EXPLANATORY MEMORANDUM TO

THE NETWORK AND INFORMATION SYSTEMS (AMENDMENT AND TRANSITIONAL PROVISION ETC.) REGULATIONS 2020

2020 No. 1245

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 This instrument makes amendments to the Network and Information Systems Regulations 2018 ("the NIS Regulations") (S.I. 2018/506), which came into force on 10 May 2018.

2.2 The purpose of the amendments is to improve the efficacy and implementation of the NIS Regulations in the United Kingdom. These amendments are primarily based upon the recommendations made in the Post-Implementation Review of the NIS Regulations published in May 2020 which can be found on gov.uk, and subsequently developed in light of evidence provided by UK competent authorities and following the public Call For Views published in August 2020.

2.3 The amendments ensure greater clarity in the legislation, reduce the potential for misinterpretation and strengthen the relationship between competent authorities and operators within scope of the NIS Regulations.

3. Matters of special interest to Parliament

Matters of special interest to the Joint Committee on Statutory Instruments

3.1 None.

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. Extent and Territorial Application

4.1 The extent of this instrument is the United Kingdom.

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

5. European Convention on Human Rights

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

6. Legislative Context

6.1 The NIS Regulations implemented a European obligation, namely implementation of the Directive on Security of Network and Information Systems ((EU) 2016/1148), known as the NIS Directive), under section 2(2) of the European Communities Act 1972. The NIS Regulations set out the legal measures required to boost the overall level of security (both cyber and physical resilience) of network and information systems that are critical for the provision of essential services (transport, energy, water, health and digital infrastructure services) and certain digital service providers (online marketplaces, online search engines, and cloud computing services).

6.2 This instrument further amends the NIS Regulations to give effect to matters arising in relation to the NIS Directive under section 2(2) of the European Communities Act 1972. This power will cease to apply at the end of the Transition Period.

7. Policy background

What is being done and why

7.1 Regulation 25 of the NIS Regulations requires the Government to publish a Post-Implementation Review every two years after the NIS Regulations are laid in Parliament. The purpose of such a review is to examine how operators have fared in implementing the NIS Regulations and identify any issues that have arisen.

7.2 The Government conducted its first review of the NIS Regulations between late 2019 and early 2020. After surveying both operators within scope of the NIS Regulations and competent authorities and carrying out relevant analysis, the Government published the first Post-Implementation Review of the NIS Regulations in May 2020.

7.3 This first Post-Implementation Review showed that whilst overall the NIS Regulations were having a positive effect on the UK's overall cyber resilience and that organisations were taking proactive steps to improve the security of their network and information systems, there were areas that could be improved and the Review included several recommendations.

7.4 This instrument implements the recommendations of the Post-Implementation Review, in order to ensure that the NIS Regulations remain effective and that operators of essential services and relevant digital service providers take adequate and proportionate measures to secure their networks and information systems. The instrument also reflects feedback received from a public Call For Views in September 2020 as well as the views of the competent authorities in the NIS Community, including in the Devolved Administrations.

7.5 The key amendments that the instrument makes are:

Information sharing powers

7.6 This instrument clarifies the ways in which regulatory authorities share information with each other and expands existing provisions to enable competent authorities to share information with law authorities for security purposes and criminal proceedings, provided for in Regulation 6 of the NIS Regulations. This will support wider efforts to

improve collective cyber security, and will give competent authorities more confidence to use information and make more effective decisions to ensure essential services are protected.

Information Notices

7.7 This instrument expands on the grounds for issuing an information notice under Regulation 15 of the NIS Regulations to allow competent authorities to establish whether any actions taken by operators led to an incident which affected their network and information systems. This will help competent authorities to gather relevant and necessary information needed to carry out the full scale of their duties under the NIS Regulations.

Enforcement regime

7.8 Further amendments have been made to Regulation 17 to improve the application of enforcement notices and provide more clarity to organisations in scope in regards to how representations can be made before decisions are reached, in the interest of facilitating transparency and collaboration. This instrument will also make enforcement notices issued by competent authorities enforceable via civil proceedings under Regulation A20 of the NIS Regulations. Competent authorities will be able initiate civil proceedings for appropriate remedies or relief in order to promote compliance with the Regulations rather than relying solely on being able to serve financial penalties. This will allow competent authorities to decide the most appropriate course of action to support operators and digital service providers.

7.9 The instrument also expands the powers of competent authorities under Regulation 16 to carry out inspections and gives inspectors clearer instructions on what they are allowed to do during an inspection. This will help operators better understand how the inspections will apply to them, including how to cooperate accordingly, and provide safeguards on what an inspector may do. There are other smaller changes to Regulation 17, including clarifications that organisations must comply with notices in full and explicitly stating that competent authorities may serve multiple notices at the same time.

Penalty regime

7.10 The instrument further clarifies some of the ambiguities in the original penalty banding regime within Regulation 18 of the NIS Regulations. This will help competent authorities issue penalties which reflect the seriousness of a breach or non-compliance rather than relying solely on the impact of an incident. Competent authorities will be able to issue sector-specific penalties which are less generic to all operators in scope of the NIS Regulations. Penalty notices can also be issued irrespective of whether an enforcement notice has previously been issued, if the situation requires such action, so long as the measures taken are proportionate and reasonable.

7.11 A two-step system is introduced enabling competent authorities to serve a notice of intent to impose a penalty before making their final decision through a penalty notice. This process will allow operators of essential services and relevant digital service providers to submit representations on the proposed penalty decision before the competent authority issues a formal penalty notice. This will reduce the risk of appeals against competent authorities' decisions and provide a more transparent,

equitable, and effective framework based on increased communication between regulated organisations and their competent authorities.

Introducing an Independent Appeals Mechanism

7.12 The instrument introduces a new mechanism for operators of essential services and relevant digital service providers enabling them to appeal decisions made against them (Regulation 19A and 19B) and omits the independent reviewer provisions in Regulation 19. This will ensure that operators have their appeals heard in a transparent and accountable way through a formal judicial process. New regulations 19A and 19B provide for appeals to be heard by the General Regulatory Chamber of the First-tier Tribunal, which already hears appeals under other regulatory frameworks. Regulation 19A specifies the grounds of appeals which will help operators identify how they can challenge decisions made against them whilst Regulation 19B specifies the powers of the General Regulatory Chamber when making their decisions and standards of review.

Timelines for Post-Implementation Reviews

7.13 The timeframes for setting Post-Implementation Reviews (see Regulation 25) of the NIS Regulations will be extended from two years to five, to bring the NIS Regulations in line with common practice for Reviews.

Changes to Schedule 2 of the NIS Regulations

7.14 The amendments to Schedule 2 of the NIS Regulations are mainly tailored around the energy sector, digital infrastructure sector, and health sector in Scotland. They are primarily based on feedback received from the respective competent authorities (BEIS for the Health and Safety Executive, the Scottish Government for the health sector in Scotland and Ofcom for the digital infrastructure sector) as the primary regulators. Changes include definitional revisions, limits on the potential of technical challenge and amendments to further support competent authorities in the designation process. The purpose of these changes is to ensure that the right entities are identified and brought into scope of the NIS Regulations, and the Government does not expect them to expand the scope of the NIS Regulations in any way.

8. European Union (Withdrawal) Act / Withdrawal of the United Kingdom from the European Union

8.1 This instrument does not relate to withdrawal from the European Union or trigger the statement requirements under the European Union (Withdrawal) Act.

9. Consolidation

9.1 There is no current plan to consolidate the legislation.

10. Consultation outcome

10.1 The government launched a Call for Views with industry between August - September 2020 to invite responses to its proposals to change the NIS Regulations. We received a total of 68 responses to the consultation.

10.2 Feedback on the Government's proposals was mixed but broadly positive, with some proposals receiving more widespread support while others being less popular. A full

account of the responses is available in the official Government Response to the Call for Views.

10.3 Principally, some feedback stated that changes are premature as the NIS Regulations are too recent, while others submitted concerns around the broad drafting of information-sharing powers, the apparent lack of safeguards on the powers of inspectors, including the need for limitations on actions which may prejudice organisations, the need to secure data removed from organisations' premises, the possibility of adding further reporting burdens on operators, and the proportionality of penalties in light of the new definition of the financial bands.

10.4 However, feedback also indicated positive support for other changes, such as those on information-sharing (including for criminal proceedings), the inclusion of a new two-stage process for levying financial penalties, and the introduction of a new appeal right to the First-tier Tribunal.

10.5 The Government carefully assessed the contributions made through the Call for Views and made changes to reflect key concerns raised by respondents. The Government believes that the instrument now addresses the majority of the themes emerging from the Call for Views. The response to the consultation can be found on gov.uk.

11. Guidance

11.1 The Government and competent authorities remain committed to ensuring that operators of essential services and relevant digital service providers have relevant guidance on what they need to do in order to fulfil their statutory duties. Once the instrument is laid, competent authorities will be updating their guidance and informing operators within their sector of the new provisions. The Government will help and assist competent authorities with issuing such guidance as necessary.

12. Impact

12.1 The impact on business, charities, or voluntary bodies is very low. There are currently 623 organisations in scope of the NIS Regulations across the five sectors of water, digital infrastructure, energy, health, transport and digital service providers. Most of the costs that will be incurred by operators of essential services and relevant digital service providers as a result of this statutory instrument will be familiarisation costs with the new amendments, which would only occur within the twelve months after the legislation has been enacted.

12.2 The impact on the public sector is very low. The Government assesses that many of the costs associated with the new legislative amendments will be borne by Government Departments, for example, for the creation of an independent appeals process within the First Tier Tribunal.

12.3 An Impact Assessment has not been prepared for this instrument. We anticipate the additional annual costs to business in scope of the NIS Regulations incurred by this instrument to be less than £5 million, as concluded by the Department's own economic assessment, and therefore a full impact assessment is not required.

13. Regulating small business

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

14. Monitoring & review

14.1 In accordance with Regulation 25 of the NIS Regulations, the next Post-Implementation Review of the Regulations will take place by May 2022. After 2022, Post-Implementation Reviews will take place no later than every five years.

15. Contact

15.1 Mihai-Alin Rusu (mihaialin.rusu@dcms.gov.uk), Toby Varian (toby.varian@dcms.gov.uk) and Jessica Howard (jessica.howard@dcms.gov.uk) at the Department for Digital, Culture, Media and Sport, can answer any queries regarding this instrument.

15.2 Emma Green, Deputy Director for Cyber Security at the Department for Digital, Culture, Media and Sport can confirm that this Explanatory Memorandum meets the required standard.

15.3 Matt Warman MP, at the Department for Digital, Culture, Media and Sport can confirm that this Explanatory Memorandum meets the required standard.