Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

The Enhanced Cyber Security Obligations Framework

On 2 April 2022, the *Security of Critical Infrastructure Act 2018* was amended, introducing a new enhanced cyber security obligations framework for systems of national significance —Australia's most important critical infrastructure assets.

Declaring a System of National Significance

Systems of national significance (SoNS) are a significantly smaller subset of critical infrastructure assets that are most crucial to the nation by virtue of their interdependencies across sectors and potential for cascading consequences to other critical infrastructure assets and sectors if disrupted.

Part 6A of the *Security of Critical Infrastructure Act 2018* (SOCI Act), enables the Minister for Home Affairs (the Minister) to privately declare a critical infrastructure asset to be a system of national significance.

The Minister may only declare an asset as a SoNS if the asset is a critical infrastructure asset and the Minister is satisfied that the asset is of national significance. In determining this, the Minister must have regard to a number of factors, including:

- the nature and extent of the asset's interdependencies with other critical infrastructure assets; and
- the consequences that would arise for Australia's social or economic stability, defence, or national security if a hazard were to occur that had a significant relevant impact on the asset.

Before declaring a critical infrastructure asset as a SoNS, the Minister must give the responsible entity a notice that sets out the proposed declaration, the reasons for the proposed declaration, and invites the entity to make submissions regarding the proposed declaration within 28 days, or a shorter period specified in the notice. The Minister must consider any submissions received within the 28 day timeframes.

Should the Minister proceed with the declaration, the Minister must notify each responsible entity for the asset of the declaration, in writing, within 30 days after making the declaration. Within this timeframe, the Minister must also notify the Parliamentary Joint Committee on Intelligence and Security and First Ministers if the asset is located wholly or partly in their state or territory.

A responsible entity may request the Secretary to review whether the asset is of national significance.

SoNS will continue to be subject to all the obligations that applied to that critical infrastructure asset under the SOCI Act before it was declared a SoNS.

In addition to these obligations, entities responsible for assets designated as SoNS may be subject to Enhanced Cyber Security Obligations (ECSO), outlined in Part 2C of the SOCI Act. Each obligation is separate and is individually applied to an asset. Being declared a SONS does not mean that all ECSO will automatically apply to the asset.

CONTACT US | 1300 27 25 24 | enquiries@CISC.gov.au | CISC.gov.au | CISC on Twitter | LinkedIn | Instagram

April 2025

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Enhanced Cyber Security Obligations

The ECSO that the Secretary may apply to a SoNS will vary between each SoNS, depending on the specific role and function of that asset. The obligations include:

- **developing cyber security incident response plans** to prepare for a cyber security incident;
- **undertaking cyber security exercises** to build cyber preparedness;
- **undertaking vulnerability assessments** to identify vulnerabilities for remediation; and/or
- **providing system information** to develop and maintain a near-real time threat picture.

ECSO can be considered upon the circumstances for the sector and/or similar assets, which recognises that different sectors have different networks and systems, and could face different risks.

When making a decision to impose ECSO on a responsible entity, the Secretary of the Department of Home Affairs (the Secretary) must consider a number of factors before making the decision, including:

- the likely **cost** to the affected entity of complying with the obligations;
- the **reasonableness and proportionality** of the decision; and
- **any other matter the Secretary considers relevant**. For example, this may include: any international trade obligations that apply; whether the entity is, or has been, subject to any other enhanced cyber security obligation; and whether the entity is subject to another regulatory regime under Commonwealth, state or territory law that is similar.

Cyber Security Incident Response Plans

An incident response plan is a written plan detailing how an entity will respond to cyber security incidents that affect its systems. This obligation will assist entities to articulate 'what to do' and 'who to call' in the event of a cyber incident.

The Secretary may give written notice to a responsible entity of a SoNS that the statutory incident response planning obligations apply to the entity in relation to the system and cyber security incidents. These obligations require the entity to adopt, maintain and comply with an 'incident response plan'. The entity must also review the plan on a regular basis.

Before giving a notice, the Secretary must:

- consider the cost, reasonableness and proportionality and any other matter the Secretary considers relevant, and
- consult the entity and any relevant Commonwealth regulator that has functions relating the security of that system (the Commonwealth regulator).

If the Secretary does decide to issue a notice, the notice will specify when the obligation comes into effect. The SOCI Act ensures that responsible entities will have a minimum 30-day notice period to make arrangements to meet this obligation.

The responsible entity must provide the Secretary with a copy of the incident response plan as soon as practicable after adoption. This applies to any varied incident response plans while the obligation applies.

The incident response plan is limited to cyber security incidents and is not intended to address hazards more generally. Best practice incident response plans do not apply to specific cyber security incidents (although components of them may focus on specific types), but rather apply to cyber security incidents generally. This ensures procedures are in place to address the various methodologies that may be adopted in a cyber-attack.

The Enhanced Cyber Security Obligations Framework

Further, there is no prescribed template or form for an incident response plan. Responsible entities are best placed to construct the plan, taking into account a variety of factors, including: the services provided by the asset, the extent and nature of interdependencies, and the threat environment. This approach also acknowledges that many entities will already have incident response plans in place.

Responsible entities of SoNS are required to comply with and regularly review the plan, and take all reasonable steps to ensure the plan is up to date.

Cyber Security Exercises

Cyber security exercises test preparedness, mitigation and response capabilities. Ultimately, an exercise is designed to reveal whether the existing resources, processes and capabilities of an entity sufficiently safeguard the system from being impacted by a cyber security incident.

There is no prescribed form for a cyber security exercise. For example, exercises may be discussion or tabletop-based, or operational or functional. The exercise can also test different capabilities—such as internal response capability, responsibilities for key staff, and/or coordination mechanisms. The Cyber and Infrastructure Security Centre, as the regulator, will work with entities to determine what the best exercise format may be in relation to the threat environment and the individual characteristics of the asset.

The Secretary may give notice requiring a responsible entity of a SoNS to undertake cyber security exercises within a period specified in the notice to test:

- general preparedness, mitigation and response capabilities by undertaking a cyber security exercise in relation to the system and all types of cyber security incidents, or
- responsiveness, preparedness and mitigation capabilities in relation to a particular threat scenario by undertaking a cyber security exercise in relation to the system and one or more specified types of cyber security incidents.

A notice may also require the responsible entity to do any or all of the following things:

- allow one or more specified designated officers (an employee/s of the Department of Home Affairs or a staff member of the Australian Signals Directorate appointed by the Secretary to be a designated officer) to observe the cyber security exercise,
- provide those designated officers with access to premises for the purposes of observing the cyber security exercise,
- provide those designated officers with reasonable assistance and facilities that are reasonably necessary to allow those designated officers to observe the cyber security exercise,
- allow those designated officers to make such records as are reasonably necessary for the purposes of monitoring compliance with the notice,
- give those designated officers reasonable notice of the time when the cyber security exercise will begin.

Before giving a notice, the Secretary must:

- consider the cost, reasonableness and proportionality and any other matter the Secretary considers relevant, and
- consult the entity and any relevant Commonwealth regulator that has functions relating the security of that system (the Commonwealth regulator).

If the Secretary does decide to issue a notice, the responsible entity must complete the cyber security exercise within the period specified in the Secretary's notice. At a

The Enhanced Cyber Security Obligations Framework

minimum, the responsible entity will have 30 days from when the notice is given.

Following the exercise, the responsible entity that has undertaken and completed the cyber security exercise must prepare an evaluation report and give a copy to the Secretary within 30 days after the completion of the exercise (unless the Secretary has allowed a longer period for the provision of the report).

The meaning of an evaluation report is outlined at section 30CS of the SOCI Act. In short, the evaluation report is a written report that should evaluate the responsible entity's:

- **ability to respond appropriately** to an incident/s that could have a relevant impact on the system,
- **preparedness to respond appropriately** to an incident/s that could have a relevant impact on the system, and
- **ability to mitigate the relevant impacts** that the incident/s could have on the system.

The evaluation report also needs to comply with requirements specified in the rules (if any).

In some circumstances, the Secretary may require the responsible entity to appoint an external auditor and arrange for an evaluation report to be prepared by the external auditor. The entity must then give the Secretary a copy of the new evaluation report. An individual is not eligible to be appointed as an external auditor if they are an officer, employee or agent of the entity. The Secretary may authorise a specified individual to be an external auditor for this purpose.

Vulnerability Assessments

Vulnerability assessments identify 'gaps' in systems that expose entities to particular types of cyber incidents. These assessments will help entities identify where further resources and capabilities are required to improve an entity's preparedness for, and resilience to, cyber incidents. A vulnerability assessment also assists Government to understand whether cyber security advice or assistance can be provided to strengthen the security or resilience of SoNS, and identify patterns of weakness across sectors and assets which could be exploited by malicious actors.

There is no prescribed form for a vulnerability assessment. However, examples include: a documentation-based review of a system's design, a hands-on assessment, or automated scanning with software tools.

The Secretary may give notice requiring a responsible entity of a SoNS to undertake a vulnerability assessment within a period specified in the notice in relation to:

- the system and all types of cyber security incidents—involving a broad spectrum assessment for vulnerabilities to all types of cyber security incidents; or
- the system and one or more specified types of cyber security incidents—for a more targeted assessment (for example, where credible intelligence exists).

Before giving a notice, the Secretary must:

- consider the cost, reasonableness and proportionality and any other matter the Secretary considers relevant; and
- consult the entity and any relevant Commonwealth regulator that has functions relating to the security of that system (the Commonwealth regulator).

If the Secretary does decide to issue a notice, the responsible entity must comply within the period specified in the Secretary's notice.

If the responsible entity is incapable or unwilling to undertake the assessment, the Secretary may give a designated officer a written request to undertake a vulnerability assessment. A designated officer is an employee of the Department of Home Affairs or a staff member of the Australian Signals Directorate who is appointed by the Secretary. In this case, the Secretary may give written notice to the entity requiring them to provide the designated officer with:

The Enhanced Cyber Security Obligations Framework

- access to the premises for the purposes of undertaking the vulnerability assessment,
- access to computers for the purposes of undertaking the vulnerability assessment,
- reasonable assistance and facilities that are reasonably necessary to allow the designated officer to undertake the vulnerability assessment. Once the vulnerability assessment is completed, the responsible entity (or designated officer) must prepare a vulnerability assessment report and give a copy to the Secretary within 30 days after completion of the assessment (unless the Secretary has allowed a longer period for the provision of the report).

The meaning of a vulnerability assessment report is outlined at section 30DA of the SOCI Act. In short, the vulnerability assessment report is a written report that:

- assesses the vulnerability of the system of national significance to all types of cyber security incidents or specified cyber security incidents, and
- complies with requirements (if any) specified in the rules.

The Government may use a report to work with the responsible entity to identify and implement proportionate measures to addresses any weaknesses contained in the report.

System Information

System information is data generated about a system for the purposes of security, diagnostic monitoring or audit—such as network logs, system telemetry and event logs, alerts, netflow and other aggregate or metadata that provide visibility of malicious activity occurring within the normal functioning of a computer network. This does not include personal information.

Systems information helps to build a near-real time threat picture, allowing the Government to share actionable, and anonymised information back out to not just the entity itself, but to industry more broadly. As a result, this anonymised information will assist all entities to improve their cyber resilience.

There are three types of system information notices that the Secretary may give to a responsible entity for a SoNS: a ‘system information periodic reporting notice’, a ‘system information event-based reporting notice’ and a ‘system information software notice’. The first two notices request information, as the last notice requests an action.

Before giving any notice, the Secretary must:

- consider the cost, reasonableness and proportionality and any other matter the Secretary considers relevant; and
- consult the responsible entity and the relevant entity for the SoNS (if the relevant entity is not the responsible entity).

System information notices

The Secretary may give a notice requiring a responsible entity of a SoNS to provide systems information. This notice can be:

- periodic reporting of system information (known as a ‘system information periodic reporting notice’), or
- in response to a specific event (known as a ‘system information event-based reporting notice’).

A system information notice can only be given if:

- a computer is needed to operate the SoNS or is a SoNS itself, and
- the Secretary believes on reasonable grounds that a relevant entity of the SoNS is technically capable of

The Enhanced Cyber Security Obligations Framework

preparing periodic reports consisting of information that relates to the operation of the computer; may assist with determining whether a power under the SOCI Act should be exercised in relation to the SoNS; and is not personal information (within the meaning of the *Privacy Act 1988*).

A **system information periodic reporting notice** can require a relevant entity to prepare periodic reports, and give each of those periodic reports to the Australian Signals Directorate within a period outlined in the notice, at particular intervals or times.

A **system information event-based reporting notice** can require a relevant entity to prepare a report each time a certain event/s occur. The report must be given to the Australian Signals Directorate as soon as practicable after the event occurs.

These types of notices can specify the information required, the manner and form of the report, and that the report be prepared in accordance with the information technology requirements specified in the notice.

If the Secretary decides to issue a systems information notice, the notice comes into force when it is given (unless a later time is specified in the notice). The notice remains in force for the period specified in the notice, which cannot exceed 12 months. A fresh notice may be issued by the Secretary before the original notice expires. The fresh notice may be in the same, or substantially the same, terms as the original notice and come into force immediately after the expiry of the original notice.

System information software notices

A system information software notice can only be given if:

- a computer is needed to operate the SoNS or is a SoNS itself, and
- the Secretary believes on reasonable grounds that a relevant entity for the SoNS would not be technically capable of preparing system information periodic reports or system information event-based reports consisting of information that relates to the operation of the computer; may assist with determining whether a power under the SOCI Act should be exercised in relation to the SoNS; and is not personal information (within the meaning of the *Privacy Act 1988*).

The Secretary may give notice requiring a responsible entity of a SoNS to:

- install a specified computer program on the computer with a period specified in the notice,
- maintain the computer program once installed, and
- take all reasonable steps to ensure the computer program is continuously supplied with an internet carriage service that enables the computer program to function.

A **system information software notice** is used as an option of last resort, and ensures that the Government can provide the entity with the capability necessary to enable the sharing of system information. The software that could be provided by the Government to the entity includes things like a host-based sensor that enables reporting of telemetry information used to monitor systems and networks for malicious behaviour. The functioning of any software is strictly limited to the acquisition and provision of specified information to the Australian Signals Directorate.

A computer program may only be specified in a *system information software notice* if:

- the computer system collects and records information that: relates to the operation of the computer; may assist with determining whether a power under the SOCI Act should be exercised in relation to the system of national significance; and is not personal information (within the meaning of the *Privacy Act 1988*), and

- information can be transmitted electronically to the Australian Signals Directorate.

If the Secretary decides to issue a system information software notice, the notice comes into force when it is given (unless a later time is specified in the notice). The notice remains in force for the period specified in the notice, which cannot exceed 12 months. A fresh notice may be issued by the Secretary before the original notice expires. The fresh notice may be in the same, or substantially the same, terms as the original notice and come into force immediately after the expiry of the original notice.