Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Cyber Incident Response: Government Assistance Measures

The *Security of Critical Infrastructure Act 2018* provides the Government with the ability to provide government assistance to critical infrastructure entities in response to serious cyber-attacks on Australian systems.

What is Government Assistance?

The objective of this framework is to assist in the defence of critical infrastructure assets from cyber security threats, in light of their criticality to the social or economic stability of Australia or its people, the defence of Australia, or national security. That is to say, this is not intended to be a regime that can be used to defend all assets economy-wide.

The Government Assistance framework provides the Minister for Home Affairs with the ability to authorise the Secretary of the Department of Home Affairs to do any or all of the following things in response to a cyber security incident:

- Gather information to determine if another power in the *Security of Critical Infrastructure Act* 2018 should be exercised.
- Direct an entity to do, or refrain from doing, a specified act or thing.
- Request an authorised agency (i.e. the Australian Signals Directorate's Australian Cyber Security Centre (ACSC)) to provide support (with agreement from the Prime Minister and Minister for Defence)

The Secretary will only be authorised by the Minister for Home Affairs to use the powers in rare or emergency circumstances when an entity is unwilling or unable to conduct their own incident response, and when there is no other regulatory mechanism in place to resolve the incident.

Why do we need Government Assistance powers?

A cyber security incident may come with warning, or suddenly, and be rapid or prolonged, but nevertheless catastrophic in its impact. Even after the compromise has been addressed, significant work may be required to restore the functioning of the asset to enable it to recommence providing essential services. The ACSC has particular expertise in responding to cyber threats that may not be available in the private sector and already provides these services to critical infrastructure organisations voluntarily

When will Government Assistance be provided?

The framework will not be used unless a cyber security incident on a critical infrastructure asset can reasonably be considered capable of causing significant damage or harm to Australian interests.

The Minister for Home Affairs will only authorise the Secretary to undertake the above actions where he or she **is satisfied of all of the following**:

1. A **cyber security incident has occurred, is occurring or imminent.**
2. The **incident has had, is having or is likely to have a relevant impact** to the availability, integrity or reliability of a critical infrastructure asset, or on the confidentiality of information held by the asset, known as the primary asset. A relevant impact may occur directly or indirectly. This reflects that a cyber security incident can significantly impede or compromise the functioning of a critical infrastructure asset by targeting a crucial dependency in its supply chain rendering the primary asset inoperable.
3. There is **a material risk** that the incident has seriously prejudiced, is seriously prejudicing or is likely to seriously **prejudice Australia's social or economic stability, defence or national security**. This assessment is likely to rely on intelligence about the potential cascading impact of the incident.

Cyber Incident Response: Government Assistance Measures

4. **No existing regulatory system of the Commonwealth, a State or a Territory could be used to provide a** practical and effective **response** to the incident. This ensures that, wherever possible and appropriate, consideration is given to whether existing regimes, which are potentially less invasive or which are designed specifically to address risks associated with particular assets, could be relied upon to effectively respond to the incident.

How long will a Ministerial authorisation last?

A Ministerial authorisation to exercise government assistance powers will remain in force for the period specified in the authorisation but cannot exceed 20 days.

Consultation

The Minister for Home Affairs must consult the specific entity that is the subject of the authorisation prior to any authorisation being made. The Minister for Home Affairs must also consult the responsible entity, or the owner or operator of a critical infrastructure sector asset, prior to issuing an authorisation to enable an intervention request.

To facilitate consultation you will receive a copy of the draft Ministerial authorisation and be invited to make a submission to the Minister about the authorisation within 24 hours of receipt. In rare circumstances consultation will not occur, if the delay caused by the consultation would frustrate the effectiveness of the Ministerial authorisation.

Types of Government Assistance

Government's continued view is that industry are primarily responsible for responding to cyber security incidents that impact privately owned assets and that Government intervention is only to be used in emergencies and as a last resort when industry will not or are unable to resolve the incident. The Cyber and Infrastructure Security Centre (CISC) considers these instances will be few and far between, and will continue to collaborate with industry on a voluntary basis in response to incidents.

A direction may be given verbally or in writ ing. If a direction is given to an entity verbally, the entity will receive a written record of the direction within 48 hours of the direction being given.

a) Information Gathering Directions

An effective and appropriate response to a serious cyber security incident requires a strong understanding of the nature and extent of the incident, as well as a strong understanding of the circumstances of the asset including its cyber maturity, its vulnerabilities and its interdependencies.

An Information Gathering Direction will ensure that the Government has access to necessary information to determine the full extent of a compromise and develop an appropriate response. An Information Gathering Direction will specify what information is required and the time period in which the information must be provided.

b) Action Directions

Where an entity is unable or unwilling to respond to a cyber security incident, this authorisation may be used to compel an entity to take actions, or refrain from taking actions, where this is reasonably necessary and proportionate to responding to the incident.

The focus of these directions is on defending the asset, which may include removing a perpetrator from the asset, but do not extend into actions that would be regarded as offensive. For example, an Action Direction cannot be used as a 'backdoor' to compel an entity to permit Government officials access to the asset. An Action Direction must also be technically feasible. A direction is technically feasible when the direction relates to a course of action that is reasonably possible to execute, or within the existing capability of the relevant entity.

Cyber Incident Response: Government Assistance Measures

c) Intervention Requests

Where directing an entity to take specified action would not be practical or effective, it may be necessary for the Government to take necessary actions to help defend the asset. This is a last resort option, within a last resort regime, and will only be used in extraordinary circumstances—including with the agreement of the Prime Minister and Minister for Defence.

However it must be recognised that in emergencies where Australia's national interests are at risk of serious prejudice and industry is unable to respond, the Government may have unique expertise that could be deployed to prevent an incident, mitigate its impact, or restore the functioning of an asset following an incident.

In some circumstances, the cyber capabilities and technical resources of the Australian Signals Directorate's ACSC will surpass those of industry. Where those circumstances exist, it is reasonable, appropriate and expected that the Government has the powers to respond.

An intervention request may include but is not limited to a direction to access or modify a computer that is part of the asset, remove or disconnect a computer from a network that is part of the asset, or access, copy, alter or delete a computer program that is installed on a computer that is, or is part of, the asset to which the Ministerial authorisation relates.

How can I be reassured the Government Assistance measures are being used appropriately?

The Government has included a suite of safeguards to ensure that these measures are used appropriately, with rigorous oversight measures:

- The powers can only be exercised as a **matter of last resort** and only where no existing regulatory mechanism can be used to address the serious cyber security incident;
- There must be **consultation** with the entity in advance of using the powers, except where consultation will frustrate the effectiveness of directions or requests;
- The intervention power can only be authorised once the Minister for Home Affairs has obtained agreement from the **Prime Minister** and the **Minister for Defence;**
- There is a **mandatory notification requirement** to the Parliamentary Joint Committee on Intelligence and Security to hold Government to account in taking these actions. This is in addition to **the annual reporting to Parliament** on the use of these powers, to ensure transparency and accountability to Parliament and the Australian public;
- The Inspector-General of Intelligence and Security (IGIS) has oversight of intelligence agencies' functions; and
- The Commonwealth Ombudsman can investigate complaints made about the actions of government agencies (excluding intelligence agencies) in the exercise of these measures.