

JOINT STATEMENT ON THE GLOBAL CYBERSECURITY LABELLING INITIATIVE

23 OCTOBER 2025

The eleven members of the Global Cybersecurity Labelling Initiative (GCLI) - named participants below - gathered for the inaugural GCLI convening. Members reaffirmed their joint interest to building a more secure and trustworthy digital future.

Our Collective Opportunity

This initiative represents our collective intention to promote a trusted global ecosystem of connected devices, built on harmonised security requirements that protect consumers, support innovation, and strengthen digital resilience across borders. In an era of unprecedented digital connectivity, the security of Internet of Things devices and connected technologies has become fundamental to protecting consumers, businesses, and critical infrastructure globally. The ubiquitous use of connected devices across all sectors of society requires a coordinated international approach.

Through this collaborative effort, we intend to establish a cooperation forum where cybersecurity features become an enabler of the global digital economy. By working together through a multilateral cooperation forum, we can amplify the positive impact of individual national initiatives whilst fostering market incentives for enhanced device security and reducing complexity for manufacturers and consumers.

GCLI highlights the importance of a collective reflection on aligning our approaches to cybersecurity labelling; more specifically on clear, harmonised security requirements that raise baseline cybersecurity hygiene to protect consumers, reduce business costs through streamlined compliance processes, and strengthen resilience of Internet of Things devices against evolving cyber threats while fostering and encouraging innovation and while respecting the national competences and legal frameworks of members.

Building on Global Momentum

The global IoT security landscape demonstrates remarkable momentum, with numerous members actively developing and implementing cybersecurity labelling schemes and/or regulatory frameworks. This widespread commitment to IoT security reflects a shared recognition of its importance and creates a strong foundation for enhanced international cooperation.

We recognise an opportunity to harness this collective momentum through a multilateral approach. Whilst bilateral arrangements have provided valuable experience and marked

important progress, a multilateral framework offers greater efficiency and scalability to serve the global nature of IoT supply chains and manufacturing.

The diversity of approaches currently being developed across jurisdictions presents both opportunities and challenges. By bringing together these varied experiences and expertise, we can consider a common approach on requirements for IoT products that draw upon best practices from different national contexts whilst ensuring manufacturers can navigate cybersecurity compliance more efficiently across multiple markets.

Moving Forward

GCLI provides the platform for like-minded members who share our vision of advancing beyond individual national initiatives towards a globally coordinated approach to cybersecurity and IoT device security. Together, we will work to ensure that the benefits of connected technologies can be realised safely and securely by consumers and enterprises globally, supported by a multilateral cooperation forum.

Named Participants

- Cyber Security Agency of Singapore, Singapore
- Cyber Security Brunei, Brunei
- Cyber Security Council, United Arab Emirates
- Department for Science, Innovation and Technology, the United Kingdom
- Department of Home Affairs, Australia
- Federal Office for Information Security, Germany
- Finnish Transport and Communications Agency Traficom, Finland
- Ministry of Science and ICT and Korea Internet & Security Agency, Republic of Korea
- Ministry of Economy, Trade and Industry, Japan
- Public Safety Canada, Canada
- Supervisory Authority for Regulatory Affairs, Hungary