National Cyber Security Centre | Te Tira Tiaki Government Communications Security Bureau

Cyber Security Guidance: Preventing unintentional operational technology device exposure

16 October 2025 CSG-2025-1616 (Version 1.1)

*The Traffic Light Protocol (TLP) marking is used to ensure that sensitive information is shared with the correct audience. Information sources may use **TLP:CLEAR** when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.*

*The rating for this guidance is **INFORMATION ONLY**. This indicates the NCSC has identified activity that does not pose a threat to the confidentiality, integrity, or availability of your systems at this time. This report is provided for situational awareness or to highlight activity which is not currently aligned with cyber security best practice.*

Executive summary

The NCSC **strongly recommends** organisations identify any unintentional or nonessential instances of internet-connected operational technology (OT) devices[1] in their networks; device connectivity configurations should be changed to **prevent insecure access** to, from, or across the internet. NCSC analysis of public-facing infrastructure has identified internet-connected OT devices in New Zealand. It is highly likely the asset owners are unaware of the risk posed by this exposure. Depending on their motivation, malicious cyber actors may opportunistically or systematically target devices in New Zealand. Historically, OT devices were isolated and designed for use in closed networks without external connectivity. As a result, most OT devices have inadequate inherent security functionality. Internet-exposed OT devices are easily discoverable with help from commonly available tools. Organisations of all sizes may be targeted; however, smaller organisations may be perceived as softer targets for financial or political gain.

This guidance provides actionable recommendations for OT asset owners, operators, and integrators to protect New Zealand OT systems against malicious cyber activity targeting public-facing infrastructure. Where possible, remote connectivity to devices should be prevented and/or secured through defensible architecture, compensating controls, and active risk management.

Overview

Over time, operational technology (OT) devices such as industrial control systems or building management systems have shifted from isolated ('air gapped') networks to increasingly complex and inter-connected networks. The drivers of this shift include:

- The convergence of information technology (IT) and OT networks for business needs.
- An increased desire or requirement to remotely manage, monitor, and support OT equipment.
- The rise of industrial internet of things (IIoT) devices that need public cloud connectivity to function.

However, most OT devices are not designed to be internet-facing and should not have direct access to the internet as they lack the necessary security controls to protect against malicious cyber activity.

[1] Examples of OT systems include industrial control systems (ICS), supervisory control and data acquisition systems (SCADA), programmable logic controllers (PLCs), and building management systems.

Threats to internet-exposed OT

Malicious cyber actors may opportunistically or systematically target internet-exposed OT devices in New Zealand for financial or political gain. All types and sizes of organisations can be targeted; malicious cyber actors do not solely focus on large organisations, as smaller organisations can be perceived as softer targets. For example, hacktivists aim to draw attention to their cause, whether political, social, or ideological, through malicious cyber activity. Their choice of target is often opportunistic and may not be linked to their cause, resulting in organisations being targeted unexpectedly. Malicious adversaries may also target New Zealand OT systems to develop their access for future malicious activity.

Insecure remote access to OT devices and systems can present significant risk. Potential impacts of unauthorised access to OT devices include financial loss, loss of asset control, environmental impacts or, in serious cases, loss of life. There are several publicly reported incidents involving operational technology, including the U.S. Colonial Pipeline[2] incident in 2021.

Exposed devices are easily discoverable using publicly available tools due to open ports on public IP ranges. These devices sometimes rely on basic password protection to guard administrative access, which does not sufficiently defend against malicious cyber activity. Secure remote access to OT devices is possible but it requires defensible architecture and active risk management.

Recommendations

- The NCSC strongly recommends that asset owners and operators **identify** internet-connected OT devices in their networks. For advice on how to achieve this, review the U.S. Cybersecurity and Infrastructure Security Agency's (CISA) Internet Exposure Reduction Guidance.
    - Where internet connectivity is unintentional or not required, asset owners and operators should change configurations for any internet-facing OT devices to **prevent or restrict access** to, from, or across the internet.
- Organisations should **identify** what additional security controls can be implemented to reduce the risk of unauthorised access to these systems.
    - For device or system specific guidance or configuration assistance, contact your integrator or the original equipment manufacturer.
- In cases where remote connectivity from outside of your OT network is required, secure remote access requires a layered defence approach. Best practice mitigations include:
    - Use of unique, non-default credentials, with multi-factor authentication (MFA) enabled and enforced where possible.
    - Design of secure remote access as an ephemeral connection through a bastion/jump host (or other secure third-party remote access solution).
    - Tight control of both ingress and egress traffic between OT networks and other networks with a default deny policy for traffic.
    - Utilising private APNs to have additional control over cellular connected devices.
    - Monitor device logs and network traffic for malicious or abnormal activity. Ensure there is appropriate alerting for this monitoring to raise detected issues to the right level of attention and response.
- The NCSC recommends that organisations review the Operational Technology section of the NCSC website.

[2] https://www.energy.gov/ceser/colonial-pipeline-cyber-incident.

Report an incident

If you suspect that your OT systems have been impacted by malicious cyber activity, please report this to NCSC through our online reporting tool: Report an incident.

Request for information

The NCSC aims to provide timely and actionable advice to industry on New Zealand's relevant vulnerabilities. Please let us know if this guidance aided you in discovering and addressing unintentionally internet-exposed OT devices. We also welcome any feedback on this product. Contact us at **info@ncsc.govt.nz** and include the title of this guidance in the subject line.

Resources

The NCSC recommends organisations review and implement the guidance outlined in the following resources where possible:

- For advice on reducing internet exposure of OT, see CISA's Internet Exposure Reduction Guidance.
- For advice on reducing cyber threats to OT, see CISA's Primary Mitigations to Reduce Cyber Threats to Operational Technology.
- For advice on creating an asset inventory for OT, see NCSC's Foundations for OT Cybersecurity: Asset Inventory Guidance for Owners and Operators webpage.
- For more information on what to require when procuring OT, see NCSC's Secure by Demand for OT Owners and Operators webpage.
- For advice on improving cyber security for IT-to-OT networks, see the U.S. National Security Agency's (NSA) Stop Malicious Cyber Activity Against Connected Operational Technology.
- For guidance on developing a comprehensive record of OT systems, see NCSC's Maintaining a Definitive View of Your OT Architecture webpage.
- For guidance on creating an effective OT security program, see Australia Signals Directorate's Principles of operational technology cyber security.

NCSC Cyber Security Framework

This advice is consistent with the **Prevent and Protect** function within the NCSC Cyber Security Framework. The advice is designed to assist with reducing actual risk and incrementally improving security now, rather than aiming for perfect security tomorrow. Assets need protection in a way that prevents incidents and addresses vulnerabilities before they are exploited. To do this effectively, asset owners need to **Identify and Understand** their assets and how they can be targeted. To create an asset inventory for OT, see Asset Inventory Guidance for Owners and Operators.

Acknowledgements

The NCSC would like to thank the NZ ICS Cyber Technical Network for their support in developing this resource for New Zealand industrial organisations and practitioners. For more information, visit the Technical Network's website: ICS Cyber.

The NCSC can be contacted by email at: **info@ncsc.govt.nz**.

NCSC Incidents can be contacted by reporting through our online reporting tool: Report an incident. For immediate support, phone **(04) 498 7654**.

We encourage you to contact us at any time if you require any further assistance or advice.

UNCLASSIFIED//TLP: CLEAR

The information within this report should be handled in accordance with the classification markings.