Supporting the Wireless Device Industry

WWW.LPRA.ORG

15th February 2021

LPRA opinion on preparations for activation of Articles 3.3 of the Radio Equipment Directive

The LPRA understands the legitimate concern and anxiety of consumers attached to the ever increasing use of poorly secured networked IoT devices and the threat that they pose to society - both to personal data held on and processed by these devices, and the threat that such insecure devices pose to the wider Internet-using community in the form of Distributed Denial of Service (DDoS) attacks. Insecure devices such as these pose a socio-economic threat far beyond the cost of individual devices and it is right that industry and regulators work together to counter this growing menace.

The LPRA has previously set out clearly its concerns about using the Radio Equipment Directive (RED) to address such deficiencies, particularly as new horizontal legislation is planned and the roll out of the Cyber Security Act (CSA) is well underway. Nevertheless, we understand the imperative to move as quickly as possible to address these concerns at a European level using legislation that is already in place.

The LPRA has been closely involved with preparatory work by both CENELEC and ETSI in anticipating new standards that will be required to implement the soon-to-be-published Delegated Acts and is concerned that the magnitude of the task of generating such standards may have been underestimated.

Our members' current experience in drafting standards associated with Article 2.2 of the RED suggests that the EC will seek legal certainty in ensuring that products placed on the European market satisfy the essential requirements set out in the new Delegated Acts. However, the nature of risk-based security assessments – such as those set out in the ISO27000 standard series - is that no products can be 'proven' to be secure; the nature of security assessments and corresponding defensive strategies are that they are designed to provide reasonable assurance given the value and nature of the data to be secured and the threat environment in which those products operate.

The EC should understand the nature – and necessary limitations – of such risk based approaches and accept that companies can, at best, demonstrate best efforts to achieve

the goals of the delegated acts. As a consequence, industry needs to be given guidance as to whether the EC would accept such a risk assessment (with no guarantee that a product cannot be hacked), or perhaps a sub-set of requirements that can be tested and *demonstrated* to be present (and which would be combined with a wider risk assessment under other legislation, such as the CSA). The EC would also need to look closely at its criteria for acceptance of proof of compliance and allow manufacturer-developed documentation (such as security architecture and underlying software inventories) to be accepted.

The impact that legislation in this domain may have on SMEs – core of the European electronic product manufacturing industry and a large proportion of our membership – is also a concern. These companies are capable of designing secure products but may not have the detailed specialist security compliance expertise that exists in larger enterprises. SMEs may also be deploying equipment in environments in which the security requirements on the device under test (as opposed to the surrounding system) are not onerous, and so a full security assessment of such a product would be unnecessary. Such companies would not be able to afford to have expensive third-party assessors evaluate products every time a new product certification is required.

The LPRA is also concerned that many of the radio products that its members produce are, in effect, ***not*** connected to the Internet, but that poor drafting of the Delegated Acts might accidently require assessment of a raft of non-IoT devices that are not intended to be included by the spirit of the legislation, for example systems that temporarily connect to the Internet (under human supervision) during their configuration phase, but which thereafter broadly operate independently.

The clarity of the forthcoming acts, therefore, is imperative. Poorly or vaguely worded measures will cause considerable anxiety and cost to our members until precedent legal cases are heard.

The availability of standards is another concern to our members. ETSI recently reported that the time for completed standards to be cited is now close to one year – even for well-understood RF standards. It seems inconceivable that a set of standards covering the delegated acts can be completed in less than twelve months. Given that the EC has set out its intention for a grace period of just two years we fear a crisis in two years' time when standards are not available. Unless the EC is prepared to extend this deadline, there must be close cooperation between the technical staff of the EC and the ESOs to ensure that no time is lost in exploring unhelpful avenues. Industry cannot afford to wait to the end of this process for the EC declare that there are fundamental issues with the structure of candidate standards.

In summary therefore, the LPRA calls on the EC to:

- publish **clear and unambiguous requirements** on products that clearly delineates the scope of this legislation and required proof of compliance;

- accept a **pragmatic risk-based approach** to securing products' operation;
- ensure that **SMEs are not penalised** for their comparative lack of specialist security expertise;
- consider an extension to the 24-month grace period and a **commitment to work closely with technical teams within the ESOs** to ensure the most efficient way of working.

Dr Saad Mezzour
Chairman
LPRA (Low Power Radio Association)

WWW.LPRA.ORG

LPRA Secretariat
Tel: +44 (0) 1268 755 394
Email: LPRAeNews@me.com