SECURITY OF CRITICAL INFRASTRUCTURE

On 2 April 2022, the Security of Critical Infrastructure Act 2018 (SOCI) amendments came into effect, with the goal of protecting critical infrastructure assets essential to the functioning of the Australian economy, society, and/or national security.

As a result, the Australian government has introduced an enhanced obligations framework and widened the scope of assets with IT and OT (operational technology) systems to which it applies.

The updated SOCI legislation impacts organisations in both the public and private sector, including energy, healthcare, government, transport, data centres, water, sewerage, food, commercial spaces, corrections, and defence.

Are you ready?

Honeywell

HOW CYBER INCIDENTS AFFECT FACILITIES WITH CRITICAL ASSETS

When most people think of cyber incidents, they think of data breaches. The reality is that any physical infrastructure with a network connection can be at risk, including OT systems that encompass everything from fire alarms, security systems and HVAC to lighting, servers, and power.

These vulnerabilities have not always been the focus of enhanced cybersecurity. However, incidents are becoming more common and can have serious consequences, including disruption of operations, fines, and legal consequences.

SOCI OBLIGATIONS AT A GLANCE

You now need to notify the Australian government of cybersecurity incidents within strict timeframes:

- 12 hours for a significant impact
- 72 hours for a relevant impact.

Depending on your assets, there are a range of obligations to meet, such as:

- updating the Register of Critical Infrastructure Assets
- developing cybersecurity incident response plans
- undertaking cybersecurity exercises
- undertaking vulnerability assessments
- meeting mandatory reporting obligations within certain time frames.

The new security obligations' framework has been in effect since 8 July 2022. To avoid fines, orders to act in a specified way, the possibility of direct government intervention over your asset, or other penalties it is essential to ensure you are currently compliant.

WHY A HONEYWELL CYBERSECURITY AUDIT IS THE RIGHT FIRST STEP

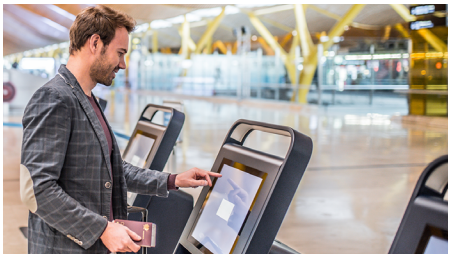
With the number and interconnectedness of today's OT systems, ensuring you are complying with the new security obligations can be complex and resource intensive.

As a leader in building technologies operating in 10 million buildings around the world, we are well prepared to assist.

A critical infrastructure cybersecurity audit from Honeywell can simplify the process and is a straightforward way to get started, providing you with clarity around your risk environment and how to respond.

WHAT A HONEYWELL CRITICAL INFRASTRUCTURE CYBERSECURITY AUDIT COVERS:

- An internal audit of your assets to assess potential risks
- Network map of the key elements of your critical infrastructure assets
- Assistance creating a tailored incident response plan
- Determining your site's cybersecurity maturity level
- A detailed summary of risk elements in order of priority with suggested mitigation actions
- How risk elements need to transition into an ongoing service plan so you can remain compliant.



Book your audit now

For more information
buildings.honeywell.com

Honeywell Building Technologies
Level 3, 2 Richardson Place,
North Ryde, NSW
Australia, 2113
T: +61 2 9353 7000
www.honeywell.com

SOCI-02 | Rev01 | 08/2022

THE FUTURE IS WHAT WE MAKE IT

Honeywell