# Regulating Cyber: the UK's plans for the NIS Directive

September 2017

**If you are a digital service provider or operate an 'essential service' then new security and breach notification obligations may soon apply to you. As the UK gets ready to implement the European Security of Network and Information Systems (or NIS) Directive into UK law, the Government has set out its plans for how this new regime will operate, and who will be caught by its reach.**

Last month the Government published a consultation seeking views on its plans to implement the NIS Directive into UK law. Member States have until next May to transpose the Directive into domestic legislation.

The consultation, which closes on 30th September, seeks views on both the Government's proposals, and whether its plans will impose additional costs and burdens on UK organisations. It is therefore of interest to organisations which may be caught by the new regime.

The consultation describes the UK's current plans regarding:

1. essential services that will be covered – omitting banking and financial market infrastructures from the list of sectors contained in the Directive;

2. UK institutions required by the NIS regime, including the competent authorities that will regulate specific sectors – the Government has suggested nominating multiple sector-based competent authorities;

3. security measures the Government proposes to impose and the timelines for incident reporting – the consultation includes high level security principles;

4. the impact of the new regime on "Digital Service Providers"; and

5. penalties – the consultation suggests GDPR-style fines.

In this article, we will look at these points in turn, comparing the Government's proposals with the requirements of the Directive.

## 1. Essential Services

The Directive requires the Government, by 9th November 2018, to identify "operators of essential services" (OES) established in the UK. Those identified as OES will need to comply with the security and incident reporting requirements set out in the Directive.

### Criteria

The Directive defines OES as entities 'of a type referred to in Annex II' which meet the following criteria:

- the entity provides a service which is essential for the maintenance of critical societal and/or economic activities;

- the provision of that service depends on network and information systems; and

- an incident affecting those systems would have significant disruptive effects on the provision of that service.

Annex II lists the sectors, sub-sectors and types of entity that are within the scope.

In the consultation, the Government has proposed its own approach to determine these operators, using the following four criteria:

- sector - the broad part of the UK's economy (listed in the box on the right);
- subsector - specific elements within an individual sector;
- essential service – describing the specific type of service; and
- identification thresholds – criteria to identify essential operators (e.g. size, or the impact of an incident).

While, in effect, there are many similarities with the Directive's approach, there are some significant differences worth noting. First, banking and financial market infrastructures, listed as sectors in the Directive, are omitted from the planned UK sectors (discussed further below). Second, the Government has introduced thresholds to capture only the most important players in a sector. For example, in the transport sector, the owner or operator of an aerodrome is only caught if annual terminal passenger numbers exceed 10 million (and more examples can be found in Annex 1 of the consultation, which lists the proposed sectors, subsectors, essential services and identification thresholds). The thresholds are intended to apply throughout the UK, although the Government is engaging separately with the Devolved Administrations on thresholds, and implementation generally. It also plans to retain a limited 'reserve power' to designate specific operators as OES where they fall outside the proposed thresholds but still provide an essential service.

**UK Sectors for OES:**

- Drinking water supply and distribution
- Energy
- Digital infrastructure
- Health
- Transport

### Banking and financial market infrastructures

The Government is proposing to exempt banking and financial market infrastructures sectors from aspects of the Directive where "equivalent provisions" already exist. This is despite the fact that OES in these sectors are specifically identified in the Directive as being within scope, although the Directive does also provide for sector specific legislation to take precedence where it provides equivalent protection. It will consequently not identify OES or competent authorities for these sectors "given provisions at least equivalent to those specified in the Directive will already exist by the time the Directive comes into force." Instead, such organisations must continue to adhere to requirements and standards set by the Bank of England and/or the Financial Conduct Authority.

This approach can be understood in light of an amalgam of ongoing international, EU and UK

regulatory initiatives on the cyber-resilience of financial services firms and market infrastructures. Depending on the nature of the firm, these might involve participating in the CBEST framework, adhering to requirements in the Financial Conduct Authority Handbook (on the effective management of risk and controls, business continuity and outsourcing and the notification to regulators of material cyber incidents, among other things), allocating a Chief Operations senior manager function to an individual with responsibility for a firm's operations and technology, or complying with the Guidance on cyber-resilience for financial market infrastructures published by the Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions.

## 2. NIS institutions

The UK must put in place a framework of institutions to facilitate the operation of the Directive. This includes adopting a national strategy, and the Government published the UK Cyber Security Strategy last November. The UK must also appoint one or more competent authorities (to oversee implementation and compliance), a single point of contact (to liaise with other Member States) and computer security incident response team(s) (CSIRTs).

Rather than nominate a single national competent authority, the Government's preferred option is to appoint multiple sector-based competent authorities. These include Defra, BEIS, Ofcom, the Departments of Health and Transport and the ICO. In its view they can use their sectoral expertise to improve security in individual sectors. Support (including technical support) would be provided by the National Cyber Security Centre (NCSC), which would also serve as the UK's single point of contact and CSIRT.

## 3. Security and incident reporting: OES

### Security measures for OES

Under the Directive, Member States must ensure that OES take:

- appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems in the provision of their service; and

- appropriate measures to prevent and minimise the impact of the incidents affecting the security of the network and information systems used in the provision of their service.

The Government proposes a guidance and principles based approach to security, setting out high level principles prescribing the mandatory security outcomes OES must achieve (a draft of which is attached to the consultation). These will be supplemented by:

- generic cross-sector guidance (including a Cyber Assessment Framework) that the NCSC will publish in January 2018; and

- information from competent authorities on how to interpret the generic guidance (due in Spring 2018) and sector-specific guidance (due in November 2018).

The consultation states that OES will be expected to meet the high level principles from 10th May 2018, and speak with their competent authority if there are any problems with doing so.

### Incident reporting for OES

The Directive requires OES to notify their competent authority or CSIRT of incidents having a significant impact on the continuity of the essential services they provide. 'Incidents' are defined, and the Directive also sets out criteria to help determine the significance of the impact of an incident.

In the consultation, the Government sets out its proposals for how incident reporting could work in the UK, suggesting that:

- all NIS incident reporting will be to the UK's CSIRT, the NCSC. It also reminds organisations that incidents are not limited to cyber incidents – physical issues such as power failures may also be relevant;
- it hopes (after this consultation) to start defining sector-specific thresholds for what constitutes a 'significant impact';
- incident reporting timeframes will align with the GDPR (reporting without undue delay and no later than 72 hours after becoming aware of an incident) – the Directive only requires reporting "without undue delay"; and
- NIS incident reporting is not intended to replace other (voluntary or mandatory) reporting regimes, or take the place of OES seeking advice from the NCSC or competent authority in the event of an incident.

## 4. Digital Service Providers (DSP)

While Member States must identify OES based on certain criteria, there is no such requirement for DSP. They are already defined in the Directive as any person that provides a digital service. They include online marketplaces, online search engines and cloud computing service providers, and smaller players (e.g. those employing fewer than 50 persons or with an annual turnover/balance sheet which does not exceed €10 million) are excluded from scope. However, in the consultation, the Government asks if DSP are able to identify themselves using this information.

### Security and incident reporting for DSP

The Government plans to adopt a principles and guidance approach to security for DSP, as with OES, but plans to link the guidance closely to that provided by ENISA (the European Network and Information Security Agency). To reduce the burden on DSP it will also set high level security principles which will closely align to the GDPR and the Commission's incident reporting framework for DSP. The Commission was due to have produced this by 9th August (although, at the time of publication, this has not been published).

In relation to incident reporting, the same approach is planned for both DSP and OES.

## 5. Penalty regime

The Directive requires Member States to lay down effective, proportionate and dissuasive penalties for infringements. The UK's proposals are to adopt GDPR-style fines, which it says will provide consistency with the Government's overall regulatory approach towards cyber security. As with the GDPR, there will be two bands for fines. These are:

- band one: €10m or 2% of global turnover for 'lesser offences' such as failure to report a

reportable incident or cooperate with a competent authority; and

- band two: €20m or 4% of global turnover for failure to implement appropriate and proportionate security measures.

Despite the Government's drive for consistency, these bands create one significant difference: a breach of security obligations under the NIS regime could result in a higher fine than under the GDPR (which only applies the lower €10m or 2% threshold to breaches of the security obligations). This may reflect the Government's concerns regarding "the theoretically high impact of a loss of an 'essential service', including possible loss of life…or major economic loss."[1] Alternatively, it may be an oversight that is flushed out following the consultation. It is also currently unclear whether organisations may face multiple fines (for example under the GDPR and NIS regimes – with the former relating to loss of data and the latter loss of service).

The consultation confirms that fines should only be levelled as a last resort, where appropriate risk mitigation measures were lacking, and the figures listed in the bands are maximum amounts for use in only the most egregious incidents. It also clarifies that competent authorities will notify operators (OES or DSP) of impending enforcement action, and that decisions will be enforceable by civil proceedings and appealable through the courts.

## Next steps

Member States have until 9th May 2018 to transpose the Directive into domestic legislation, and the new measures shall apply from 10th May. The Government has also confirmed that it intends this legislation to stay on the books following Brexit, seeing it as supporting the 'Defend' strand of the UK's three pronged (Defend, Deter, Develop) National Cyber Strategy.

In the shorter term, we should know by early December whether the proposals in the consultation will be followed, as the Government has promised to issue a formal response to the consultation within 10 weeks of its closing date. This timing is tight, giving those affected by the NIS regime less than six months to prepare before the Directive applies. Organisations who may be caught, or who supply services to OES or DSP, should therefore start preparations now.

[1] Page 25 of the DCMS Public Consultation "Security of Network and Information Systems (August 2017)

*This article was written by Duncan Blaikie, Ben Kingsley and Natalie Donovan of Slaughter and May's Cyber Team.*

*In our cyber advisory unit we have experts from across the firm helping clients understand and mitigate cyber risks, and prepare for and respond to cyber-attacks.*

*For further information, please contact your usual Slaughter and May contact, or any of the following:*

Duncan Blaikie
T +44 (0)20 7090 4275
E duncan.blaikie@slaughterandmay.com

Ben Kingsley
T +44 (0)20 7090 3169
E ben.kingsley@slaughterandmay.com

Natalie Donovan
T +44 (0)20 7090 4058
E natalie.donovan@slaughterandmay.com



**DateSeptember 2017d September 2017**

546643409