimeter access controls (like fences, and security barriers), and implementing and maintaining appropriate surveillance and security alarm systems, such that critical components and critical systems are subject to continuous monitoring.
Protective security measures required for: • the site as a whole	✓	Implementing protective security measures that apply to the whole asset or CI organisation.
• particular areas within the site (e.g. a floor or part of a floor that will hold information of a higher classification than the rest of the site)	✓	Consideration of physical access controls to the CI asset, sensitive areas within the asset that hold business critical data, or areas that contain critical systems and critical components. This includes identification of business hours and out-of-hours access controls, such as CCTV, alarms, secure doors, and sensors.
• storage, handling and processing of security classified information	✓	
• business hours and out-of-hours, as they are likely to be different	✓	
• security classified and other security classified discussions and meetings	×	
• security classification of information and resources, including technology assets and related equipment, to be stored, handled or processed in each part of the site, this includes considering the need to hold security classified discussions and meetings	×	*Security classification of information and resources is not a requirement for industry, noting that Commonwealth security classified information used, stored or processed by a CI organisation must be done so in accordance with the PSPF requirements.*
N/A	✓	The responsible entity will need to consider the interaction between their physical security plan and other organisational security plans, as well as organisational incident response plans, for all-hazards. Including testing security arrangements and whether security arrangements for the asset are effective and appropriate to detect, delay, deter, respond to and recover from a breach in the arrangements.