Submission to the Australian Federal Government

Policy Discussion Paper – Horizon 2

Genetec Inc, a global software company, whose physical security solutions are used by over 42,500 organisations and governments in 159 countries, is pleased to submit the following response.

Genetec has consistently advocated for the highest standards of ethical conduct and cybersecurity best practice across the global physical security industry.

In this submission, we outline recommended actions the Australian government could take over the next three years to address national and cybersecurity concerns linked to video surveillance equipment from companies governed by the National Intelligence Law of the People's Republic of China.

We believe responsible technology manufacturers must work together to protect and educate users—collaborating with legislators, technologists, civil rights organisations, and corporations.

We remain available to discuss our recommendations further.

NOTE: Only questions related to these points are addressed in this submission:

Genetec Australia Pty Ltd
[redacted]
Genetec.com

Q18. What are best practice examples internationally that Australia should consider for enhancing our secure technology standards and frameworks? In particular, what approach do you consider would work best for edge devices, CER and operational technology?

Change must often be driven from the top. In the case of cybersecurity and national cyber defense, we have seen the benefits of this in the United States:

- The *Executive Order on Strengthening and Promoting Innovation in the Nation's Cybersecurity*, signed by former President Biden in January 2025, calls for improved threat information sharing between government and the private sector. It is expected to enhance national resilience and responsiveness to cyberattacks.
- To date, the order has proven effective in raising awareness, focusing attention, and providing strategic direction to state and federal agencies.

Other countries, including the UK and Canada, have taken proactive steps to regulate and oversee cybersecurity. Australia could benefit from adopting a similar approach.

Key recommendations:

- **Supply chain guidance and Software Bills of Materials (SBOMs)**: The US requirement for vendors to disclose third-party dependencies improves supply chain transparency and supports informed purchasing decisions. In Australia, end users of edge devices (like surveillance cameras) often face a difficult decision when economic factors (i.e price of equipment) are prioritized over security concerns. Government guidance, and mandated minimum standards, would strengthen national security by discouraging the use of poorly protected (often less expensive) surveillance equipment.
- **Security Best Practices**: Encryption, password changes, and other basic protections should be standard across all commercially available operational technology. Procuring tools that are not following best practices, or maintaining older technology that cannot comply, should be discouraged or regulated against.

- **Standards and Compliance**:
    - ISO 27001 and SOC 2 Type 2 are global standards that provide detailed guidance that could be prioritized by Australia. Local certifications, such as IRAP, also offer value but prioritising compliance with international standards may be a more efficient baseline.

Q20. What additional guidance do you or your organisation need to manage foreign ownership, control or influence risks associated with technology vendors?

Physical security hardware (such as video surveillance cameras and other IoT sensors including access control controllers and readers) produced by Chinese state-owned manufacturers have posed a known cyber threat for nearly a decade. Despite this, low-cost edge devices from such sources continue to be deployed across industrial, commercial, and government environments in Australia—including critical infrastructure settings.

Australia has already removed Chinese-made surveillance cameras from defence sites due to national security concerns. This is a positive first step and should form part of a broader initiative to safeguard Australia and its critical infrastructure.
Internationally, western nations have taken decisive action:

- In June 2025, the Canadian Government ordered Chinese surveillance camera manufacturer Hikvision to cease operations in Canada over national security risks. In addition, the Government of Canada is prohibiting the purchase or use of Hikvision products in government departments, agencies, and crown corporations.
- The UK government has restricted Hikvision equipment in government and sensitive sites, committing to its phased removal.
- Similar restrictions are in place in the United States for both Hikvision and for Dahua Technology.

Issuing clear guidance—rather than simply discouraging purchases from non-trusted vendors with unverified components and opaque supply chains—would help Australian leaders and procurement officers make informed decisions.

Aligning with trusted Five Eyes partners to prohibit the installation of cameras from state-owned manufacturers (such as Hikvision) would be neither unprecedented nor impractical. In 2018, Australia became the first Five Eyes member to issue security guidance to telecom providers, requiring them to avoid purchasing 5G equipment and services from Chinese manufacturer Huawei. This was intended to mitigate risks of espionage and state-sponsored sabotage of critical infrastructure. Physical security technology, such as cameras connected to networks, presents similar risks of cyber espionage and attacks.

Compliance with a wide range of government-mandated standards and regulations for critical infrastructure can be complex and costly for manufacturers. This increases the risk of delays or, worse, non-compliance in technology delivery. In the longer term, collaborating with other western governments to replace fragmented regulations with a unified set of standards could reduce the bureaucratic and compliance burden for Australia and its allies.

Genetec Australia Pty Ltd
[redacted]
Genetec.com

Q26. How could government further support industry to block threats at scale?

While the Security of Critical Infrastructure (SOCI) Act 2018 provides fit-for-purpose legislation, enforcement needs to be prioritized. Many industries covered by the Act continue to deploy physical security devices that breach its provisions, with few repercussions. Organisations and contractors are still able to install insecure devices without consequence.

Recognising that regular audits under the SOCI Act would impose a bureaucratic burden on both government and industry, Genetec recommends restricting use (and potentially access) to non-compliant devices as a solution. The government should define criteria for surveillance equipment to help organisations transition to trusted suppliers that prioritise cybersecurity. Although individual organisations are responsible for maintaining cyber defences proportionate to their risk exposure, there is scope for the government to take a more proactive role in regulating against technology that is known to pose cyber threats, as well as to pursue and penalise organisations that do not comply with regulation.

In addition, currently no Australian threat-sharing initiative exists with the physical security industry. Establishing mechanisms for information exchange with trusted vendors would enable greater participation in collective defence. Other nations have addressed this by creating standardised threat feeds and opening two-way communication channels between cybersecurity authorities and selected vendors.

Q33. How effective do you consider the SOCI Act at protecting Australia's critical infrastructure? Are the current obligations proportionate, well understood and enforceable?

While the SOCI Act is fit for purpose, its lack of enforcement offers limited protection for Australia's critical infrastructure.

- Financial penalties and restrictions on grant funding could be effective enforcement tools. However, banning the sale of insecure hardware would be a simpler, less resource-intensive solution, avoiding the need for a dedicated compliance function within the relevant government agency.

- Wholesale removal of existing surveillance fleets may feel impractical but mandating their replacement with compliant alternatives at end-of-life, and prohibiting their repurchase, is a common and practical approach. A useful parallel is asbestos: although its sale was banned decades ago, removal was not mandated. Legislation now requires replacement with safe materials during renovations. Applying the same principle to non-compliant surveillance devices could resolve the issue within a decade, given their average lifespan of five to seven years.

- Vendors complying with the SOCI Act may face commercial disadvantages. For example, when an Australian airport sought new physical security systems, Genetec won two tenders but could not proceed due to legacy, non-compliant SOCI technology in use on site. Genetec no longer supports such devices due to associated cyber threats and its commitment to prioritising cybersecurity. The airport operator chose not to implement a plan to replace the existing cameras, and as a result, Genetec withdrew from the project. Despite the SOCI Act, the non-compliant devices remained in use as part of the airport's infrastructure.

Q35. Is the regulatory burden on industry proportionate to the risk and outcomes being sought?

Currently, there is little incentive for industry players to comply with the SOCI Act. Despite the significant cyber risk, building contractors are not held accountable for their choice of surveillance equipment in critical infrastructure settings.

In many cases, contractors have free rein to procure and install devices from Chinese state-owned suppliers, introducing cyber vulnerabilities. This contrasts with other safety systems—such as intrusion and fire alarms—which are heavily regulated, regularly tested, and subject to strict compliance standards. As a result, contractors are discouraged from deploying systems with known weaknesses.

At present, the burden of risk falls entirely on end-user organisations, which face multi-million-dollar remediation costs in the event of a breach. Shifting responsibility for surveillance equipment integrity to suppliers and installers would incentivise better cybersecurity practices. Legislation enabling the State to impose penalties on entities using non-compliant solutions could act as a catalyst for change.

Prevention is better than cure. Enforcing specifications that restrict the installation of unsafe physical security technology in critical infrastructure would significantly strengthen the sector's security posture.

Genetec Australia Pty Ltd
[redacted]
Genetec.com

Q38. How are Australian Government security requirements or frameworks being considered or adopted among private sector partners, including in critical infrastructure?

There is insufficient awareness of the cyber risks facing critical infrastructure. In the absence of a major incident, many organisations remain unaware.

Numerous airports, stations, and other critical infrastructure sites across Australia continue to use unsecure surveillance devices. While frameworks such as IRAP and the Essential Eight offer valuable guidance, they appear to have limited influence on procurement decisions.

In other jurisdictions, cybersecurity leadership and compliance are managed by a single, well-resourced agency—unlike the Australian Signals Directorate, which has more limited reach. While such a body could positively influence cyber security in Australia, Genetec believes that stronger preventative measures would be effective. Restricting the supply and/or installation of surveillance devices from Chinese state-owned manufacturers that are known to introduce a cyber threat could gradually improve security across critical infrastructure without the need for resource-intensive compliance programmes.

Aligning Australia's compliance standards with those of like-minded nations would also be beneficial. Greater government and industry participation in the development of global standards, such as ISO 27000, would raise awareness and encourage broader adoption of robust security frameworks

Genetec Australia Pty Ltd
[redacted]
Genetec.com

Q45. What are the areas of most concern for ICT concentration and what do you consider would be most effective as mitigation strategies to explore?

Data sovereignty and recovery should be key concerns for both government and industry. Effective measures can be implemented to address both.

1. Using a leading cloud provider with infrastructure hosted in an Australian-owned data centre is the most reliable way to ensure sensitive data remains within national borders. Guidelines for vendors that host their own data centres offshore should be considered.

2. Maintaining a diverse supply chain, sourcing technology from trusted vendors, helps reduce the impact of potential disruptions.

3. Government mandates that prohibit the deployment of surveillance equipment failing to meet defined specifications and cybersecurity best practices would allow organisations to mitigate risk by default.

4. While regulation is essential, suppliers should not be overburdened with excessive certifications and approvals, which can unintentionally hinder innovation and delay compliance. Collaborating with other Five Eyes nations to establish broadly aligned standard would reduce the compliance burden for trusted suppliers while maintaining strong security expectations.

Genetec Australia Pty Ltd
[redacted]
Genetec.com