EUROPEAN CENTRAL BANK

EUROSYSTEM

EN **ECB-PUBLIC**

OPINION OF THE EUROPEAN CENTRAL BANK

of 11 November 2019

on the security of network and information systems

(CON/2019/38)

Introduction and legal basis

On 10 October 2019 the European Central Bank (ECB) received a request from the Banco de España, on behalf of the *Secretaría de Estado para el Avance Digital* (SEAD, the Spanish State Secretary for Digital Progress), for an opinion on a draft royal decree (hereinafter the 'draft royal decree') on the security of network and information systems (NIS). The draft royal decree implements Royal decree-law No 12/2018 of 8 September 2018 on the security of network and information systems[1].

The ECB's competence to deliver an opinion is based on Articles 127(4) and 282(5) of the Treaty on the Functioning of the European Union and the third, fifth and sixth indents of Article 2(1) of Council Decision 98/415/EC[2], as the draft royal decree relates to the Banco de España, payment and settlement systems, rules applicable to financial institutions insofar as they materially influence the stability of financial institutions and markets, and the tasks conferred upon the ECB concerning the prudential supervision of credit institutions pursuant to Article 127(6) of the Treaty. In accordance with the first sentence of Article 17.5 of the Rules of Procedure of the European Central Bank, the Governing Council has adopted this opinion.

1. Purpose of the draft royal decree

1.1 The purpose of the draft royal decree is to further implement certain aspects of Royal decree-law No 12/2018. These legal acts transpose Directive (EU) 2016/1148 of the European Parliament and of the Council[3] into Spanish law. The legal acts also complement the relevant legislation enacted in Spain prior to the adoption of Directive (EU) 2016/1148, in particular Law No 8/2011of 28 April, on protection measures for critical infrastructures[4].

1.2 *Designation of the Banco de España and the Comisión Nacional del Mercado de Valores as competent authorities*

1.3 The draft royal decree designates the Banco de España, for the purpose of NIS, as the competent authority for credit institutions as operators of essential services, insofar as they are not critical operators. Neither Royal decree-law No 12/2018 nor the draft royal decree identify any operators of

1 Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información (BOE núm. 2018, de 8 de septiembre de 2018).

2 Council Decision 98/415/EC of 29 June 1998 on the consultation of the European Central Bank by national authorities regarding draft legislative provisions (OJ L 189, 3.7.1998, p. 42).

3 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

4 Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de infraestructuras críticas (BOE núm. 102, de 29 de abril de 2011).

essential services. Should a credit institution be classified as a critical operator, the competent authority would be the *Centro Nacional de Protección de Infraestructuras y Ciberseguridad* (CNPIC, National Centre for the Protection of Infrastructures and Cybersecurity), which is part of the *Secretaría de Estado de Seguridad* (the State Secretary for Security), which in turn is part of the *Ministerio del Interior* (the Ministry of Home Affairs).

1.4 The draft royal decree confers upon the competent authorities the task of supervising compliance with the obligations imposed on operators of essential services relating to the NIS and the notification of incidents. Operators of essential services must cooperate with the competent authority and provide all information required. Under the draft royal decree, competent authorities may conduct inspections for the purpose of carrying out their tasks. Under the draft royal decree, the Banco de España as a competent authority may also adopt delegated regulations (*circulares*) to ensure effective communication with credit institutions and oversee applicable requirements.

1.5 The draft royal decree sets forth that its provisions apply without prejudice to the competences and tasks conferred upon the Banco de España, the ECB and the ESCB pursuant to the Treaty, the Statute of the European System of Central Banks and the European Central Bank (hereinafter the 'Statute of the ESCB'), Council Regulation (EU) No 1024/2013[5]. The provisions of the draft royal decree also appliy without prejudice to Law No 13/1994 of 1 June on the autonomy of the Banco de España[6]. The provisions of the draft royal decree only apply to the Banco de España insofar as they do not conflict with the relevant rules applicable to the Banco de España and are compatible with the Banco de España's nature, tasks and independence.

1.6 The draft royal decree also designates, for the purpose of the NIS, the *Comisión Nacional del Mercado de Valores* (CNMV, the Spanish Securities Commission) as the competent authority for investment service companies and managing companies of collective investment institutions. Should such an entity be designated as acritical operator, the competent authority would be the State Secretary for Security, through the CNPIC.

1.7 *Obligations of operators of essential services*

1.8 The draft royal decree establishes certain security requirements for the operators of essential services that are applicable, among others, to credit institutions designated as such, and consist of: (i) the requirement to adopt security policies, which as a minimum must cover the following: risk analysis, management, management of third party or suppliers' risks, detection and management of incidents, recovery plans and business continuity, and system interconnections; and (ii) the requirement to designate a person responsible for the security of information as a point of contact for the relevant competent authority who will liaise with that authority in the event of security incidents. The tasks assigned to the person responsible for the security of information include preparing security policies, overseeing their implementation, and notifying any incidents to the competent authority. Under the draft royal decree, that person must be staffed with personnel who have adequate knowledge and experience, and sufficient resources to carry out their tasks and must be independent from the persons responsible for the security of network and information systems.

---

5 Council Regulation (EU) No 1024/2013 of 15 October 2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions (OJ L 287, 29.10.2013, p. 63).

6 Ley 13/1994, de 1 de junio, de Autonomía del Banco de España (BOE no. 131, de 2 de junio de 1994).

1.9 Operators of essential services must manage and resolve security incidents affecting network and information systems used in the provision of their services, including those detected by the operator itself and those notified by the competent authority or the relevant Computer Security Incident Response Team (CSIRT). Operators of essential services must also notify the competent authority, through the relevant CSIRT, of incidents where the impact level is high, very high or critical. Furthermore, they must notify the competent authority of incidents that may affect the network and information systems used to provide the essential services, even if the incident has not yet caused real adverse effects.

1.10 *Other measures*

1.11 The draft royal decree also includes provisions for cooperation among the different CSIRTs and between CSIRTs and competent authorities through a National Platform for Notifications and Oversight of Cyber Incidents, which ensures the secure exchange of information.

1.12 The draft royal decree includes an annex containing a national instruction on the notification and management of cyber incidents, which sets out criteria for the classification of cyber incidents, a ratings system to assign a hazard level to cyber incidents, and a template setting out the information to be reported by operators of essential services to competent authorities.

2. General observations

2.1 As previously noted by the ECB[7], the ECB supports the aim of Directive (EU) 2016/1148 of ensuring a high common level of network and information security across the Union and of achieving a consistency of approach in this field across business sectors and Member States. It is important to ensure that the internal market is a safe place to do business and that all Member States have a certain minimum level of preparedness for cybersecurity incidents. Concurrently, it should be ensured that the provisions of the national legislation transposing Directive (EU) 2016/1148 are coordinated with the Eurosystem's competences[8] and respect the principle of independence of central banks enshrined in Article 130 of the Treaty. In line with the ECB's recommendation, recital 14 of Directive (EU) 2016/1148 states that the Directive does not affect the Eurosystem's oversight of payment and settlement systems[9]. On the other hand, NIS benefits from synergies and economies of scale. In particular, dedicated national competent authorities have the potential to become repositories of considerable resources and expertise which the Eurosystem may draw upon in the area of NIS. Moreover, recognition of the ECB and its decision-making bodies' independence does not have the consequence of separating the Eurosystem entirely from the Union and exempting it from every rule of Union law[10]. The national implementing measures of Directive (EU) 2016/1148 are not *prima facie* precluded from applying to the Eurosystem[11].

---

7 See paragraph 2.1 of Opinion CON/2014/58; paragraph 2.1 of Opinion CON/2017/10; paragraph 2.2 of Opinion CON/2018/22; paragraph 2.2 of Opinion CON/2018/27 and paragraph 2.2 of Opinion CON/2019/17. All ECB opinions are published on the ECB's website at www.ecb.europa.eu.

8 See also paragraph 2.2 of Opinion CON/2014/58; paragraph 2.2 of Opinion CON/2017/10; and paragraph 3.1.1 of Opinion CON/2018/22.

9 See paragraph 3.1 of Opinion CON/2014/58 and paragraph 3.5 of Opinion CON/2017/10.

10 See judgment of the Court of Justice of 10 July 2003, *Commission* v *ECB*, C-11/00, ECLI:EU:C:2003:395, paragraphs 134 to 136.

11 See paragraph 2.2 of Opinion CON/2019/17.

2.2 Against this background, the ECB welcomes the designation of the Banco de España as a sectoral authority for NIS purposes. It also welcomes that the provisions of the draft royal decree apply without prejudice to the competences and tasks conferred upon the Banco de España, the ECB and the ESCB pursuant to the Treaty, the Statute of the ESCB, Regulation (EU) No 1024/2013, and Law No 13/1994[12]. Thereby the draft royal decree applies to the Banco de España only insofar as it does not conflict with the relevant rules applicable to the Banco de España and is compatible with the Banco de España's nature, tasks and independence.

2.3 The designation of the Banco de España as a sectoral NIS authority ensures that it may benefit from the resources and information specific to the NIS area, in particular being informed about actual and potential cyber incidents or threats in the financial sector's systems and infrastructures, and about planned and adopted measures, in an effective and timely manner[13]. On the other hand, the draft royal decree ensures that the Banco de España may carry out its tasks as a sectoral NIS authority without prejudice to its tasks as part of the Eurosystem and the Single Supervisory Mechanism (SSM). In this respect, the ECB understands that the clarification that the draft royal decree applies without prejudice to the competences and tasks conferred upon the Banco de España, including as part of the ESCB and the SSM, pursuant to the Treaty, the Statute of the ESCB, Regulation (EU) No 1024/2013 and Law No 13/1994, means that the draft royal decree applies in respect of all competences and tasks of the Banco de España and not only in respect of its designation as a sectoral NIS authority.

2.4 The ECB also welcomes that the draft royal decree shall apply without prejudice to the competences and tasks conferred upon the ECB pursuant to the Treaty, the Statute of the ESCB and Regulation (EU) No 1024/2013.

2.5 In addition, the ECB stands ready to cooperate with the Spanish authorities in relation to the systems and infrastructures which the Eurosystem oversees or operates, such as payment systems, instruments and schemes, and the prudential supervision of credit institutions, with a view to ensuring that best practices with regard to NIS are established and followed[14]. The ECB has previously called for the establishment of such effective cooperation and information-sharing arrangements between the national NIS authorities and, through the national central banks (NCBs), the ECB[15]. In this respect, the ECB understands[16] that Banco de España may share the relevant information it receives from different stakeholders in its capacity as a sectoral NIS authority with the ECB in a timely and efficient manner within the framework of the respective responsibilities of the Banco de España and the ECB[17].

3. Impact of the draft royal decree on payment systems and securities settlement systems

3.1 *Impact on other operators of essential services within the financial and tax strategic sector*

12 Fourth additional provision of the draft royal decree.

13 See paragraphs 3.2.4 and 3.4.3 of Opinion CON/2018/22 and paragraph 4.4 of Opinion CON/2018/47.

14 See paragraph 6.3 of Opinion CON/2018/22.

15 See paragraphs 2.3 and 6.2 of Opinion CON/2018/22 and paragraphs 2.4, 3.1.6, 3.2.4 and 4.7 of Opinion CON/2019/17.

16 This understanding is based in Article 14 of the Royal Decree-law No. 12/2018, which allows the exchange of information between authorities, and the general secrecy provisions that apply to Banco de España.

17 See paragraph 4.3 of Opinion CON/2018/27, paragraph 6.2 of Opinion CON/2018/47 and paragraph 2.4 of Opinion CON/2019/17.

3.1.1 Law No 8/2011 identifies the 'financial and tax system' as a strategic sector, i.e., as an area of economic activity that provides an essential service. Essential services are defined both in Law No 8/2011 and Royal decree-law No 12/2018 as services necessary for: (i) the maintenance of basic social functions, health, security, the economic and social welfare of citizens; or (ii) the efficient functioning of State institutions and public authorities that rely on network and information systems. Royal decree-law No 12/2018 clarifies that 'operators of essential services' are public or private entities that provide essential services within one of the strategic sectors identified in Law No 8/2011. Royal decree-law No 12/2018 also makes clear that an operator will be classified as an operator of essential services if an incident suffered by such an operator may have significant disruptive effects on the supply of the services depending, inter alia, on the alternatives available or the number of service users.

3.1.2 The draft royal decree explicitly designates the NIS competent authorities for credit institutions, insurance companies, managing companies of collective investment institutions and investment service companies qualifying as operators of essential services for the financial and tax system, where these do not qualify as critical operators. However, it does not expressly designate NIS competent authorities for other entities also belonging to the financial and tax system, such as operators of trading venues, or central counterparties (CCPs), to which Annex II of Directive (EU) 2016/1148 makes express reference, or other payment and securities settlement systems, where these do not qualify as critical operators, or provide additional guidance on what constitutes an operator of essential services. The ECB understands that these other infrastructures, over which the ECB or the Banco de España have an oversight role, might have been designated as critical operators, in which case the NIS competent authority would be the State Secretary for Security, through the CNPIC, based on the designation set out in Royal Decree-law No 12/2018. In this respect, it is unclear whether the Banco de España itself is also bound by the obligations on operators of essential services imposed by the draft royal decree, in its capacity as operator of a systemically important payment system (SIPS), such as the Spanish component of TARGET2, namely TARGET2-Banco de España.

3.2 *Impact on operators of market infrastructures: systemically important payments systems*

3.2.1 In its oversight role and on the basis of Articles 3.1 and 22 and the first indent of Article 34.1 of the Statute of the ESCB, the ECB adopted Regulation (EU) No 795/2014 of the European Central Bank (ECB/2014/28)[18]. Regulation (EU) No 795/2014 (ECB/2014/28) implements the Principles for financial market infrastructures (PFMIs) issued by the Committee on Payment and Settlement Systems (CPSS) and the International Organization of Securities Commissions (IOSCO)[19] (hereinafter the 'CPSS-IOSCO PFMIs') which are legally binding and cover both large-value and retail payment systems of systemic importance, operated either by a Eurosystem central bank or a private entity.

18 Regulation (EU) No 795/2014 of the European Central Bank of 3 July 2014 on oversight requirements for systemically important payment systems (ECB/2014/28) (OJ L 217, 23.7.2014, p. 16).

19 Available on the Bank for International Settlements' website at www.bis.org.

3.2.2 Thus, SIPS are subject to regular assessment against the requirements of Regulation (EU) No 795/2014 (ECB/2014/28) related to operational risk[20], which allows the competent Eurosystem central bank, as competent authority, to verify that the systems are in compliance. In cases of non-compliance, the competent Eurosystem central bank has the power to impose sanctions or corrective measures to ensure compliance[21]. Amendments to Regulation (EU) No 795/2014 (ECB/2014/28) recently[22] introduced a number of new requirements for SIPS operators addressing new risks, including those related to operational and security risks, such as cyber resilience[23], taking into account, inter alia, the Guidance on cyber resilience for financial market infrastructures which was published in 2016 by the Committee on Payments and Market Infrastructures (CPMI) and IOSCO[24] (hereinafter the 'CPMI-IOSCO Guidance on cyber resilience').

3.2.3 Furthermore, in line with the requirements set out in Directive (EU) 2016/1148, Regulation (EU) No 795/2014 (ECB/2014/28) already provides competent Eurosystem central banks with the power to obtain information concerning, inter alia, major and minor incidents, the nature and type of the incidents, their seriousness and their duration[25]. The amended Regulation (EU) No 795/2014 (ECB/2014/28) further enhanced competent Eurosystem central banks' powers to conduct on-site inspections and request independent reviews of and investigations into the functioning of the systems.[26]

3.2.4 Among listed SIPS, TARGET2 plays a distinct role, as it is owned and operated by the Eurosystem and subject to strict regulation and oversight[27.] While the draft royal decree does not refer explicitly to SIPS, the ECB understands that the Spanish component of TARGET2, TARGET2-Banco de España, for which Banco de España acts as an operator, could potentially fall within the scope of the draft royal decree. TARGET2 has been identified, pursuant to Decision ECB/2014/35 of the European Central Bank[28], as a SIPS and is overseen by the ECB as the competent authority under Regulation (EU) No 795/2014 (ECB/2014/28).

3.2.5 The ECB understands that the draft royal decree does not prejudice in any respect the competence of the Eurosystem with respect to the oversight of SIPS, given that such oversight is performed on

---

20 See Article 15 of Regulation (EU) No 795/2014 (ECB/2014/28), which imposes an obligation on SIPS operators to take steps such as: (a) establish comprehensive physical and information security policies that adequately identify, assess and manage all potential vulnerabilities and threats, (b) to ensure that critical information technology systems can resume operations within specified timeframes where an event poses a significant risk of disrupting the SIPS' operations etc.

21 See paragraph 3.4 of Opinion CON/2017/10.

22 Amendments introduced by Regulation (EU) 2017/2094 of the European Central Bank, of 3 November 2017, amending Regulation (EU) No 795/2014 on oversight requirements for systemically important payment systemsb (ECB/2017/32

23 See Article 15(1a) and (4a) of Regulation (EU) No 795/2014 (ECB/2014/28), which imposes an obligation on SIPS operators to take the following steps: (i) review, audit and test systems, operational policies, procedures and controls periodically and after significant changes; (ii) establish an effective cyber resilience framework with appropriate governance measures in place; (iii) identify their critical operations and supporting assets, and have appropriate measures in place to protect them from, detect, respond to and recover from cyber-attacks; (iv) regularly test the established measures; and (v) have a sound level of situational awareness of cyber threats, including through a process of continuous learning.

24 Available on the Bank for International Settlements' website.

25 See Article 21(1a) of Regulation (EU) No 795/2014 (ECB/2014/28).

26 See Articles 21(1b) and (1c) of Regulation (EU) No 795/2014 (ECB/2014/28).

27 See paragraph 3.1.5 of Opinion CON/2019/17.

28 Decision ECB/2014/35 of the European Central Bank of 13 August 2014 on the identification of TARGET2 as a systemically important payment system pursuant to Regulation (EU) No 795/2014 on oversight requirements for systemically important payment systems (OJ L 245, 20.8.2014, p. 5).

the basis of ECB regulations. As noted in paragraph 2.5, the ECB understands that the information that the Banco de España receives as a sectoral NIS authority about actual and potential cyber incidents, as well as planned or adopted measures which may affect SIPS and TARGET2, may be shared with the ECB in a timely and efficient manner.

3.3 *Impact on non-systemically important payment systems*

3.3.1 Non-*systemically important payment systems (non*-SIPS) include non-systemically important large-value payment systems (LVPS) and non-systemically important retail payment systems (non-SIRPS). Under the revised oversight framework for retail payment systems[29], non-SIRPS have been divided into two distinct groups: prominently important retail payments systems (PIRPS) and other retail payment systems (ORPS). The *Sistema Nacional de Compensación Electrónica* (the Spanish local retail payment system) has been classified as belonging to the group of PIRPS[30]. The ECB understands that its services could be included in the list of essential services pursuant to the draft royal decree and that the operators of this system might be designated as an operator of essential services.

3.3.2 Under the Eurosystem's oversight policy framework, non-SIRPS must follow the CPSS-IOSCO PFMIs and the Oversight expectations for links between retail payment systems (OELRPS)[31]. Both the CPSS-IOSCO PFMIs and the OELRPS are soft law instruments, meaning that non-systemically important LVPS, PIRPS and ORPS are subject to oversight standards comparable to the standards under Regulation (EU) No 795/2014 (ECB/2014/28) however there is no Union legislation regulating the oversight or supervision of these systems[32]. The Banco de España's competences in relation to oversight over non-SIPS are also conferred pursuant to Law No 13/1994[33].

3.3.3 The revised oversight framework for retail payment systems specifies that all retail payment systems are an integral part of the payment and settlement landscape of the euro area and thus fall within the scope of oversight. Hence, the Eurosystem has an interest in ensuring that the oversight framework and standards applicable to such systems are not prejudiced through the implementation of Directive (EU) 2016/1148 or when introducing other NIS-related laws[34].

3.3.4 If the intention is for non-SIPS to be within the scope of the draft royal decree, the ECB understands that the draft royal decree does not prejudice the Banco de España's ability to carry out its oversight tasks. As suggested in paragraph 2.5, the ECB understands that the Banco de España may share with the ECB any relevant information on non-SIPS it receives as a sectoral NIS authority.

3.4 *Impact on payment services, payment instruments and payment schemes*

3.4.1 The Eurosystem oversight policy framework identifies payment instruments (such as cards, credit transfers, direct debit and electronic money) as an 'integral part of payment systems' and thus

29 See the Eurosystem's 'Revised oversight framework for retail payment systems' (February 2016), available on the ECB's website at www.ecb.europa.eu.

30 See the Eurosystem's 'Overview of payment systems', available on the ECB's website.

31 See the Eurosystem's 'Oversight expectations for links between retail payment systems', available on the ECB's website.

32 See paragraph 2.4.4 of ECB Opinion CON/2017/31, paragraph 3.2.3 of Opinion CON/2018/22 and paragraph 3.2.2 of Opinion CON/2019/17.

33 See Article 7 and Article 16 of Law No 13/1994.

34 See paragraph 3.4.2 of Opinion CON/2018/22, paragraph 4.3 of Opinion CON/2018/47 and paragraph 3.2.3 of Opinion CON/2019/17.

includes these within the scope of its central banking oversight. For payment instruments, the role of primary overseer for the Eurosystem is assigned by reference to the national anchor of the payment scheme and the legal incorporation of its governance authority. For credit transfer schemes and direct debit schemes within the Single Euro Payments Area, as well as some of the international card payment schemes, the ECB has the primary oversight role. Payment service providers (PSPs), including credit institutions, payment institutions and electronic money institutions, are subject to Directive (EU) 2015/2366 of the European Parliament and of the Council[35], which is applicable as of January 2018, as implemented into national law. The legal and regulatory framework sets out requirements pertaining to operational and security risks and incident reporting. Nevertheless, prudential supervisors need to exercise careful judgment when deciding whether to publish information concerning individual cybersecurity incidents, to ensure public confidence in the affected institutions is not undermined. Furthermore, the European Banking Authority (EBA) has produced guidelines on the security measures for the management of operational and security risks in relation to payment services under Directive (EU) 2015/2366[36], and is preparing draft guidelines on information and communication technology (ICT) and security risk management[37] which are intended to harmonise standards applicable to PSPs regarding ICT security, incident reporting, project management and business continuity. Therefore, PSPs are subject to Union legislation, Spanish legislation, and regulations based on Union legislation. However, the oversight of international and domestic card schemes is not subject to Union legislation as such[38].

3.4.2 The ECB understands that the various payment schemes, instruments and PSPs may potentially fall within the scope of the draft royal decree. The ECB reiterates its understanding that the Banco de España may share with the ECB any relevant information it receives as a sectoral NIS authority in a timely and efficient manner and in accordance with the framework of respective responsibilities of the Banco de España and the ECB.

3.5 *Impact on central securities depositories*

3.5.1 Central securities depositories (CSDs) are strictly regulated and supervised by different authorities pursuant to Regulation (EU) No 909/2014 of the European Parliament and of the Council[39], which sets out requirements pertaining to operational risk. Furthermore, CSDs should take note of the CPMI-IOSCO Guidance on cyber resilience which applies to all financial market infrastructures.

3.5.2 In addition to the supervisory competences entrusted to national competent authorities (NCAs) under Regulation (EU) No 909/2014, national authorities, and in particular the members of the ESCB, are entrusted with the oversight of authorisation and supervision of CSDs in their capacity

35 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, p. 35).

36 Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2) (EBA/GL/2017/17), of 12 January 2018.

37 See the EBA Guidelines on internal governance under Directive 2013/36/EU of 26 September 2017 (EBA/GL/2017/11) and the draft EBA Guidelines on ICT and security risk management of 13 December 2018 (EBA/CP/2018/15) available on the EBA's website at www.eba.europa.eu.

38 See paragraph 2.4.3 of Opinion CON/2017/31, paragraph 3.4.2 of Opinion CON/2018/22 and paragraph 3.4.1 of Opinion CON/2019/17.

39 Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012 (OJ L 257, 28.8.2014, p. 1).

as 'relevant authorities'[40]. In this regard, recital 8 of Regulation (EU) No 909/2014 states that the Regulation should apply without prejudice to the responsibilities of the ECB and the NCBs to ensure efficient and sound clearing systems and payment systems within the Union and other countries. Recital 8 also states that Regulation (EU) No 909/2014 should not prevent the members of the ESCB from accessing information relevant to the performance of their duties[41], including the oversight of CSDs and other financial market infrastructures[42].

3.5.3 Iberclear is the Spanish Central Securities Depository, authorised under Regulation (EU) No 909/2014 and supervised by the CNMV. Pursuant to Regulation (EU) No 909/2014, Iberclear is the operator of a securities settlement system which is overseen jointly by the Banco de España and the CNMV. Insofar as Iberclear may be an operator of essential services and may fall within the scope of the draft royal decree, the ECB understands that the draft royal decree would apply without prejudice to the Banco de España's tasks in relation to oversight, also taking into account that such oversight is performed on the basis of Union legislation.

3.6 *Eurosystem cyber resilience strategy for Financial Market Infrastructures*

3.6.1 The ECB understands that the provisions of the draft royal decree apply without prejudice to the Eurosystem cyber resilience strategy for Financial Market Infrastructures (FMIs)[43], which is intended to support the implementation of the CPMI-IOSCO Guidance on cyber resilience from an oversight perspective. The objectives of this strategy are to: (i) improve the cyber resilience of the euro area financial sector as a whole by enhancing the 'cyber readiness' of individual FMIs that are overseen by the Eurosystem central banks; and (ii) foster collaboration among FMIs, their critical service providers and the relevant authorities. As part of the strategy, the Eurosystem has developed a range of tools that can be used by FMIs to enhance their cyber resilience, such as a European red team testing framework[44], and other tools, such as cyber surveys and focused assessments to assess the level of cyber maturity of Eurosystem payment systems and to develop cyber resilience oversight expectations[45], which will provide more detailed guidance to payment system operators.

4. Impact of the draft royal decree on credit institutions

4.1 Recital 13 of Directive (EU) 2016/1148 states that requirements in respect of information systems, which often exceed the requirements provided for under Directive (EU) 2016/1148, are set out in a number of Union legal acts, including the rules on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms. Member States should consider those requirements in their application of provisions transposing Directive (EU) 2016/1148 as *lex specialis*. Indeed, the Union legal acts harmonising the area of supervision of credit institutions

40 See Article 12 of Regulation (EU) No 909/2014.

41 See also Articles 13 and 17(4) of Regulation (EU) No 909/2014.

42 See paragraph 7.3 of Opinion CON/2017/10; paragraph 7.2 of Opinion CON/2018/47; and 3.5.2 of Opinion CON/2019/17.

43 See more at https://www.ecb.europa.eu/paym/cyber-resilience/fmi/html/index.en.html

44 See the Eurosystem's Framework for Threat Intelligence-based Ethical Red Teaming (TIBER-EU) (May 2018), available on the ECB's website.

45 See the Eurosystem's 'Cyber resilience oversight expectations for financial market infrastructures' (CROE) (December 2018), available on the ECB's website.

include Regulation (EU) No 575/2013 of the European Parliament and of the Council[46] and Directive 2013/36/EU of the European Parliament and of the Council[47], jointly establishing the CRR/CRDIV framework.

4.2 The ECB and the Banco de España are the competent authorities exercising specified supervisory powers under the CRR/CRDIV framework, by virtue of Regulation (EU) No 1024/2013 which confers specific tasks on the ECB concerning the prudential supervision of credit institutions within the euro area and makes the ECB responsible for the effective and consistent functioning of the Single Supervisory Mechanism (SSM) within which specific supervisory responsibilities are distributed between the ECB and the participating NCAs, including the Banco de España. In particular, the ECB carries out the task to authorise and to withdraw the authorisations of all credit institutions. For significant credit institutions the ECB also has the task, among others, to ensure compliance with the relevant Union law that imposes prudential requirements on credit institutions, including the requirement to have in place robust governance arrangements, such as sound risk management processes and internal control mechanisms[48]. To this end, the ECB is given all supervisory powers to intervene in the activity of credit institutions that are necessary for the exercise of its functions.

4.3 The prudential supervision of credit institutions, as exercised by the ECB and the Banco de España within the SSM, covers several aspects related to cybersecurity as part of the prudential supervision of operational risk, which means the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events[49]. In addition, the EBA has produced guidelines on internal governance covering aspects of IT risks[50], and, as noted in paragraph 3.4.1, draft guidelines on ICT and security risk management[51] which are intended to harmonise requirements for credit institutions, investment firms and payment service providers as regards ICT security, incident reporting, project management and business continuity. Further EBA Guidelines are under development, concerning inclusion of cyber risk aspects in the Supervisory Review and Evaluation Process[52]. The ECB has developed comprehensive IT risk questionnaires for supervised credit institutions that are fed into their SREP outcomes and also uses insights on cyber-security issues that may be drawn from thematic reviews, on-site inspections and reports of cyber incidents[53]. Such insights may form the basis for ad hoc institution-specific recommendations and general sector-wide comparisons and policies. At the same time, prudential supervisors need

46 Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).

47 Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).

48 See Article 4(1)(e) and Article 6(4) of Regulation (EU) No 1024/2013.

49 See Article 4(1)(52) of Regulation (EU) No 575/2013.

50 Guidelines on Internal Governance (EBA/GL/2017/11), of 21 March 2018.

51 See the EBA Guidelines on internal governance under Directive 2013/36/EU of 26 September 2017 (EBA/GL/2017/11) and the draft EBA Guidelines on ICT and security risk management of 13 December 2018 (EBA/CP/2018/15), available on the EBA's website.

52 See the EBA's draft Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP) of 6 October 2016 (EBA/CP/2016/14), available on the EBA's website.

53 See also the Newsletter article of 13 February 2019 on 'IT and cyber risk - the SSM perspective', available on the ECB's website.

to exercise careful judgment when deciding to publish information concerning individual cybersecurity incidents so as to not undermine public confidence in the affected credit institutions.

4.4 Moreover, the ECB and the NCAs within the SSM are responsible for the assessment of recovery plans and taking early intervention measures under Directive 2014/59/EU of the European Parliament and of the Council[54] (as transposed into national law). Further, the primary responsibility for determining that a significant credit institution is failing or likely to fail as a condition to the resolution of a credit institution lies with the ECB[55]. In the case of resolution, one of the resolution objectives is to ensure the continuity of critical functions[56], which can include the continuing functioning of the credit institution's payment and cash circulation systems.

4.5 Central banks are excluded from the scope of Directive 2013/36/EU and are thus not supervised institutions falling within the scope of Regulation (EU) No 575/2013. Therefore, neither the ECB nor the Banco de España falls within the scope of the 'banking sector' for the purposes of point (3) of Annex II to Directive (EU) 2016/1148[57].

4.6 In this context, the ECB welcomes the designation of the Banco de España as a sectoral NIS authority for credit institutions which are operators of essential services but not critical operators. There are undoubtedly overlaps in the prudential supervision of operational risk for credit institutions and the supervision of compliance with credit institutions obligations as operators of essential services. The ECB also welcomes the draft royal decree's explicit clarification that Banco de España should carry out its NIS tasks without prejudice to its supervisory tasks in the context of the SSM. In this respect, the ECB notes that there is an obligation to ensure the exchange of information between the ECB and the national competent authorities under Union law. The national competent authorities are required to provide the ECB with all information necessary for the purposes of carrying out the tasks conferred upon the ECB pursuant to Regulation (EU) No 1024/2013[58]. In this context, the ECB reiterates its understanding that the Banco de España may share with the ECB any relevant information it receives as a sectoral NIS authority in a timely and efficient manner and within the framework of the respective responsibilities of the Banco de España and the ECB.

5. NIS-related role of the Banco de España

5.1 The draft royal decree designates the Banco de España as the competent authority for credit institutions in their capacity as operators of essential services insofar as they are not critical operators. Such supervision consists of overseeing the compliance by credit institutions as operators of essential services with their NIS obligations, including the power to request documents

54 See Articles 27 to 30 of Directive 2014/59/EU of the European Parliament and of the Council of 15 May 2014 establishing a framework for the recovery and resolution of credit institutions and investment firms and amending Council Directive 82/891/EEC, and Directives 2001/24/EC, 2002/47/EC, 2004/25/EC, 2005/56/EC, 2007/36/EC, 2011/35/EU, 2012/30/EU and 2013/36/EU, and Regulations (EU) No 1093/2010 and (EU) No 648/2012, of the European Parliament and of the Council (OJ L 173, 12.6.2014, p. 190).

55 See Article 32(1)(a) of Directive 2014/59/EU.

56 See Article 31(2)(a) of Directive 2014/59/EU.

57 See paragraph 2.4 of Opinion CON/2017/10 and paragraph 4.5 of Opinion CON/2019/17.

58 See Article 6(2) and Article 6(7)(c)(i) and (iii) of Regulation (EU) No 1024/2013; Article 21(1), Articles 97 and 98 of Regulation (EU) No 468/2014 of the European Central Bank of 16 April 2014 establishing the framework for cooperation within the Single Supervisory Mechanism between the European Central Bank and national competent authorities and with national designated authorities (SSM Framework Regulation) (ECB/2014/17) (OJ L 141, 14.5.2014, p. 1).

and conduct inspections if necessary. The Banco de España must also cooperate with other competent authorities regarding the performance of its NIS tasks, including in the provision of technical advice on the suitability of security measures adopted by credit institutions. The Banco de España must liaise and cooperate with the relevant CSIRTs. Royal decree-law No 12/2018 confers sanctioning powers upon competent authorities for minor and severe breaches of NIS obligations.

5.2 Many of the Banco de España's tasks as a sectoral authority, including supervising compliance by credit institutions and liaising and coordinating with other authorities, are already carried out by the Banco de España in its role as prudential supervisor of credit institutions. The draft royal decree significantly overlaps with the prudential supervisory tasks of the Banco de España within the framework of the SSM, in particular regarding the supervision of operational risk where Banco de España must examine the adequacy of internal processes, crisis management procedures, continuity plans and IT risks. Thus, the task conferred upon the Banco de España by the draft royal decree is related to, and overlaps with, the prudential supervisory tasks conferred upon the ECB and the NCBs under the Treaty and the Statute of the ESCB. This task is not atypical. Many NCBs are assigned prudential supervisory tasks and there are a number of Member States in which NCBs have been entrusted with NIS-specific tasks, including the identification of operators of essential services and/or the supervision of their compliance with cybersecurity obligations[59].

59 In Belgium the National Bank of Belgium (NBB) has been appointed under the Law of 1 July 2011 on the security and protection of critical infrastructures as the sectoral authority for the financial sector responsible for the identification, designation and monitoring of critical infrastructures. The NBB has also been appointed under the national legislation transposing Directive (EU) 2016/1148 as the sectoral authority responsible to ensure compliance by credit institutions and central counterparties, in their capacity as operators of essential services, with their obligations so far as concerns incident notifications. The provisions on security requirements, internal and external audit, control, verifications and inspections, which apply to all other sectors, are waived in respect of operators of essential services in the financial sector. See paragraphs 1.2, 1.3 and 1.5 of Opinion CON/2018/27. In Croatia the Cybersecurity Law implementing Directive (EU) 2016/1148, adopted in July 2018, entrusted Hrvatska narodna banka (HNB) with tasks related to the identification of operators of essential services, the supervision of operators and the receipt of incident notifications. The HNB has to assess whether they comply with cybersecurity obligations, entailing supervision once every two years or if an operator of essential services fails to comply with obligations under the law. The HNB is empowered to request and receive from operators of essential services data needed to assess the security level of their network and information systems, including documented security policies and evidence of effective implementation of security measures. The HNB is also empowered to issue mandatory guidance, to submit indictments and to receive reports on incidents. In Ireland Statutory Instrument No 360 of 2018 EU (Measures for a high common level of security of network and information systems) Regulations 2018 conferred the following tasks on the Central Bank of Ireland: (i) preparing and maintaining a list of essential services in the relevant sector; (ii) designating a person as an operator of essential services in the relevant sector; (iii) establishing and maintaining a Register of Operators of Essential Services containing particulars of operators of essential services in the banking/FMI sector, and (iv) bringing and prosecuting summary proceedings for an offence under the Regulations committed by an operator of essential services. In the Netherlands Article 28 of the Act on the security of network and information systems (*Wet beveiliging netwerk- en informatiesystemen*) and the Order in Council on security of network and information systems (*Besluit beveiliging netwerk- en informatiesystemen*) confers on competent authorities the powers to initiate a security audit, give binding instructions and impose administrative sanctions and enforcement measures. The obligations related to security audit and instructions do not apply to financial infrastructures and financial institutions, but these entities remain however subject to the obligation to report incidents. The main tasks of DNB are therefore receiving incident notifications and imposing enforcement measures and sanctions for breaches of the obligation to report incidents.

Although cybersecurity clearly relates to national security, due to the strong overlap with the prudential supervisory tasks of the Banco de España, in particular as regards the supervision of operational risk, it can be concluded that the draft royal decree does not confer genuinely new tasks on the Banco de España in this respect.

This opinion will be published on the ECB's website.

Done at Frankfurt am Main, 11 November 2019.

[signed]

The President of the ECB
Christine LAGARDE