House of Commons Committee
Product Security and Telecommunications Infrastructure Bill
Palo Alto Networks Recommendations
18 March 2022

Submitted via email: hooki@parliament.uk.
Attachment: "Governments Must Promote Network-Level IoT Security at Scale" (PDF)

Palo Alto Networks welcomes the opportunity to provide written comments to the House of Commons Committee on the Product Security and Telecommunications Infrastructure Bill. As a leading cybersecurity company, we work with an array of organisations globally across all industry verticals that are involved in deploying and running IoT systems or otherwise have a stake in IoT security. We also have done extensive research into threats to IoT. We have used this experience and expertise to inform our response to the Committee's examination of the Bill.

Whilst we support the Government's overarching objective of developing policy interventions to address the security of consumer IoT devices, we believe its efforts could be improved by addressing further cybersecurity solutions. The Bill specifies that device manufactures will be required to adhere to the security requirements set out by the Secretary of State. ***However, there are limitations to a device-centric approach, and we believe the Government's approach to consumer IoT security could be enhanced by also focusing on network-level IoT security, which is deployed across all devices and uses, regardless of device type.***

As set out in the Bill's Explanatory Notes "*insecure products can act as the 'point of entry' across a network, enabling attackers to access valuable information"*, and this risk has been compounded as people increasingly work from home. In fact, the Covid-19 pandemic has exacerbated the IoT security challenges for enterprises and governments as their employees have transitioned much of their work to their homes. Even in cases when employees at home have a VPN on their laptops, that security is limited just to that device—if the laptop connects to an untrusted home network, it might be the target of a lateral threat movement from a connected, compromised IoT device that might then allow an attack to make its way into the corporate network. Securing work-from-home equals securing the home, which requires bringing network-level security to all the IoT devices in the home.

To address the limitations in embedded device security, we recommend that the Government references the need for network-level IoT security at scale in the Explanatory Notes (under the section on Product Security, from paragraph six) and that the Government produce guidance on how enterprises and governments can secure the use of IoT devices at the network level.

The attached position paper, "Governments Must Promote Network-Level IoT Security at Scale", describes the cyber threats and risks to IoT, limitations of embedded device security, and how network-level IoT security can complement this approach. We have excerpted some of this information below and stand ready to provide further information to the Committee at your convenience. Please contact Carla Baker via email at cbaker@paloaltonetworks.com should the Committee need further information.

Policy interventions aimed at addressing the IoT threat landscape
It is evident that IoT adoption is growing rapidly across industry verticals and consumers worldwide, leading to a growing attack surface and new threat landscape. In turn, governments are exploring regulations or codes of practice to promote IoT security. However, many governments focus on promoting measures that IoT device manufacturers should take when building or maintaining devices.

We commend governments' intentions to address IoT security. But while built-in IoT device security measures are important – and arguably manufacturers can make improvements – this approach does not account for or address the full picture of cybersecurity threats and risks to IoT devices, users, and networks.

Limitations to relying solely on security controls embedded in devices
Embedded device security is very important. Approaches that IoT device makers should take, such as prohibiting universal default passwords, keeping software securely updated, making systems resilient to outages, and others are important steps. Devices also must be secure so that their identities are not spoofed, and their root of trust stays intact -- this is imperative to an understanding of a device's baseline behaviour and detection of anomalous behaviour

However, relying just on IoT device-based security is insufficient due to inherent limitations related to many IoT devices themselves, threats, and risks in the supply chains of IoT device manufacturers, and the threats and risks arising from real-world deployments of IoT devices.

Security limitations related to IoT devices themselves

- *It is impossible to embed security in certain IoT devices***.** Some IoT devices simply lack capacity for built-in security. For example, some devices do not have sufficient storage or processing power to support logging or cryptographic abilities to protect sensitive information being processed. Sensors such as thermostats, smart lighting hardware, and smart blinds are examples of IoT devices that typically would not have sufficient capacity for built-in security. Many already deployed IoT devices are low cost, with no security embedded, making easy entry points for adversaries.
- *Legacy devices are a challenge.* Billions of already-deployed IoT devices globally cannot be retroactively (retrospectively) designed for security (nor can they be certified or labelled). For some devices, secure update mechanisms may be inadequate; some continuously operating, mission-critical devices (e.g., robotics, factory production line sensors, video surveillance, and IoMT devices) receive updates infrequently. Some already deployed devices may already have reached their end-of-life date or may never have had the functionality to update.
- *Heterogeneous nature of devices makes a uniform built-in standard impossible***.** Too many different types of devices and manufacturers exist to expect a uniform standard for embedded device security.
- *Lack of vendor action.* Some vendors simply provide poor or non-existent product security or patch support, even if required to do so.

Whilst we welcome the efforts of the Department for Digital, Culture, Media and Sports (DCMS) to improve the security of consumer IoT devices, as set out above, we believe the Government's approach to the security of consumer IoT devices could be significantly enhanced by also focusing on network level security.