Department for Digital, Culture Media & Sport

The Security of Network and Information Systems Directive

Public Consultation

What is NIS?

- On 6 July 2016 European Parliament adopted the Directive on Security of Network and Information Systems (NIS).
- First EU-wide rules on cyber security. Legally requires essential services to have adequate cyber security safeguards, cyber risk management and report when significant incidents take place.
- Similar but lighter requirements for certain Digital Service Providers
- Member States have until 9 May 2018 to implement.

Who is in scope?

Essential Services

Water, Energy, Transport, Health, Digital Infrastructure (TLDs, IXPs, DNS)

Banking and Finance excluded under UK proposals (similar legislation exists in UK)

Digital Service Providers

Online Marketplaces, Search Engines, Cloud Service Providers (with 50 or more staff and/or a turnover of €10m a year)

Public consultation

- The Government wants to hear the views of industry on these proposals. Important that we get these right.
- Cyber security threat is increasing. Companies in all walks of life need to be more active in their cyber defence.
- Loss of an essential service or a Digital Service Provider will have an impact - either on the country or on other businesses.
- Want to find the correct balance between ensuring the security of our essential services and digital service providers, and avoiding undue burdens on business.

Public consultation (cont.)

UK Government launched a public consultation on 8 August, setting out its proposed approach to implementation. Consultation closes on 30 September. Consultation covers:

- Identification of Essential Services (thresholds)
- National Framework (who regulates)
- Security Measures
- Incident reporting
- Digital Service Providers
- Penalties

What about Brexit?

- Cyber security remains a top priority for the Government.
- It is important to ensure the cyber security of our essential services is maintained, irrespective of EU Membership.
- It is therefore the UK Government’s intention to keep this legislation post Brexit.

NIS - the detail

As previously mentioned, there are six key areas we are seeking your views:

- Identification of Essential Services (thresholds)
- National Framework (who regulates)
- Security Measures
- Incident reporting
- Digital Service Providers
- Penalties

Identification of Essential Services

- The UK must identify “operators of essential services” (OES). OES will be required to comply with the requirements of the Directive.

- Have set out a number of thresholds in the consultation. Important that thresholds are set at an appropriate level.

  Question: Are the identification thresholds set at a level that captures the most important operators in your sector based on their potential to cause a significant disruptive effect if disrupted?

National Framework

- The UK needs to put in place a national (that is to say UK wide) framework of institutions to facilitate the operation of the Directive. This national includes:

    - a national strategy;
    - a competent authority (or authorities);
    - a single point of contact; and
    - computer security incident response teams (CSIRTs).

National Framework (cont.)

- National Strategy will be the UK's Cyber Security Strategy, published in November 2016
- Propose that the CSIRT and single point of contact will be the NCSC
- Propose that we will have multiple competent authorities - where possible using existing regulators.

Question: Do you agree with the government's proposed approach of adopting a multiple competent authority model?

Question: Is the proposed competent authority for your sector a suitable choice?

Security Measures

- Operators of essential services must:
    - 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
    - take appropriate measures to prevent and minimise the impact of the incidents affecting the the security of the network and information systems used in the provision of their service.

Security Measures (cont.)

- The UK Government proposes to take a guidance and principles approach. T Consultation contains a set out the high level security principles. These will be complemented by more detailed guidance..

- These principles describe the mandatory security outcomes that all operators will be required to achieve. The generic and sector specific guidance will be issued by the NCSC and competent authorities over time, and will be updated as necessary to reflect the nature of the threats to network and information systems.

Security Measures (cont.)

Question: Do these high level principles cover the right aspects of network and information systems security to ensure that risks will be appropriately managed?

Question: Will these principles would impose any additional costs on designated operators, or on the sectors in scope as a whole?

Question: what do you consider would be the anticipated resource implication on designated operators, or on the industry as a whole of meeting these principles?

Question: Do you have any plans to make additional security related investments as a result of this Directive?

Incident Reporting

- OES must notify their relevant competent authority or CSIRT of incidents having a significant impact on the continuity of the essential services they provide.

- The Government considers that there is an impact on continuity where there is a loss, reduction or impairment of an essential service. OES encouraged to voluntarily report incidents that do not impact continuity of service.

- OES must report an incident "*without undue delay and as soon as possible, at a maximum no later than 72 hours after having become aware of an incident.*"

Incident Reporting (cont.)

- *Question: Do you consider these incident reporting proposals to be reasonable to ensure that serious incidents affecting the network and information systems of essential services are reported?*

- *Question: If not, can you suggest revised incident reporting proposals that ensure serious incidents are reported?*

- *Question: Do you consider that the proposed timeframe for providing incident reports place an undue burden on designated operators of essential services?*

Digital Service Providers (Definitions)

- Online marketplaces - a platform that acts as an intermediary between buyers and sellers, facilitating the sale of goods and services.

- Online search engines -a digital service that allows users to perform searches of all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found.

- Cloud computing services - any company that offers: ‘Infrastructure as a Service’ (IaaS); ‘Platform as a Service’ (PaaS);Business to Business ‘Software as as Service’ (SaaS).

Digital Service Providers (Definitions)

Question: Are Digital Service Providers easily able to identify themselves using these criteria?

Question: Would using these definitions create any unfair competitive advantage or disadvantage for Digital Service Providers within scope?

Digital Service Providers (Security Measures)

- DSPs must identify, and take appropriate and proportionate technical and organisational measures, to manage the risks posed to their security of network and information systems.

- Propose to follow a principles and guidance approach to security measures for Digital Service Providers, with the guidance closely linked to that provided by the European Network and Information Security Agency (ENISA).

- Compliance with European guidelines will be a requirement for access to the Single Market, therefore the Government will aim to ensure that the UK's guidance is a close to ENISA's guidance as possible.

Digital Service Providers (Security Measures)

A. proportionate security measures in place to protect services and systems from cyber-attack or systems failure;

B. appropriate organisational structures, policies, and processes in place to understand, assess and systematically manage incidents;

C. capabilities to minimise the impacts of a cyber security incidents on the delivery of services including the restoration of those services;

D. capabilities to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect, services;

E. measures in place are, where possible, compatible or comparable to

Digital Service Providers (Security Measures)

Question: Are these principles reasonable?

Question: If NO, Why Not? Can you suggest revised principles that would enable important incidents to be reported?

Question: What would be the impact on your business in applying these principles?

Question: Do you have an alternative preferred approach?

Digital Service Providers (Incident Reporting)

- The Government is proposing that companies must report an incident "*without undue delay and as soon as possible, at a maximum no later than 72 hours after having become aware of it.*"

Question: Would this incident reporting timeframe place an undue burden on your business or operations?

Question: Do you wish to take part in the proposed targeted consultation exercise once the security and incident reporting thresholds have become clearer?

Penalties

- Penalties provided for in national legislation should be effective, proportionate and dissuasive.

- Given the theoretically high impact of a loss of an “essential service”, including possible loss of life or major economic loss to associated industry or regions, the Government believes that the NIS Directive needs to set a high bar for the maximum level of penalty.

- Therefore propose to adopt an approach for the penalty regime for NIS similar to that of the General Data Protection Regulation (GDPR). This will provide consistency in the Government’s regulatory approach towards overall cyber security.

Penalties (cont.)

- The Government proposes to have two bands of penalties under the NIS Directive:

  Band one - set at a maximum €10m or 2% of global turnover - for lesser offences, such as failure to cooperate with the competent authority, failure to report a reportable incident, failure to comply with an instruction from the competent authority.

  Band two - set at a maximum of €20m or 4% (whichever is greater) - for failure to implement appropriate and proportionate security measures.

Penalties (cont.)

- *Question: Do you consider the proposed penalty regime to be proportionate to the risk of disruptions to operators of essential services?*

- *Question: Do you believe that the proposed penalty regime will achieve the outcome of ensuring operators take action to ensure they have the resources, skills, systems and processes in place to ensure the security of their network and information systems?*

- *Question: If you answered NO to either of these two questions, please explain how the penalty regime could be amended to address your concerns.*

What next?

- End of public consultation - 30 September 2017
- Response to consultation - November 2017
- Updated Impact Assessment - November 2017
- Review draft legislation - September - December 2017
- Parliamentary clearance & prepare guidance- Winter 2017 to Spring 2018
- Comes into force - May 2018

Department for Digital, Culture Media & Sport

Stuart Peters
Head of EU Cyber Security Regulatory Policy
4th Floor, 100 Parliament Street,
London SW1A 2BQ
stuart.peters@culture.gov.uk
| 020 7211 6769 | 07926 964308
@dcms /dcmsgovuk | www.gov.uk/dcms