**EXPLANATORY MEMORANDUM TO**

**THE NETWORK AND INFORMATION SYSTEMS REGULATIONS 2018**

**2018 No. 506**

## 1. Introduction

1.1 This explanatory memorandum has been prepared by the Department of Digital, Culture, Media and Sport and is laid before Parliament by Command of Her Majesty.

1.2 This memorandum contains information for the Joint Committee on Statutory Instruments.

## 2. Purpose of the instrument

2.1 To establish a legal framework to ensure that essential services and selected digital service providers within the UK put in place adequate measures to improve the security of their network and information systems, with a particular focus on those services which if disrupted, could potentially cause significant damage to the UK's economy, society and individuals' welfare; and to ensure serious incidents are promptly reported to the competent authorities.

## 3. Matters of special interest to Parliament

***Matters of special interest to the Joint Committee on Statutory Instruments.***

3.1 The JCSI will note that these Regulations breach the 21-day rule. The Department attempted to lay the Regulations on the deadline day of 19 April, but unfortunately delays in signing and finalising the Regulations meant that by the time the Regulations were ready for laying, both Houses had risen. The Department is therefore laying at the first opportunity the following day. As these Regulations are required to come into force from 10 May 2018 in order to meet the UK's European Union legal obligations (set out in paragraph 4.1 below) it is necessary to breach the 21-day rule.

***Other matters of interest to the House of Commons***

3.2 As this instrument is subject to negative resolution procedure and has not been prayed against, consideration as to whether there are other matters of interest to the House of Commons does not arise at this stage.

## 4. Legislative Context

4.1 These Regulations are being made to implement a European obligation, namely implementation of the Directive on Security of Network and Information Systems ((EU) 2016/1148), known as the NIS Directive. Member States have until 9 May 2018 to bring this Directive into their domestic legislation.

4.2 It is important to note that the Government supports the overall aim of the NIS Directive and believes that strengthening the security of network and information systems, and supporting the UK's essential service and digital service providers, is consistent with the Government's aim to ensure the UK is secure and resilient to cyber threats, prosperous and confident in the digital world.

4.3 The National Cyber Security Centre (NCSC) will undertake two roles in these Regulations (see paragraph 7.6), but, in accordance with its legal remit, in its role as CSIRT the NCSC can respond only to cyber security incidents. Although the scope of the Directive covers both cyber and non-cyber incidents the UK, like many Member States, splits responsibilities for cyber and non-cyber incidents across government. We have therefore secured agreement with the Commission and Member States, through the NIS Cooperation Group, that we can transpose the Directive in a way that allows the CSIRT to focus only on cyber attacks provided we ensure that the definitions of an incident remain as set out in the Directive (that is, include both cyber and non cyber incidents) and that operators and digital service providers know where they can seek support for non cyber incidents. We understand that other Member States have taken a similar approach.

4.4 In line with Recital 9 and Article 1(7) of the NIS Directive, and set out in detail in the transposition note, these Regulations have not been applied to the banking sector and the financial market infrastructures sector, as equivalent EU legislation applies.

## 5. Extent and Territorial Application

5.1 The extent of this instrument is the United Kingdom.

5.2 The territorial application of this is the whole of the United Kingdom including the territorial sea adjacent to the UK, the Continental Shelf, the sea (including the seabed and subsoil) in any area designated under section 1(7) of the Continental Shelf Act 1964.

## 6. European Convention on Human Rights

6.1 As the instrument is subject to negative resolution procedure and does not amend primary legislation, no statement is required.

## 7. Policy background

***What is being done and why***

7.1 The UK's modern economy, and the economic security it brings, is based on secure infrastructure. Network and information systems and the essential services they support play a vital role in society, from ensuring the supply of electricity, water, and health services, to the provision of passenger and freight transport. Their reliability and security are essential to economic and societal activity, and the functioning of UK and European markets.

7.2 Such systems can be a target for malicious actors that intend to damage or interrupt their operation through cyber attacks. Some systems may also be single points of failure for essential services and may be susceptible to other forms of compromise such as power failures, hardware failures and environmental hazards. Adverse incidents affecting such systems could cause significant damage to the UK economy, impeding economic activity and undermining user confidence, or result in substantial financial losses or a risk to public safety. The magnitude, frequency and impact of network and information system security incidents is increasing.

7.3 There is a need to therefore improve the security of network and information systems across the UK, with a particular focus on essential services (energy, health, transport, water and digital infrastructure) which if disrupted, could potentially cause significant damage to the UK economy, society and individuals' welfare. Recent events such as

the 2017 WannaCry ransomware attack, the 2016 attacks on US water utilities, and the 2015 attack on Ukraine's electricity network clearly highlight the impact that can result from adversely affected network and information systems.

7.4 Network and information systems also play an essential role in facilitating the cross-border movement of goods, services and people. Given the transnational nature of some of the services provided using such systems, substantial disruptions of those systems, whether intentional or unintentional and regardless of where they occur, can affect other countries as well as the UK.

***How it is being done and why***

7.5 The Government has prioritised using existing resources where possible. It has taken a multiple competent authority approach, rather than establishing a new single national body, to ensure that competent authorities have a detailed understanding of their sectors and to encourage cyber security to become more mainstream.

7.6 The NCSC, which is part of the Government Communications Headquarters (GCHQ), will undertake two of the key roles under the National Framework: the Single Point of Contact and the Computer Security Incident Response Team. As the National Technical Authority for cyber security the NCSC will continue to provide security advice and guidance which will assist both competent authorities and operators of essential services. The NCSC will undertake its responsibilities under these Regulations acting in the exercise of its functions under section 3(1)(b) of the Intelligence Services Act 1994.

7.7 The NCSC will not undertake any regulatory functions and, in its role as the CSIRT, will only respond to incidents which arise as a result of a cyber-attack and have been notified to it by the Competent Authorities. The UK's approach to security duties is to set out a number of sector-agnostic principles that operators of essential services must consider. Each principle describes security outcomes with associated guidance on how these may be achieved. The Government will not set out specific measures that operators must take - the decision on how operators meet the principles is for the operators to take and for competent authorities to assess in line with their published guidance. This approach ensures that decisions on what measures to put in place remains the responsibility of the operator and is able to accommodate sectoral differences.

7.8 Under the Regulations, penalties imposed by national or English Competent Authorities will be paid into the national consolidated fund. Where those penalties have been imposed by Welsh or Scottish Competent Authorities, the penalties will be paid into the Welsh or Scottish consolidated funds. As Northern Ireland's consolidated fund (NICF) does not permit direct payment of fines, the Government will commit to net receipts from Northern Ireland against the money which the Northern Ireland Office pays to the NICF to fund public services in Northern Ireland.

## 8. Consultation outcome

8.1 The Department for Digital, Culture, Media and Sport published a public consultation on its plans to transpose the security of Network and Information Systems Directive into UK law on 8 August 2017. The Department received 358 responses, from respondents in all sectors covered by the Directive, Competent Authorities, legal advisers and the devolved administrations. On 29 January 2018, the Department published its formal response to the public consultation, along with a paper analysing

the responses. These consultation documents can be found at https://www.gov.uk/government/consultations/consultation-on-the-security-of-network-and-information-systems-directive.

8.2 The responses showed that there was broad support for the Government's approach and that in the main, the Government's proposals were thought to be appropriate and proportionate. Respondents highlighted some areas of concern and the Government addressed these through changes to its approach. The main changes that the Government made were to clarify:

- the thresholds required to identify operators of essential services;
- the role of the Competent Authority and how powers may be delegated to agencies;
- that the role of the National Cyber Security Centre is limited to cyber security;
- the expectations on operators within the first year or so; and
- the definitions of Digital Service Providers

8.3 The Government also simplified:

- the incident response regime to separate incident response procedures from incident reporting procedures; and
- the penalty regime slightly, including setting the maximum fine at £17m.

8.4 It is the Government's belief that these changes have provided further reassurance to industry on the impact and implementation of the NIS Directive. The Government's approach is intended to be reasonable, proportionate and appropriate, and the Government and Competent Authorities will work closely with industry to ensure that this legislation will be a success.

## 9. Guidance

9.1 The Government and Competent Authorities are committed to producing substantive guidance to give clarity on how this Regulation will work in practice. The National Cyber Security Centre published guidance (https://www.ncsc.gov.uk/guidance/nis-guidance-collection) on 28 January 2018 to assist Operators of Essential Services in meeting the cyber security requirements set out in these Regulations. Further guidance on how Operators and Competent Authorities can assess whether they meet the security requirements of these Regulations will be published in April 2018.

9.2 The Department of Digital, Culture Media and Sport will publish guidance on its website (https://www.gov.uk/government/organisations/department-for-digital-culture-media-sport) to Competent Authorities on how they should approach regulating these Regulations, setting out the Government's view that their approach should be proactive, engaging with operators in advance of any incident, and that any measures that they take should be appropriate and proportionate. Competent Authorities will publish guidance before May on when Operators of essential Services should report incidents, which will be tailored to individual sectors, along with further guidance on how they will approach regulating these Regulations. It is expected that Competent Authorities will produce further detailed guidance as necessary.

## 10. Impact

10.1 At least 432 businesses will be affected by these Regulations across the five sectors of water, digital infrastructure, energy, health, transport and digital service providers.

The UK energy companies are likely to face limited extra costs, provided the Directive reporting rules are relatively flexible.

10.2 Administrative costs will be incurred by businesses as they familiarise themselves with the legislation and its implications for their firm. Familiarisation cost for large essential services is estimated to be £278,601 while for medium and small businesses they are £12,544 and £1,320 respectively. The estimated total cost of operating the competent authorities is £4,104,035 per year. All associated costs borne by the competent authorities will be passed to businesses.

10.3 The impact on the public sector is primarily on the health sector and other publicly owned essential services. There are 268 estimated number of health sector organisations consists entirely of public organisations across the UK. Any cost borne by these organisations due to the Directive will be counted as costs to government and not included in the business impact target. Organisations in the UK health sector could face limited additional costs, providing the Directive reporting rules are relatively flexible.

10.4 The total set-up costs for implementing these Regulations is £23,410,341 for government, and £32,483,885 for businesses, in year 1. Annual on-going costs to businesses are £21,786,176 (from Year 2) in the best estimate. Costs to government includes £176,931 familiarisation cost, £147,148 compliance cost, £38,262 reporting cost, and £23,048,000 additional cyber security spending.

10.5 An Impact Assessment is submitted with this memorandum and is published alongside the Explanatory Memorandum on the legislation.gov.uk website.

## 11. Regulating small business

11.1 The legislation does not apply to activities that are undertaken by small businesses.

## 12. Monitoring & review

12.1 The Regulations include a provision (regulation 25) to carry out a biennial review of the regulatory provisions incorporated in this legislation. This will be completed by the Secretary of State for Digital, Culture, Media and Sport.

12.2 In addition, the Regulations include provisions (regulation 8) to review the number and nature of the Operators of Essential Services every two years to ensure that they remain relevant, and that the appropriate organisations are included and the organisations incorporated by virtue of these Regulations remain appropriate.

12.3 In addition, the Secretary of State for Digital, Culture, Media and Sport is committed to carrying out a substantive review of the impact of these Regulations, the security measures, scope, and thresholds in 2020 in order to assess their effectiveness and whether any of these provisions need to be amended.

## 13. Contact

13.1 Stuart Peters at the Department for Digital, Culture, Media and Sport, Telephone: 020 7211 6769 or email: stuart.peters@culture.gov.uk can answer any queries regarding the instrument.