Computer & Communications Industry Association
Tech Advocacy Since 1972

CCIA Europe
6 Rond Point Schuman, 1040 Brussels

4th November, 2014

Open Letter to Member State Telecoms Ministers:

EU Network and Information Security (NIS) Directive must focus on critical infrastructure

CCIA Europe welcomes the proposed Network and Information Security (NIS) Directive. This proposal complements other related EU initiatives including the European Commission's Cyber Security Strategy, the NIS Platform, and EU research programs. The NIS Directive can help ensure that Member States adopt capabilities and a high common level of security across the EU in critical sectors such as energy, banking, and transport.

The European Parliament's vote from March 2014 correctly improved the scope of the text by focusing protection on truly critical infrastructure.

As the Council continues its negotiations toward reaching a common position, we urge EU Member States to similarly consider excluding Internet enabling services (IES) from the scope of the NIS Directive for the following reasons:

Focus protection on truly critical infrastructure

Citizens rightfully expect that scarce economic resources and technical expertise are prioritized to focus on protection of truly critical infrastructure such as nuclear power plants and transportation facilities - rather than on online gaming, social networks, and other IES. Security considerations for such entities are inherently different, and placing them under the same regulatory umbrella risks conflating truly critical security concerns and incidents with breaches that are already, and more appropriately, addressed via different instruments. Focus should remain on the highest end of the risk/threat spectrum; a significantly broader scope of the NIS Directive risks undermining the law's ability to protect what really needs protection.

Avoid fragmentation of the EU Digital Single Market

As a "minimum harmonization" directive Member States can broaden scope and include additional requirements for all operators as they see fit. This opens the door for a harmful and uneven cybersecurity regulatory patchwork emerging where pan-European companies could face different or even contradictory requirements within the 28 Member States. This would significantly increase compliance costs especially for European SMEs which represents 99% of all businesses. Forcing a "protect all services equally approach" will actually only create a less secure environment in a more fragmented European Single Market.

Recognise existing protections

Many IES are already regulated for the cybersecurity incidents envisioned here, and additional legislation would only introduce complexity and confusion. The EU's Data Protection legislation for instance covers critical parts of these services. The soon to be concluded EU Data Protection Regulation has broader reporting and security obligations as well. This means that even if the NIS Directive is focused to critical infrastructure sectors, such as finance, this would include the protection of online banking and other related services in the scope of the Directive. Basic and essential telecom services are moreover regulated by the EU's 2009 telecom framework. Moreover, the level of security and protection for many internet services that some would wish to cover here, is often already governed by commercial contracts and service level agreements between such services and critical infrastructure partners. The digital sector and its clients have the core responsibility to ensure and define the protection of their own services, taking into account the continuously changing threat landscape. Multiple regulations of the same products or services effectively increases red tape but reduces security.

Avoid new data protection risks

Inclusion of broader information society services risks unleashing an avalanche of random personal data for often struggling regulatory agencies. The incident reporting requirement for information society services would cover broad range of IT vendors that would be required to individually report incident data (including random personal customer data) to national authorities at an unprecedented scale. Such massive reporting, and often double-reporting, to poorly resourced authorities would expose citizens' personal data to unnecessary risk at no significant security benefits.

Pay attention to global approaches

Other key regions with which we compete and compare ourselves are pursuing a different approach based on business-driven cybersecurity risk management, market accountability, and innovation. Europe must take note of such emerging global security frameworks. Relying entirely on a regulatory approach would burden Europe's digital industry and take resources away from companies' proactive security management. It would also decrease European competitiveness relative to the our global competitors.

We thank you for considering our suggestions. We stand at your disposal for additional information in support of your important work.

James Waterworth

Vice President
CCIA Europe