Andrews & Arnold Ltd
Enterprise Court
Downmill Road
BRACKNELL
RG12 1QS

4th September 2017

# Response of Andrews & Arnold Limited to DDCMS's public consultation on the security network and information systems

Andrews & Arnold Limited welcomes DDCMS's consultation on the security network and information systems.

## About Andrews & Arnold

Andrews & Arnold is a small UK-based communications provider, offering high quality and specialised services to consumers and businesses throughout the UK. Andrews & Arnold provides broadband, mobile and VoIP services, as well as advanced routers and firewalls.

More information is available at http://aa.net.uk.

## The potential impact of the Regulations and small businesses

As an introductory point, we note that, if we were required to adhere to the obligations envisaged in the consultation, we would be faced with a considerable additional regulatory burden, and a considerable increase in the cost of operating.

We are concerned that, while made in the name of ensuring reliability of key infrastructure, excessive burdens could lead to smaller providers being forced out of business, increasing reliance on other ISPs. Overall, this seems undesirable.

## Essential services (questions 1 and 2)

### DNS Service Providers

We are concerned by your proposal to define Domain Name Services (DNS) Service Providers" as "Operators who provide DNS resolution and who service an average of 60 million queries or more in 24 hours."

Our main concern is that your proposal appears to include providers of recursive DNS, rather than just providers of root and authoritative DNS services.

We note that, by virtue of its definition of "domain name system (DNS)" in Article 4(14), the directive appears to impose obligations only on providers of those parts of the DNS infrastructure which "refer queries", thereby covering only providers of root and authoritative DNS services.

This narrower approach to the scope of DNS providers is in keeping with the context of the directive, targeting those operators whose reliability and security are essential to economic and societal activities.

A provider of recursive DNS services is unlikely to be "essential" for either of those purposes, on the basis that, if a subscriber's chosen recursive DNS provider should fall away, it is a matter of a few clicks to change to use a different recursive DNS provider, with no noticeable difference in user experience. There is unlikely to be any significant disruptive effect.

More worryingly, if the obligations applicable to essential services providers are imposed on smaller companies operating recursive DNS services, there is a reasonable likelihood that they will cease to operate rather than attempt to bear the cost associated with the increased regulation.

This would have the effect of decreasing the number of providers available to users and increasing the number of users of the remaining providers: a failure would impact more users, and those impacted users would have fewer other providers to remove to. This would seem to be weakening of the status quo, rather than a strengthening.

If removing recursive DNS providers is not considered to be a viable option, on the basis of the (small) inconvenience associated with moving providers, we would welcome an increase in the proposed 60 million queries or more in 24 hours to a considerably greater figure per 24 hour period, to ensure that the only providers in scope are those where the effect of a failure would be felt by a significant number of end users.

Additionally, you might consider an approach of having the threshold as so many queries per server per period, rather than simply per period. This is likely to incentivise ISPs to operate an increased number of servers, so that no server exceeds the threshold, and, in doing so, further improve resiliency and redundancy.

We also note that the proposed definition is not limited to providers located in the UK; we do not know how many end users of the Internet in the UK use an overseas DNS provider, but persuading an overseas provider to accept obligations arising from being a critical infrastructure provider to UK end users might be challenging.

**Other, more essential, actors are omitted**

We note that proposals do not appear to cover other services and facilities, where disruption could have major ramifications to the provision of Internet access services.

For example, as was experienced recently in Japan, an accidental BGP leak could result in considerable problems.[1] Of course, addressing this would be a huge challenge to address, as a lot of relevant providers will be outside UK.

Similarly, someone intent on disrupting Internet access in the United Kingdom would do well to look at key data centre / co-location facilities, such as Telehouse and Telecity, as we feel that someone could cause catastrophic disruption by attacking these facilities.

It is our understanding that both of these fall outside the scope of the communications regulatory framework, and its security and resiliency obligations.

### Scope of obligations

We note that none of the obligations proposed in Annex 3 relate to the ongoing operation of the services in question. We suspect that the biggest risk for most users is the financial stability of the operator, and its ability to simply decide to no longer provide the services in question. In terms of ensuring integrity and resiliency, these would appear to be key factors.

## Digital service providers (questions 17 - 20)

### Online search engines

As we do not operate in this space, we do not intend to make detailed comment, but we note that your proposed definition is “a digital service that allows users to perform searches of all websites or websites in a particular language”.

As no search engine covers “all websites”, we doubt that any search provider would be caught by this definition.

It might be more appropriate to refer to providers who offer search services over the Internet (as opposed to those offered over a private network, such as a corporate intranet), perhaps with a reference to a volume of search queries in a period.

### Cloud computing services

Our primary concern is that the proposed definition of “cloud computing services” appears to go considerably further than is required by the directive.

The directive defines “cloud computing service” as “a digital service that enables access to a scalable and elastic pool of shareable computing resources”.

Recital 17 expands on this, providing that:

> “Those computing resources include resources such as networks, servers or other infrastructure, storage, applications and services. The term ‘scalable’ refers to computing resources that are flexibly allocated by the cloud service provider, irrespective of the geographical location of the resources, in order to handle

[1] https://bgpmon.net/bgp-leak-causing-internet-outages-in-japan-and-beyond/

> fluctuations in demand. The term 'elastic pool' is used to describe those computing resources that are provisioned and released according to demand in order to rapidly increase and decrease resources available depending on workload. The term 'shareable' is used to describe those computing resources that are provided to multiple users who share a common access to the service, but where the processing is carried out separately for each user, although the service is provided from the same electronic equipment."

Based on this definition, we understand why you propose to include both IaaS and Paas services within the scope of the Regulations.

We do not read the definition as requiring the UK to include SaaS within the definition of "digital service providers". As currently drafted, your proposed definition would appear to include anyone who meets the minimum size threshold who offered a business access to an email, VoIP, or instant messaging server.

If this is what is intended, it strikes us as going too far in terms of its scope. If it is not what is intended, the lack of clarity is likely to be problematic from the perspective of self-identification: if a provider cannot tell with ease whether they are caught by the Regulations or not, the definition is insufficiently clear.

In this regard, we are wary of the term "business to business". Does this cover providers who only sell to other businesses? Or does it apply to providers who sell to both business and consumers? Or is it intended to apply to all providers other than whose who sell exclusively to consumers?

**Other digital service providers**

We note that you are not proposing to include within the scope of obligations companies which provide DDoS mitigation and proxying services, even though these appear to be used widely. An outage suffered by the major providers of these services could well have a substantial impact on the availability of many services on the Internet.