SECURITY OF CRITICAL INFRASTRUCTURE ACT OBLIGATIONS

CS Energy's assets are considered critical infrastructure under the *Security of Critical Infrastructure (SOCI) Act*.

SOCI legislation requires CS Energy to identify and manage material risks or hazards that could have an impact on our critical infrastructure, including supply chain risks.

It requires entities responsible for critical infrastructure assets to have a positive risk management program that goes beyond existing cyber security obligations and covers the following key hazard domains:

- **Personnel:** The risk posed by critical workers who have the access and ability to disrupt the functioning of the asset.
- **Supply chain:** The risk of disruption, malicious or otherwise, or exploitation of critical supply chains leading to a disruption of the critical infrastructure asset.
- **Physical and natural:** The physical risks to parts of the asset critical to the functioning of the asset, such as physical access to sensitive facilities or 'control rooms', or natural disasters.
- **Cyber and Information Security:** The risks to the digital systems, computers, datasets, and networks that underpin critical infrastructure systems.

Expectations for CS Energy suppliers

A full review is under way across all CS Energy precedent contract terms and purchase/service order terms for future engagement to include SOCI specific obligations.

In the interim, there have been updates to CS Energy's Site Conditions, specifically Section 13.3 in relation to SOCI obligations for suppliers. Details about these obligations are as per below.

General

- Comply with any reasonable requests relating to, or necessary for, CS Energy to meet obligations under the SOCI Act.
- Ensure there is no action taken by the supplier or their personnel that would prevent CS Energy from complying with SOCI obligations.

Critical workers

- If putting forward a candidate for a critical worker position at CS Energy, the candidate must complete a new ASIC Banned and Disqualified/Bankruptcy check.

Notification of cyber security incidents

- Suppliers must notify CS Energy:
    - **As soon as possible and no later than three hours** if a cyber security incident has occurred that has a significant impact[1] (directly or indirectly) and materially disrupts a service that ensures the availability of a CS Energy critical infrastructure asset.
    - **Within 20 hours** if a cyber security incident has occurred where there is a relevant impact[1] to a CS Energy critical infrastructure asset.

- Suppliers must provide CS Energy with all relevant details available to the supplier at the time about the nature and cause of the cyber security incident, and provide reasonable assistance in investigating, responding to, and remedying the cyber security incident including correcting any security flaws and consequences.
- Where the incident impacts CS Energy systems or data, CS Energy's prior written consent is required to notify further parties.

Protected information

- All information disclosed or generated (including by CS Energy or the supplier) in connection with the SOCI Act is deemed protected information and should be used in accordance with the direction of CS Energy and in accordance with the SOCI Act.

Additional canvassing

- CS Energy may ask suppliers at regular intervals to complete a SOCI related questionnaire and assessment to help us better understand our suppliers' upstream supply chains and countries of origin for goods supplied.

Contact

If you have any questions, please contact csprocurement@csenergy.com.au. We appreciate your support to further protect our assets.

[1] Definitions as per the SOCI Act.