House of Commons

European Scrutiny Committee

Seventeenth Report of Session 2022–23

Documents considered by the Committee on 19 April 2023

Report, together with formal minutes

Ordered by The House of Commons
to be printed 19 April 2023

HC 119-xv
Published on 25 April 2023
by authority of the House of Commons

Notes

Numbering of documents

Three separate numbering systems are used in this Report for European Union documents:

Numbers in brackets are the Committee's own reference numbers.

Numbers in the form "5467/05" are Council of Ministers reference numbers. This system is also used by UK Government Departments, by the House of Commons Vote Office and for proceedings in the House.

Numbers preceded by the letters COM or SEC or JOIN are Commission reference numbers.

Where only a Committee number is given, this usually indicates that no official text is available and the Government has submitted an "unnumbered Explanatory Memorandum" discussing what is likely to be included in the document or covering an unofficial text.

Abbreviations used in the headnotes and footnotes

AFSJ	Area of Freedom Security and Justice
CFSP	Common Foreign and Security Policy
CSDP	Common Security and Defence Policy
ECA	European Court of Auditors
ECB	European Central Bank
EEAS	European External Action Service
EM	Explanatory Memorandum (submitted by the Government to the Committee)*
EP	European Parliament
EU	European Union
JHA	Justice and Home Affairs
OJ	Official Journal of the European Communities
QMV	Qualified majority voting
SEM	Supplementary Explanatory Memorandum
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union

Euros

Where figures in euros have been converted to pounds sterling, this is normally at the market rate for the last working day of the previous month.

Further information

Documents recommended by the Committee for debate, together with the times of forthcoming debates (where known), are listed in the European Union Documents list, which is published in the House of Commons Vote Bundle each Monday and is also available on the parliamentary website. Documents awaiting consideration by the Committee are listed in "Remaining Business": www.parliament.uk/escom. The website also contains the Committee's Reports.

*Explanatory Memoranda (EMs) can be downloaded from GOV.UK: https://www.gov.uk/government/collections/explanatory-memoranda-on-eu-documents. EMs can be searched by Council or Commission reference number. Letters from the Committee and those issued by Ministers can be found in the correspondence section of the Committee's website: https://committees.parliament.uk/committee/69/european-scrutiny-committee/publications/3/correspondence/.

Explanatory Memoranda and letters published before 31 March 2022 can be found on the National Archives website—https://webarchive.nationalarchives.gov.uk/search/—by restricting searches to https://europeanmemoranda.cabinetoffice.gov.uk/

Staff

The staff of the Committee are Ravi Abhayaratne (Committee Operations Assistant), Hannah Barlow (Committee Specialist), Joanne Dee (Deputy Counsel for European and International Law), Alistair Dillon and Leigh Gibson (Senior Committee Specialists, European Affairs Unit), Nat Ireton (Committee Operations Officer), Daniel Moeller (Committee Operations Manager), Foeke Noppert (Senior Committee Specialist, European Affairs Unit), Indira Rao MBE (Counsel for European and International Law), Emily Unwin (Deputy Counsel for European and International Law), Dr George Wilson (Clerk).

Contacts

All correspondence should be addressed to the Clerk of the European Scrutiny Committee, House of Commons, London SW1A 0AA. The telephone number for general enquiries is (020) 7219 3292/8185. The Committee's email address is escom@parliament.uk.

Contents

1 Northern Ireland Protocol: Technical standards and the EU Standardisation Strategy (update)[1]

This EU document is politically important because:

- The EU has agreed new legislation that limits the role of non-EU bodies, including the British Standards Institution (BSI), within the European Standardisation Organisations (ESOs). This could impact on UK efforts to influence international standard-setting in strategic areas such as artificial intelligence and hydrogen. In addition, a significant sub-set of technical standards set by the ESOs continue to have direct legal implications in Northern Ireland under the Northern Ireland Protocol.

Action

- Write to the Parliamentary Under Secretary of State at the Department for Business and Trade (Kevin Hollinrake MP) to clarify how the EU proposal may affect the UK's influence over technical standards of relevance to the UK.

Overview

1.1 Standards are technical specifications that companies can use, for a fee, to ensure goods, services, systems, or processes are fit for purpose and in line with industry best practice. They facilitate international trade, by aligning expectations around the quality and safety of particular products even where buyers and sellers are in different jurisdictions. In Europe, the development of standards is principally carried out within the three European Standardisation Organisations (ESOs): the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC) and the European Telecommunications Standards Institute (ETSI). These are independent entities, not agencies or bodies of the EU, but they do have a formalised role in setting standards that underpin EU law and policy.

1.2 In 2022, the EU passed legislation to reduce the formal voting rights of non-EU stakeholders, including from the UK, over certain new ESO technical standards to limit "undue influence of actors from outside the EU [...] during the development of standards for key areas". A reduction in British input within the ESOs, and by the British Standards Institution in particular, is relevant to the UK's interests for two reasons. First, many European standards developed by the ESOs continue to play a direct legal role in Northern Ireland under the EU product legislation that still applies there under the Protocol on Ireland/Northern Ireland (even under the changes to its operation foreseen by the recent

1 Proposal for a Regulation amending Regulation (EU) No 1025/2012 as regards the decisions of European standardisation organisations concerning European standards and European standardisation deliverables; COM(2022) 32; Legal base: Article 114 TFEU; ordinary legislative procedure, QMV; Department: Business and Trade; Devolved Administrations: Consulted; ESC number: 42020.

'Windsor Framework' agreement). Second, Ministers have identified a strategic interest in UK leadership in developing international standards, which could be affected by any reduction in the formal role for UK stakeholders within the ESOs.

The amendment to the EU Standardisation Regulation

1.3 While standards are by definition voluntary, the EU also uses standards developed by the ESOs for regulatory purposes. In particular, the European Commission can formally approve them as 'harmonised standards' under pieces of EU product legislation. Where manufacturers apply a relevant harmonised standard when making a particular good, they are given legal certainty that they are compliant with the associated product requirements under EU law in areas such as safety or environmental performance (known as the 'presumption of conformity').[2] In many cases, relying on harmonised standards makes it easier for producers to pass conformity assessments, and use the EU's 'CE' mark on their goods to facilitate their sale throughout the Single Market.[3] The EU is also planning to use standards in this way to help companies meet new legal requirements relating to emerging digital technologies and services, including artificial intelligence and cyber-security.

1.4 Due to the quasi-legislative role of standards in the EU product safety framework,[4] the ESOs work closely with the EU even though they are independent bodies. This relationship is formalised in the 2012 EU Standardisation Regulation,[5] which sets out the specific procedures for the European Commission to request the ESOs to develop a technical standard in a particular area to supplement EU law and policy.[6] As part of a new Standardisation Strategy for the European Union,[7] which we reported to the House in May 2022,[8] the EU has amended that Regulation to reduce the formal voting rights of non-EU stakeholders over certain new ESO technical standards to limit "undue influence of actors from outside the EU [...] during the development of standards for key areas, like cybersecurity or hydrogen standards".[9] The Commission's proposal was primarily targeted at the telecommunication standards body ETSI, where the private sector—mostly representing American and Chinese commercial interests—has been the dominant

2 The UK broadly speaking retained this approach to the use of standards for its product safety framework for Great Britain after Brexit in its domestic law, although referring to them as 'designated' rather than 'harmonised' standards. Northern Ireland is in a unique position in still applying EU product laws even after Brexit, as discussed in this chapter.

3 The 'CE' mark denotes a manufacturer's acceptance that it has met the relevant product requirements under EU law.

4 The use of standards under EU law was significantly affected by the EU Court of Justice (CJEU) in 2016, when it ruled that harmonised standards "form part of EU law" even though their use remains voluntary. See the judgement in case C-613/14 (James Elliott Construction Limited v Irish Asphalt Limited).

5 Regulation (EU) No 1025/2012 on European standardisation.

6 Each year, the Commission produces a 'Standardisation Work Programme' in which it identifies strategic priorities for European standardisation for the year ahead. Based on this Work Programme, the Commission draws up individual requests for specific standards, which contain requirements the envisaged standard should meet and a deadline for its delivery.

7 European Commission, 'Communication from the Commission: An EU Strategy on Standardisation Setting global standards in support of a resilient, green and digital EU single market' COM(2022) 2 February 2022.

8 European Scrutiny Committee, Second Report (2022–23) HC 119–ii, chapter 1 (25 May 2022).

9 The Regulation, effectively, requires the ESOs to adapt their internal procedures to make them compliant with the EU's new approach.

driver of new standards for digital products and services.[10] However, it applies equally to CEN and CENELEC, where national standardisation bodies, like the British Standards Institution (BSI), are dominant in the decision-making process.[11]

1.5 The amendment to the EU Standardisation Regulation will take effect on 9 July 2023. The legislative change will effectively ban national standardisation bodies and other entities based outside the European Economic Area (which consists of the EU's 27 Member States, plus Norway, Iceland and Liechtenstein) from voting when the ESOs make formal decisions in response to a request by the European Commission for a new technical standard under EU law.[12] They are excluded, in particular, from decisions on whether to accept a request to develop a new standard, and when formally approving a technical standard at the end of the process.[13]

Potential implications for British Standards Institution and other UK stakeholders

1.6 When we considered the EU Standardisation Strategy in more detail in our Second Report of this Session,[14] we concluded that the change to the Standardisation Regulation would affect the UK directly. In particular, the British Standards Institution (BSI), the UK's representative national standardisation body, will from July 2023 be excluded from formal ESO decisions on many new technical standards as described above.[15] Similarly, in ETSI, where industry has historically played a key role, more than 100 British companies and other organisations with membership status will also lose voting rights.[16]

1.7 A reduction in British input within the ESOs, and by the British Standards Institution in particular, is relevant to the UK's interests for two reasons. First, European standards developed by the ESOs continue to play a direct role in Northern Ireland. There, EU legislation on product safety in principle continues to apply automatically under the Protocol on Ireland/Northern Ireland, even after the changes to its operation foreseen under the 'Windsor Framework' recently agreed in principle between the UK and the European Commission. As such, any 'harmonised standards' confer a presumption of

10 This is also reflected in the fact that the European Commission has requested new technical standards relating to artificial intelligence from CEN and CENELEC, relegating ETSI—which might otherwise be seen as the principal. ESO in this field—to a consultative role. See Euractiv, 'Commission leaves European standardisation body out of AI standard-setting' (7 December 2022).

11 In CEN and CENELEC, new standards are developed in sector-specific Technical Committees, where the National Standardisation Bodies (NSBs) of all participating countries—like the BSI for the UK—can send a delegation. Once a standard has been developed, it is formally approved (almost always by consensus, but by weighted votes of the NSBs where necessary). In ETSI, voting rights are available to all members—including industry representatives—and weighted proportional to their financial contribution to the organisation. Collectively, non-EU companies have accrued a majority of voting rights within ETSI.

12 Industry stakeholders have argued that the proposed change itself risks making European standards less influential globally by reducing the involvement of non-EU expertise in their development. See, for example, Digital Europe, 'DigitalEurope comments on the Standardisation Strategy' (April 2022).

13 More specifically, non-EEA NSBs will lose their right to vote on decisions relating to: the acceptance and refusal of standardisation requests by the EU; the acceptance of new work items that are needed for the fulfilment of such requests; and the adoption, revision and withdrawal of European standards or European standardisation deliverables.

14 European Scrutiny Committee, Second Report (2022–23) HC 119–ii, chapter 1 (31 May 2022).

15 The BSI maintained its membership of the ESOs following Brexit (in the case of CEN and CENELEC this required a change to their statutes).

16 There are currently 110 UK-based members of ETSI besides the BSI; they include BT and Vodafone, as well as various public authorities, notably Ofcom, the Home Office, and the National Cyber Security Centre (NCSC). Even so there is still an expectation, but not a strict legal requirement, that the non-EEA NSBs who participate in the ESOs, like the BSI, will implement all new European standards as national standards domestically.

conformity that a product meets the relevant requirements to be on sale in Northern Ireland.[17] In practice, that means that the standards produced by the ESOs in many cases effectively continue to determine the safety and quality characteristics for goods on the market in Northern Ireland.[18] As such, the BSI's continued full involvement in the development new European product safety standards would be optimal.

1.8 Second, there may be longer-term implications for the UK Government's overarching ambitions in relation to international standard-setting, as articulated in a policy paper on the 'Fourth Industrial Revolution' in July 2021.[19] This set out a strategic interest in UK leadership in developing international standards in areas such as artificial intelligence, robotics and hydrogen infrastructure, much like the European Commission did in its Standardisation Strategy. If the BSI's role as the UK's voice in Europe's standardisation fora is diminished, this could affect its "international engagement activities", which the Government explicitly identified as a key part of the UK's ability to "project [its] interests on a global stage".[20] The loss of formal decision-making powers for other British stakeholders when ETSI develops new standards for digital technologies should be seen in a similar light.

1.9 However, the *practical* impact of the EU's amendment on the ability of the BSI and other UK stakeholders to provide their considerable expertise within the three ESOs during the standard-setting process is unclear. It does not appear to restrict their involvement during the actual, technical work to develop new standards, only over formal decisions to direct and approve the ESOs' work. The then-Department for Business, Energy and Industrial Strategy said in its initial Explanatory Memorandum in March 2022 that the BSI "should not be unduly affected" by the changes, not least because the new restrictions on non-EU input relate only to standards developed at the EU's formal request, which only make up 20% of standards produced by the ESOs. However, this Committee concluded standards in that cohort, even if numerically smaller, may be of particular strategic or economic importance to the UK.[21]

Conclusions and action

1.10 The amendment to limit the role of non-EU representatives in the European Standardisation Organisations has now been adopted and will take effect shortly. We have therefore written to the Parliamentary Under Secretary of State at the Department for Business and Trade (Kevin Hollinrake MP) to seek more information on the practical impact of this change on the involvement of the British Standards Institution and other

17 An overview of sectors where the EU uses harmonised standards that remain of relevance to Northern Ireland under the Protocol is shown at the end of this chapter.

18 Moreover, under UK law, any goods on the market in Northern Ireland that meet EU-approved safety standards can be sold freely into Great Britain. This is, however, unlikely to raise any substantive issues unless UK and EU product safety rules for a particular product diverge to the point where an EU harmonised standard would no longer ensure compliance with UK safety rules.

19 Department for Business, Energy and Industrial Strategy, 'Policy paper: Standards for the Fourth Industrial Revolution' (21 July 2021).

20 ibid, p. 16.

21 For example, the BSI and other UK stakeholders will soon have a more limited role in relation to technical standards the EU requests not only in relation to product safety, but also under its new legislation relating to artificial intelligence, hydrogen and cyber-security. That is despite the fact the Government also identified those areas as international standardisation priorities. By definition, all technical standards created to help manufacturers meet product requirements under EU law still applicable in Northern Ireland will also be covered by the exclusion of non-EEA organisations in formal decisions of the ESOs.

UK stakeholders in the full range of the ESOs work, especially in key areas relevant under the Northern Ireland Protocol/ or the UK's own standardisation strategy. Separately, we understand the European Commission is due to publish a full review of the EU's Standardisation Regulation, later in 2023. Whether any further proposed changes to the Regulation are of relevance to the UK would need to be assessed separately in due course.

Letter from the Chair to the Parliamentary Under Secretary of State (Kevin Hollinrake MP), Department for Business and Trade

You will be aware of our previous interest in the EU's recent amendment to its Standardisation Regulation, as set out in our Second Report of this Session. This aims to restrict the involvement of non-EU entities, including the British Standards Institution (BSI), when formal decisions are taken in relation to the development of certain new European technical standards in areas such as product safety, cyber-security and artificial intelligence within the European Standardisation Organisations (ESOs).

We note that the European Parliament and the Council have adopted the change as Regulation (EU) 2022/2480, which is due to take effect on 9 July 2023. Now the legislation has been finalised, we would welcome an updated assessment from you on the ramifications this change is expected to have, in practice, on British contributions to the development of new technical standards by the ESOs. What, if any, impact does the Government believe the restrictions on the role of the BSI and other UK entities within the ESOs will have on the UK's interests in the field of standardisation, especially in relation to standards under EU laws that continue to apply in Northern Ireland under the Protocol and in those areas identified by the Government as UK priorities in its 'Standards for the Fourth Industrial Revolution' policy paper?

We look forward to receiving your response by 5 May 2023.

2 Northern Ireland Protocol: the EU Cyber Resilience Act[22]

This EU document is legally important because:

- It would establish a new set of minimum cyber security requirements for "digital goods", including laptops, tablets and smart phones, sold in the Single Market. The Government has said that, although the proposal comes within the scope of the Northern Ireland Protocol, in its view the practical effects in Northern Ireland are non-existent. The new legislation is likely to create new obligations and costs for UK businesses exporting digital devices and software to the EU.

Action

- Draw the new EU cyber-security proposal to the attention of Science, Innovation and Technology Committee.

Overview

2.1 The EU is considering a new Regulation—the proposed EU Cyber Resilience Act (CRA)—to establish cyber-security requirements for "products with digital elements" like laptops, as well as non-tangible software products like smartphone applications.

2.2 The proposal is of particular legal interest for the UK in the context of the Protocol on Ireland/Northern Ireland to the UK/EU Withdrawal Agreement, which keeps EU laws relating to product safety requirements in force in Northern Ireland for the time being (including future amendments, now subject to the "Stormont Brake").[23] The CRA, as proposed, would make a consequential amendment to EU rules on market surveillance (trading standards), to ensure products that do not meet the new cyber requirements can be investigated and withdrawn from the market. As the EU's Market Surveillance Regulation still applies under the Protocol, this consequential amendment would therefore, in due course, also apply by default in Northern Ireland.

2.3 However, the lion's share of the EU proposal—setting out the actual cyber-security requirements for relevant products—will *not* automatically apply under the Protocol because it is an entirely new area of EU law. The Government has set out its legal position, stating that the amendment relating to market surveillance, while technically applicable in Northern Ireland, is in practice of "no effect" because the rest of the EU Cyber Resilience Act is outside the scope of the Protocol. To our knowledge, this is the first time the Government has articulated so precisely its position on the legal effects of consequential

22 Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020; 12429/22, COM(2022) 454; Legal base: Article 114 TFEU; Department: Science, Innovation and Technology; Devolved Administrations: Consulted; ESC number: 42121.

23 The Windsor Framework agreement between on the UK and the EU on the operation of the Protocol includes the "Stormont brake", under which Members of the Northern Ireland Assembly can empower the UK Government to block some new EU laws from taking effect under Article 13(3) in certain scenarios. The brake is inoperative while the Northern Ireland Assembly is not sitting, as is currently the case.

amendments to EU laws that still apply in Northern Ireland under the Protocol. Due to the specific legal issues raised by this EU proposal in that context, we have considered it further below.

The proposed EU 'Cyber Resilience Act'

2.4 The EU has a recent history of policy activity on cybersecurity. These include the 'Network Information Security Directive' (NIS),[24] which sets out specific resilience measures for IT systems in important sectors, including banking and healthcare, and the 2019 EU 'Cybersecurity Act' on voluntary cybersecurity certification schemes for companies.[25] However, in light of the continued increase in the use of digital products across society[26] and the increasing severity of digital threats (including Russia's increasingly concerning cyber posture following its attack on Ukraine),[27] the EU Member States in May 2022 explicitly requested the European Commission draft new EU legislation on cyber-security for a wider range of digital products.[28]

2.5 As a result, in September 2022, the Commission proposed to build on the EU's earlier measures in this area through a new EU 'Cyber Resilience Act' (CRA). Taking the form of a Regulation, this EU law—once adopted—would introduce mandatory "essential requirements" in terms of cyber-security for "products with digital elements". This would cover many common items such as laptops, toys and smartphones, as well as non-tangible software products (including operating systems, smartphone apps, and video games).[29]

2.6 The new requirements would include, for example, that products should have adequate protection from unauthorised access through control mechanisms such as authentication systems. Products within the scope of the CRA would have to undergo a "conformity assessment" to satisfy the manufacturer that the relevant cyber-security features were compliant.[30] In practice, companies are likely to rely extensively on technical standards developed by the ETSI, the European Telecommunications Standards Institute, at the request of the European Commission to meet the "essential requirements" set out in the

24 Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union. From October 2024, this will be replaced by the NIS2 Directive (Directive (EU) 2022/2555).

25 Regulation (EU) 2019/881 on ENISA and on information and communications technology cybersecurity certification.

26 The use of digital products is growing. One recent report forecast that there will be 29.3 billion networked devices by 2023. See, Cisco, 'Cisco Annual Internet Report (2018–2023) White Paper' (9 March 2020).

27 ENISA, 'Threat Landscape 2022' (October 2022).

28 Council of the EU, 'Council conclusions on the development of the European Union's cyber posture' (23 May 2022).

29 Some products with digital elements are excluded, notably where cybersecurity requirements are already covered by product-specific EU legislation (such as motor vehicles, aircraft components and medical devices).

30 See, in particular, Article 24 of the proposed Regulation. This establishes four categories of products according to their perceived cyber-security risks and sets requirements for the type of conformity assessment required. In ascending order of risk, these are: non-critical products (the default category); class I critical products (for example VPNs); class II critical products (like operating systems); and highly critical products, which are to be listed after the Regulation itself has been agreed. After having undertaken the conformity assessment, the manufacturer would indicate they declare their good to be in conformity with the requirements of the CRA by affixing the EU's 'CE' mark to the product.

proposed Regulation.[31] Enforcement of the new cyber-security requirements under the CRA would be the responsibility of "market surveillance" (trading standards) authorities in all EU Member States: these will get legal powers to require manufacturers to ensure a digital product no longer presents a risk, to recall or withdraw a product, and to impose fines for non-compliance.[32]

2.7 The Regulation (the legal form that the EU Cyber Resilience Act will take) can only take effect after its legal text has been approved jointly by the EU's Council of Ministers and by the European Parliament. Those institutions are currently considering their views on, and possible amendments to, the proposal. As such, the timetable for its formal adoption, and final substance, of the Regulation are not yet known at this point.[33] Once adopted, the European Commission envisages companies will have two years to implement the new requirements, meaning the EU Cyber Resilience Act is unlikely to be fully in effect until 2025 at the earliest.

Potential implications of the EU Cyber Resilience Act for the UK

2.8 The proposed EU Cyber Resilience Act may still be of relevance to the UK, despite its withdrawal from the European Union in 2020. This is, first, because it may have direct legal implications for the UK under the terms of the Northern Ireland Protocol. Second, it will affect British companies exporting relevant goods and software to the EU market (and could overlap with obligations they face under the UK's own cybersecurity laws, in particular, connected consumer devices under the Product Security and Telecommunications Infrastructure Act 2022).

The proposed EU Cyber Resilience Act and the Northern Ireland Protocol

2.9 The 2020 Northern Ireland Protocol, as amended in 2023 under the 'Windsor Framework', requires Northern Ireland to continue applying a range of EU legislation relating to trade in goods, including those governing product safety and performance requirements. New EU laws in those areas can also have direct legal ramifications in the UK under the Protocol. The original effect of Article 13(3) of the 2020 Northern Ireland Protocol was that new EU laws which amended or replaced EU legislation already applicable under the Protocol would take effect in Northern Ireland automatically, without the need for further UK agreement. This is now subject to the Stormont Brake.[34] Conversely, where the EU adopts new legislation that does not 'amend or replace' an existing law under the

31 See separately chapter 1 of this Report for more information on the EU's use of technical standards in its product requirements legislation. ETSI in 2019 already published the 'EN 303 645' standard, which provides a baseline for cybersecurity of physical consumer devices connected to the internet (the 'Internet of Things'). ETSI itself has said that it could also form the basis for more detailed future standards, which could in turn be approved as EU "harmonised standards" under the CRA. Standard EN 303 645 itself- is likely to be made the statutory cybersecurity baseline for connected consumer products in the UK under the Product Security and Telecommunications Infrastructure (PSTI) Act 2022 (see paragraph 2.12 below).

32 In exceptional circumstances, under the proposed CRA the European Commission itself could order a product's withdrawal or recall, depending on the nature of the risk.

33 EU Telecommunications Ministers are due to discuss the proposal at their meeting on 2 June 2023. The European Parliament's Industry Committee, which leads on this file, is scheduled to vote on the draft legislation in July 2023.

34 A recent innovation under the Windsor Framework is the "Stormont brake", under which Members of the Northern Ireland Assembly can empower the UK Government to block some new EU laws from taking effect under Article 13(3) in certain scenarios. The Stormont brake is inoperative while the Northern Ireland Assembly is not sitting, as is currently the case.

Protocol, but which it believes to be within the 'scope' of the Protocol, it can ask the UK to consent for the new law to be added to the Protocol (and therefore become applicable in Northern Ireland).[35]

2.10 The proposed Cyber Resilience Act is relevant under both Articles 13(3) and 13(4). Its provisions on market surveillance by trading standards authorities include a single amendment to the EU Market Surveillance Regulation,[36] which still applies in Northern Ireland under the Protocol.[37] As such, that amendment would, under Article 13(3), automatically take effect in Northern Ireland in due course, subject to the Stormont Brake. By contrast, the remainder of the proposed CRA—for example in relation to the "essential requirements" for digital products—do not 'amend or replace' EU legislation already applicable under the Protocol. Therefore, those elements of the new EU legislation, once adopted, will *not* apply in Northern Ireland automatically. However, the EU could theoretically still request that the new Regulation, insofar as it relates to cyber-security requirements for physical goods, be added to the Protocol under Article 13(4). We understand the EU has not, to date, made such a request, and that precedent suggests the EU would have normally communicated this when the proposal was first published in September 2022.[38]

2.11 The question therefore becomes what practical effect the CRA's amendment to the Market Surveillance Regulation would have in Northern Ireland once severed from the rest of the cyber-security proposal. In an Explanatory Memorandum on the EU proposal submitted by the then-Minister of State for Media, Data and Digital Infrastructure (Julia Lopez MP) in December 2022, the Government argues that, because the substantive elements of the new Regulation would not apply in Northern Ireland[39] "any consequential changes to other legislation that does apply [there] cannot have effect".[40] In a subsequent letter dated 13 February 2023, the Minister clarified the Government's reasoning to arrive at that position.[41] It follows that digital products on the market in Northern Ireland will have to comply with any applicable UK, not EU, statutory requirements on cyber-security.[42]

Other potential implications of the EU Cyber Resilience Act for the UK

2.12 Aside from any direct legal implications of the CRA under the Northern Ireland Protocol (or absence thereof), the European Commission proposal is also of relevance to

35 This process is set out in Article 13(4), and under UK domestic law will also requires cross-community consent in the Northern Ireland Assembly. See Part 4 of Schedule 6B to the Northern Ireland Act 1998 to be inserted by the Windsor Framework (Democratic Scrutiny) Regulations 2023.

36 Regulation 2019/1020 on market surveillance and compliance of products.

37 See the Office for Product Safety & Standards, 'EU Regulation on Market Surveillance and Compliance of Products (2019/1020). Guidance for Market Surveillance Authorities applying in respect of Northern Ireland from 16 July 2021' (June 2021). Regulation 2019/1020 replaced Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 which is listed in Annex 2 of the Northern Ireland Protocol.

38 Letter from Julia Lopez MP to Lord Jay of Ewelme, dated13 February 2023.

39 Except subject to the UK's consent under Article 13(4), which the EU has not requested.

40 The Explanatory Memorandum also stated that the CRA's *potential* effect was that "economic operators making products with digital elements available to customers in Northern Ireland *could* be subject to the obligation to cooperate with market surveillance authorities" and that those authorities acting in Northern Ireland "*could* also be legally obligated to provide economic operators with information concerning the implementation of the proposed Regulation applicable to their products" [own emphasis added].

41 Letter from Julia Lopez MP to Lord Jay of Ewelme, dated 13 February 2023.

42 This does appear to suggest that the use of the 'CE' mark in Northern Ireland will no longer denote acceptance of all relevant product performance requirements, given that insofar as it relates to cyber-security requirements under the CRA it will not be applicable.

companies that want to place relevant "digital products" on the EU market. The Minister highlighted in her Memorandum that these will have to comply with the new cyber-security requirements set out in the Regulation, which she says means UK businesses "may incur costs" to adapt to these new obligations (in particular if there is divergence between the requirements for the same products under the EU CRA and the UK's Product Security and Telecommunications Infrastructure Act 2022).[43]

2.13 Even if the substantive cyber-security requirements for a particular device were the same in the UK and the EU, there would still be administrative hurdles. In particular, the EU has not indicated it intends to recognise an assessment of the cyber-security performance of a particular product carried out in the UK as valid for assessing compliance with the obligations under the Cyber Resilience Act.[44] The Minister has said, however, that she is "look[ing] forward to further discussions with the EU on the prospect of mutual recognition [of conformity assessment] ahead of the CRA being brought into force".[45] If such talks are successful, that could allow UK-based bodies to carry out conformity assessments on goods destined for the EU market for the purposes of the CRA. The "discussions" to which the Minister refers may be part of a wider exchange of views between the UK and the EU on the mutual recognition of conformity assessments as part of the review of the EU/UK Trade and Cooperation Agreement in 2025.[46]

Conclusions and action

2.14 We welcome the Minister's assurance that the proposed EU Cyber Resilience Act will, as things stand, have no substantive effect in Northern Ireland under the Protocol because of the consequential nature of the sole provision of the proposal that engages Article 13(3).

2.15 To our knowledge, this is the first time the Government has publicly articulated this interpretation of the UK's legal obligations in relation to consequential amendments that fall within the scope of Article 13(3) of the Protocol within broader proposals for new EU laws that do not. The Minister has not, however, unambiguously stated that the EU shares this interpretation. We are aware that a similar matter is likely to arise in relation to the EU's proposed Artificial Intelligence Act, which—while in itself not covered by Article 13(3)—also makes a number of consequential amendments to EU legislation that does still apply in Northern Ireland under the Protocol.[47] Other EU proposals in the future could also raise the same issue.

2.16 Due to the unusual legal situation described above, the precise implications of the Cyber Resilience Act under the Protocol are somewhat ambiguous. This could, in the

43 The Act creates powers for Ministers to specify security requirements for physical products that connect to the internet, and that can transmit and receive digital data. Its scope is therefore substantially similar to the proposed EU Cyber Resilience Act but the specific technical requirements for products may differ. See, oral evidence before the Culture, Media and Sport Committee, 31 January 2023, Q418.

44 Conversely, the Government has, since Brexit, often automatically recognised compliance with EU product requirements as sufficient for a product also to be placed on the UK market. See, for example, the Government's guidance on 'CE' marking, which is still accepted on the Great Britain market until the end of 2024.

45 Letter from Julia Lopez MP to Lord Jay of Ewelme, dated 13 February 2023.

46 Currently, the EU does not recognise UK-based conformity assessments under EU law for any product category (unlike in its trade relations with Australia, New Zealand, Canada, the US and others). For more information on the lack of UK-EU mutual recognition of conformity assessments, see guidance issued by the UK Office for Product Safety and Standards.

47 See our Fourth Report of Session 2021–22 (HC 121–iv), chapter 2 (29 June 2021).

future, give rise to differences of interpretation between the UK and the EU about its legal effects in Northern Ireland. As the Minister acknowledges, there is also a likely, and potentially costly, impact of the CRA for British businesses exporting digital products to the EU. These will have to adapt to the new requirements (incurring compliance costs and potentially having to apply different cyber-security standards for the UK and EU markets). As such, we will follow the progress of the draft EU Cyber Resilience Act as it develops and may engage with the Minister on it further if circumstances so require. In particular, we expect the Minister to notify us if it emerges that the EU has a different view on the legal implications of the CRA in Northern Ireland under the Protocol compared to the Government's position as set out in her original Explanatory Memorandum and subsequent letter of 13 February 2023.

2.17 We have drawn this chapter to the attention of Science, Innovation and Technology Committee.

3 Northern Ireland: PEACE PLUS Programme[48]

These EU documents are politically important because:

- Northern Ireland will continue to participate in the EU's PEACE Plus Programme, part-financed by the UK Government.
- Agreement has been reached between the UK, Ireland and EU over their respective financial contributions

Action

- Report to the House.
- Draw to the attention of the Northern Ireland Affairs Committee.

Overview

3.1 The EU's 'PEACE' Programme was initially created in 1995 to support cooperation across the Irish border as a positive response to the paramilitary ceasefires of 1994. Throughout negotiations on the UK's withdrawal from the EU, both the EU and UK were clear that they wished the Programme—now known as 'PEACE PLUS'—to continue. The PEACE PLUS Programme will run until the end of 2027 with a budget of €1.14 billion (almost £1 billion), to be jointly financed by the UK Government, the EU, the Republic of Ireland and the Northern Ireland Executive. This budget represents a substantial increase on the PEACE 'IV' Programme (2014–20), which was worth around €270 million (£240 million).

3.2 A Financing Agreement[49] has recently been reached setting out the respective contributions and the financial governance arrangements. As the Programme largely supports Northern Ireland, the UK Government will be the majority contributor. It will make a total contribution of €852 million (£753 million), with the EU paying €234 million (£207 million) and Ireland paying €59 million (£52 million).

3.3 The Secretary of State for Northern Ireland (Rt Hon. Chris Heaton-Harris MP) wrote to us following adoption of the Financing Agreement. In addition to the agreed contributions, the Minister drew our attention to specific elements of the Agreement. He noted that the provisions on financial management are akin to those for the other EU financial programmes to which the UK may associate under the terms of the UK/EU Trade and Cooperation Agreement (TCA). The Minister also highlighted:

48 (a) Proposal for a Regulation of the European Parliament and of the Council on a mechanism to resolve legal and administrative obstacles in a cross-border context; (b) Proposal for a Regulation of the European Parliament and of the Council on specific provisions for the European territorial cooperation goal (Interreg) supported by the European Regional Development Fund and external financing instruments; Council and COM number: (a) 9555/18, COM(18) 373 (b) 9536/18 + ADD 1, COM(18) 374; Legal Base: (a) Article 175 TFEU, Ordinary legislative procedure, QMV (b) Articles 178, 209(1), 212(2) and 349 TFEU, Ordinary legislative procedure, QMV; Department: Northern Ireland Office; Devolved Administrations: Consulted; ESC Numbers: (a) (39809) (b) (39811).

49 Financing Agreement between the United Kingdom of Great Britain and Northern Ireland, Ireland and the European Commission on the PEACE PLUS Programme 2021–2027 (13 and 15 March 2023)

- parity for the UK Government crest alongside the EU emblem in Programme promotional material and communications;
- agreement that disputes are subject to international arbitration without any power of referral to the European Court of Justice;
- confirmation that where the Agreement obliges the UK and Ireland to implement the Programme in accordance with a limited number of EU Regulations, these will apply only until the closure of the Programme and only insofar as relevant to the Programme; and
- securing a no-fault termination clause for the Agreement, which provides the ultimate protection for UK interests, giving any Party the right to unilaterally terminate.

3.4 On 24 March 2023, the Agreement was laid for parliamentary scrutiny for 21 sitting days under the Constitutional Reform and Governance Act 2010 before it can be ratified and enter into force.

Background

3.5 In the TCA, the UK and EU recalled their commitment to PEACE PLUS and indicated that it would be the subject of a bespoke financing agreement, separate to the TCA's provisions on the UK's involvement in other EU financial programmes.

3.6 The EU legal basis for the Programme is the Regulation on European Territorial Cooperation (otherwise known as 'Interreg' (inter-regional cooperation)). This is a long-established strand of the EU structural funds, designed to promote regional cooperation across borders within the EU and with 'third' (non-EU) countries. The latest iteration of that Regulation[50] was adopted in 2021.

3.7 The cross-border Special EU Programmes Body (SEUPB) is responsible for administering the Programme and has been preparing for the Programme's launch.[51] The SEUPB has identified six different themes: peaceful and thriving communities; economic regeneration and transformation; investing in young people; healthy and inclusive communities; sustainability and connectivity; and partnership and collaboration. The Government will lay a Statutory Instrument in due course to make formal provision for the cross-border SEUPB to administer the Programme.

3.8 We last wrote to the Government about the PEACE PLUS Programme on 9 June 2021,[52] when we sought an update on the negotiations and raised the matter of dispute resolution.

Our assessment

3.9 The Financing Agreement is a balanced one, largely in line—as the Secretary of State notes—with the TCA's provisions for the financial management of other EU Programmes

50 Regulation (EU) 2021/1059 of the European Parliament and of the Council of 24 June 2021 on specific provisions for the European territorial cooperation goal (Interreg) supported by the European Regional Development Fund and external financing instruments

51 Special EU Programmes Body, 'PEACE PLUS', [Accessed 17 April 2023].

52 Letter from Sir William Cash MP to Rt Hon. Brandon Lewis CBE MP, dated 9 June 2021

in which the UK may also participate. We trust that the Programme will now move swiftly to implementation so that it can provide tangible benefits on the island of Ireland. We look forward to the further detailed information promised by the Secretary of State, but would ask that the information include details on the timetable for implementation.

Action

3.10 We are reporting the letter to the House and we draw our Report to the attention of the Northern Ireland Affairs Committee.

Annex

Documents drawn to the attention of select committees:

('SNC' indicates that scrutiny (of the document) is not completed'; 'SC' indicates that scrutiny of the document is completed)

Northern Ireland Affairs Committee: Northern Ireland: PEACE PLUS Programme [Proposed Regulation][SC]

Science, Innovation and Technology Committee: Northern Ireland Protocol: the EU Cyber Resilience Act [Proposed Regulation][SNC]

Formal Minutes

Wednesday 19 April 2023

Members present:

Sir William Cash, in the Chair

Mr John Baron

Richard Drax

Margaret Ferrier

Mr Marcus Fysh

Mr David Jones

Craig Mackinlay

Greg Smith

Document scrutiny

Draft Report, proposed by the Chair, brought up and read.

Ordered, That the draft Report be read a second time, paragraph by paragraph.

Paragraphs 1.1 to 3 read and agreed to.

Annex agreed to.

Resolved, That the Report be the Seventeenth Report of the Committee to the House.

Ordered, That the Chair make the Report to the House.

Adjournment

Adjourned till Wednesday 26 April 2023 at 1.45 pm

Standing Order and membership

The European Scrutiny Committee is appointed under Standing Order No.143 to examine European Union documents and—

a) to report its opinion on the legal and political importance of each such document and, where it considers appropriate, to report also on the reasons for its opinion and on any matters of principle, policy or law which may be affected;

b) to make recommendations for the further consideration of any such document pursuant to Standing Order No. 119 (European Committees); and

c) to consider any issue arising upon any such document or group of documents, or related matters.

The expression "European Union document" covers—

i) any proposal under the Community Treaties for legislation by the Council or the Council acting jointly with the European Parliament;

ii) any document which is published for submission to the European Council, the Council or the European Central Bank;

iii) any proposal for a common strategy, a joint action or a common position under Title V of the Treaty on European Union which is prepared for submission to the Council or to the European Council;

iv) any proposal for a common position, framework decision, decision or a convention under Title VI of the Treaty on European Union which is prepared for submission to the Council;

v) any document (not falling within (ii), (iii) or (iv) above) which is published by one Union institution for or with a view to submission to another Union institution and which does not relate exclusively to consideration of any proposal for legislation;

vi) any other document relating to European Union matters deposited in the House by a Minister of the Crown.

The Committee's powers are set out in Standing Order No. 143.

Current membership

Sir William Cash MP (*Conservative, Stone*) (Chair)

Tahir Ali MP (*Labour, Birmingham, Hall Green*)

John Baron MP (*Conservative, Basildon and Billericay*)

Jon Cruddas MP (*Labour, Dagenham and Rainham*)

Geraint Davies MP (*Labour, Swansea West*)

Allan Dorans MP (*Scottish National Party, Ayr Carrick and Cumnock*)

Richard Drax MP (*Conservative, South Dorset*)

Margaret Ferrier MP (*Independent, Rutherglen and Hamilton West*)

Mr Marcus Fysh MP (*Conservative, Yeovil*)

Dame Margaret Hodge MP (*Labour, Barking*)

Adam Holloway MP (*Conservative, Gravesham*)

Mr David Jones MP (*Conservative, Clwyd West*)

Stephen Kinnock MP (*Labour, Aberavon*)

Craig Mackinlay MP (*Conservative, South Thanet*)

Gavin Robinson MP (*Democratic Unionist Party, Belfast East*)

Greg Smith MP (*Conservative, Buckingham*)