G7 Cybersecurity Working Group Statement on IoT Security

In recent years, the Internet of Things (IoT) has rapidly increased to include a diverse range of products that connect directly or indirectly to the internet, such as routers and network cameras, industrial control equipment, and even household appliances. The volume of malicious cyber activity that targets IoT products is increasing. Against this backdrop, many G7 members desire to increase the awareness of procurers by informing them of product security by implementing certification frameworks and/or labelling schemes for IoT cybersecurity.

In order to address IoT cybersecurity in its entirety, both technical and non-technical cyber threats should be taken into account to the extent possible. IoT cybersecurity has not only a technical nature/implication, but also specific political, economic or other behavioral implications that malicious actors seek to exploit. This is especially important for IoT products used in highly sensitive areas, in particular central and local government agencies and critical infrastructure. The G7 Cybersecurity Working Group, after consulting with relevant stakeholders outside the Working Group, has concurred on a set of proposals to both government policy and to industry to address IoT cybersecurity in its entirety.

A. Proposals to G7 Member States (Government)

- **The overall risk of influence of an IoT product vendor by a third country should be taken into account**, such as the jurisdiction of production of the IoT products. This could include adherence to international declarations against unlimited government surveillance, or if threat actors are operating out of the jurisdiction of a third country, or whether there is an obligation on the vendor to report information on software or hardware vulnerabilities to the authorities prior to those vulnerabilities being known to have been exploited.

B. Proposals to Industry (IoT Vendors and End-users)

- **Risk assessments of IoT vendors' products should take into account all relevant factors**, including applicable legal environment and product connectivity mechanisms.
- **Such assessments should take into account rule of law, security environment, vendor malfeasance, and compliance with open, interoperable, secure standards, and industry best practices** to promote a vibrant and robust cyber security supply of products and services to deal with the rising challenges.

G7 2025 KANANASKIS