GARMIN.

Garmin International, Inc.
1200 East 151st Street
Olathe, Kansas 66062
P: 913-397-8200 F: 913-397-8282

NIST’s Call for Papers on Cybersecurity Labeling Programs for Consumers: Internet of Things (IoT) Devices and Software [1], requests diverse stakeholders to submit “one- or two-page position papers providing suggestions and feedback on the challenges and practical approaches to consumer software labeling.” Garmin respectfully submits this position paper for consideration of challenges faced by manufacturers of IoT devices.

For more than 30 years, Garmin has developed innovative products guided by our mission: *To be an enduring company by creating superior products for automotive, marine, outdoor, and sports that are an essential part of our customers’ lives*. As noted in the Product Security section of our 2020 Sustainability report [2], we follow security and privacy by design principles for all our products, from design through customer use, decommissioning and refurbishment.

Cyber security attacks and defenses are dynamic, changing rapidly with advances in technology. In contrast, labels (as well as related certification schemes for security) suffer from being static, point in time assessments. As an alternative to labeling, instead focusing on the principles and processes used by IoT manufacturers is a more enduring approach because A) it better withstands time as attacks and defenses evolve and advance, and B) risk-based principles better account for the diversity across consumer IoT products. If not thoughtfully approached, consumer IoT labeling programs have the potential to increase cost for the manufacturer, while at worst providing a false sense of security to the consumer.

Garmin believes that any consumer-facing label (on-a box or otherwise digitally presented) has substantial drawbacks when the product life cycle is considered. A label affixed to a product at the time of manufacture could cause a given product to appear "outdated" if significant time is required for a product to make its way through the logistics chain between the manufacturer and retail point of sale. Additionally, any tiered security features communicated via a tiered/graduated labeling scheme could differ substantially depending on the exact nature of the product and its usage context.

Another related (perhaps more fundamental) challenge of consumer IoT labeling efforts (and backing certification schemes) is defining the scope of applicability. This point is especially relevant to Garmin given our diverse range of purpose-built consumer products. Determining scope for our products is especially challenging given that IoT itself as a term is not well defined. Paraphrasing [3], NIST itself has not offered a definition of IoT, but instead describes IoT in terms of characteristics and capabilities. In similar fashion, UK DCMS [4] and EN 303 645 [5] respectively use the terminology “network connectable” and “connected to network infrastructure”, without accounting for the frequency with which a device may be connected.

Consider continuously-connected and rarely-connected devices as two opposite classifications in this regard. Continuously-connected devices, especially those exposing remotely accessible services, present a greater risk for exploitation and participation in botnets/DDoS attacks than rarely-connected devices. As an example of a rarely connected device, consider a Fish-finder that infrequently connects only for downloading software updates. Such a rarely-connected product should fall outside the scope of any proposed schemes -- the nature and function of such an outdoor recreational product is inconsistent with the risks of continually-connected devices routinely considered IoT.

As a manufacturer of consumer electronics products, many of which are likely to be considered within the scope of any consumer IoT labeling proposals, Garmin has an interest in (a) ensuring fair competition with our competitors world-wide, and (b) consistency among regulations and standards to which in-scope products are held.

- If NIST moves forward with a security label for IoT, then any process used by manufacturers to *self-certify* must be well defined and have appropriate punitive provisions in place for violators. Self-certification from unscrupulous manufacturers that squeak by at lowest-cost (rather than what is appropriate) is a concern for Garmin.
- If NIST instead follows precedents of UK DCMS [4], opting not to mandate labels, but to instead mandate baseline criteria as a predicate for market access, then we implore NIST to carefully align with existing world-wide efforts. For example, adhering to top provisions from EN 303 645 [5] as also advocated by the UK DCMS will help simplify compliance efforts for manufacturers and reduce related expenses.

Though current pilot efforts imply adoption would be voluntary, we want to express longer term concerns with any future mandatory schemes used as barriers to gate access to market access, such as currently promulgated by UK DCMS. Rather than mandating consumer-facing labels, mandate that manufactures have processes/programs in place ensuring risk-based ‘secure by design’ and ‘privacy by design’ principles are followed, consistent with the legislative approach taken by the European Union in its General Data Protection Regulation. This levels the playing field across manufacturers and removes the burden of marketing a new label to consumers. Another advantage of a process/program-based approach is not divorcing the devices themselves from their supporting services. A label on the product puts emphasis on the device without considering the (often greater) exposure and risk on the service side.

[1] "Workshop and Call for Papers on Cybersecurity Labeling Programs for Consumers: Internet of Things (IoT) Devices and Software." *NIST*, 3 Aug. 2021, https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/workshop-and-call-papers-cybersecurity-labeling. Accessed 13 Aug. 2021.

[2] Garmin. “2020 SASB REPORT: Reporting under the sustainability accounting standards board (SASB) standards for the year ended Dec 26, 2020”. Product Security. Page 4. SASB_2020.pdf (garmin.com)

[3] Ande, R and Adebisi, B and Hammoudeh, M and Saleem, J. “Internet of Things: Evolution and technologies from a security perspective.” *Sustainable Cities and Society*, Vol 54. 2020. pages 8-9. ISSN 2210-6707 https://doi.org/10.1016/j.scs.2019.101728.

[4] UK DCMS "Government response to the call for views on consumer connected product cyber security legislation". Policy Paper. *GOV.UK*, April 21, 2021. https://www.gov.uk/government/publications/regulating-consumer-smart-product-cyber-security-government-response/government-response-to-the-call-for-views-on-consumer-connected-product-cyber-security-legislation Accessed Aug 16, 2021.

[5] ETSI. Cyber Security for Consumer Internet of Things: Baseline Requirements. EN 303 645 v 2.1.1. June, 2020. https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf Accessed Aug 16, 2021.