ISPA Response to DCMS Consultation on the Network and Information Systems (NIS) Directive.

Introduction

The Internet Services Providers' Association (ISPA) welcomes the opportunity to respond to this DCMS consultation on the Network and Information Systems (NIS) Directive. ISPA is a trade body representing approximately 200 ISPs of various sizes, ranging from SMEs (who account for 90% of our membership) to large multinational corporations, and covers the whole Internet value chain, including access, hosting and content.

Security is a priority issue for the Internet industry. It is an integral part of our members business and company reputation, and CSPs have been consistently working with existing bodies to continue to build protection within their systems. This includes through formal regulations that go beyond the requirements of NIS – such as the Framework Directive and the Privacy and Electronic Communications Regulations – but also best practice or voluntary measures, such as work with the National Cyber Security Centre and ISO accreditation.

In our response to this consultation ISPA is calling for Government to take a proportionate and consistent approach so as not to unnecessarily burden providers not thought to be the 'most important operators' and who are already dealing with a patchwork of regulations in the cyber security space. As the consultation covers a broad range of areas, this response focuses on the aspects which affect ISPA members most keenly and does not address questions directed at more traditional OES as defined by the Directive. Our concerns largely surround issues that arise from the new obligations placed on Digital Infrastructure Providers and Digital Service Providers, namely:

1. The threshold for DNS service providers should be reviewed to only capture the most important operators in each sector
2. The scope of cloud computing services remains unclear and should be narrowed down

Essential Service Definitions

DNS service provider definition

Annex 1 defines the threshold for DNS service providers as "Operators who provide DNS resolution and who service an average of 60 million queries or more in 24 hours." Having discussed this threshold with members that operate their own DNS service, we are concerned that this is likely to bring many small, medium sized and niche members into the scope of the

regulations. This is despite the consultation's clear intention to include only 'the most important operators in each sector'. Furthermore, the number of DNS requests processed is only likely to increase over time and there are other technical considerations around different types of DNS.

We would urge Government to review this threshold by either substantially raising the number of queries processed or by using another means of determining who is in scope. We would be happy to help Government work through this important point as part of the consultation exercise and before regulations are laid.

National Framework

ISPA agrees with a multicompetent authority approach, and the appointment of the NRA with the most experience and expertise in each sector. We have no issue with the ICO having authority for DSPs and Ofcom having responsibility for Digital Infrastructure Providers as this builds on the existing regulatory framework. We are conscious, however, that the current cyber security and data protection landscape is already crowded with regulatory bodies and NIS introduces new powers to request data, issue binding instructions and fines. The ICO, Ofcom, DCMS and NCSC are active in regulating our members in this area, and ISPA suggests that keen attention is made to harmonise asks on businesses to avoid duplication and confusion.

Security requirements

ISPA welcomes the consultation's approach to security requirements based on high-level principles that will then be finalised by the relevant competent authorities, as opposed to a blanket approach which would be unfeasible and inflexible across all sectors. The ENISA guidance for Electronic Communications Providers in the Telecoms Framework Directive highlights the need to maintain this flexibility and harmonise requirements across regulators and international boundaries. We would strongly encourage the Government to continue this approach to allow providers to implement effective and appropriate measures within their businesses according to principles, rather than descending into a 'tick-box' exercise.

Incident reporting

While we recognise the importance of incident reporting which is at the heart of NIS, it is clearly important to ensure that all requirements are in line with existing demands to minimise the regulatory burden and encourage efficiency in reporting or resolving incidents. We welcome the fact that further detail on the definition of a 'significant impact' will follow sector

specific consultation as it remains unclear. We further welcome the bid to align NIS with the reporting requirements under GDPR, and understand the designation of the NCSC as the reporting body for all DSPs and OES across the directive. There is an argument to be made, however, for further harmonisation of reporting requirements across regulations in the future. This would aid further streamlining and reduce the considerable administrative burden involved in reporting incidents to multiple authorities. The passing of NIS and the GDPR in 2018, in addition to existing requirements under the Framework Directive and PECR, means there is a real risk of duplication of reporting.

Digital Service Providers

The creation of a new category of Digital Service Providers (DSPs) needs to be implemented carefully and proportionately and we have identified several ways in which we feel it could be strengthened. Furthermore, among our members are a number of pan-European providers, as such, ISPA looks for consistency across all member states in the definition of DSP services included in this regulation. We would welcome the opportunity to take part in the further targeted consultation on this issue.

Definition of Cloud Computing Services

The Directive defines a cloud computing service as a "digital service that enables a scalable and elastic pool of shareable computing resources". Whilst the definitions included in the consultation go some way to clarify this definition, the current drafting is too broad. For instance, a number of our business-to-business ISP members that resell cloud services could be brought into scope. We do not feel the directive should apply to resellers of services, instead it should only apply to significant cloud operators that operate and own their own infrastructure. We would welcome clarification from Government on this point.

Thresholds for smaller DSPs

We seek greater clarity from Government on the proposed thresholds designed to exclude smaller DSPs. Currently the thresholds are set at 50 employees and a turnover of €10m. In order to achieve the aim of excluding smaller DSPs such as small cloud providers, we strongly urge Government to define this as 'relevant' turnover/employees (i.e. only revenue generated from digital services), and to be turnover/employees within the UK. Without such clarification, there is a risk that the scope of the definition will inadvertently capture a large proportion of small DSPs who would find the requirements unduly burdensome.

Light touch approach

While we recognise that the directive applies in a lighter touch manner after an incident has occurred and only applies to companies with turnover of 10m euros, Government could still go further in minimising the impact of the regulation. Although Government is committed to a more lenient approach to enforcement, DSPs are still required to adhere to the 72-hour reporting threshold and are subject to the same level of fines. ISPA would argue that more proportionate measures appropriate to an actual 'lighter touch' would be warranted.

Penalties

ISPA understands from the consultation that penalties will only be used in extreme circumstances as a "last resort", and will not be used without significant warning. Given the unpredictability of the cyber threat, regardless of measures in place to mitigate the risk, it is important that a flexible approach is taken to enforcement. Penalties should only be pursued where there is deemed to be "intentional" negligence. Further to earlier points made on harmonisation across different regulations and regulatory bodies, ISPA would strongly encourage the Government to make provisions for a scenario where a company is subject to a breach that contravenes multiple pieces of regulation - for example NIS, GDPR and the Framework Directive – which are overseen by multiple bodies and all entail their own penalties. In this scenario, it would be entirely counter-productive and disproportionate for a business to receive multiple fines, and, as such, the Government should ensure that these penalties would not be cumulative.