OPINION OF THE EUROPEAN CENTRAL BANK

of 6 April 2017

on the identification of critical infrastructures for the purpose of information technology security

(CON/2017/10)

Introduction and legal basis

On 27 February 2017 the European Central Bank (ECB) received a request from the German Ministry of the Interior for an opinion on a first amendment to a German draft regulation of the German regulation to identify critical infrastructures under the Law on the Federal Office for Information Security (hereinafter the 'draft regulation').

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 fifth indent of Article 2(1) of Council Decision 98/415/EC[1], as the draft regulation relates to payment and settlement systems. 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 regulation

1.1 The purpose of the draft regulation is to identify critical infrastructures and their operators that are subject to the Law on information technology security[2] (hereinafter the 'Law on IT security'), which stipulates the obligations of such operators to take appropriate organisational and technical precautionary measures to protect infrastructure-related information technology (IT) systems and to report severe IT incidents to the Federal Office for Information Security (BSI, *Bundesamt für Sicherheit in der Informationstechnik*). The BSI is empowered to carry out inspections and require the implementation of measures to safeguard compliance with the Law on IT security. Under the Law on IT security, the operators of critical infrastructures are also entitled to privileged advice and information provided by the BSI.

1.2 By providing specifications of infrastructures which have a key function in relation to various areas of society, the draft regulation aims to remove uncertainties as to which entities operate a given critical infrastructure.

1.3 Regarding the finance and insurance sector, the draft regulation covers the following: (a) the supply of cash in respect of authorisation of withdrawals, entering into payment transactions, charging customer accounts and cash logistics; (b) card-based payment transactions linked to cards within

1 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).

2 Act on the strengthening of the safety of information technology systems of 17 July 2015.

the meaning of Regulation (EU) No 2015/751 of the European Parliament and of the Council[3] in respect of the authorisation of and entering into payment transactions, as well as charging customer accounts and crediting the payment recipient's account; (c) conventional payment transactions carried out by means of transfer and direct debit within the meaning of Regulation (EU) No 260/2012 of the European Parliament and of the Council[4] in respect of acceptance of a transfer or direct debit, entering into payment transactions and charging and crediting customers' accounts; (d) the settlement and processing of securities and derivatives transactions including posting securities and funds; and (e) the utilisation of insurance services.

1.4 Both the Law on IT security and the draft regulation implement Directive (EU) 2016/1148 of the Parliament and of the Council[5], on which the ECB has issued an opinion[6]. The draft regulation implements Article 5(1) of and Annex II to Directive (EU) 2016/1148, which together specify the scope of application of the Directive.

1.5 Beyond what is required by Directive (EU) 2016/1148, the explanatory memorandum to the draft regulation explicitly lists TARGET2, SWIFT, EURO1, STEP1 and STEP2-T as examples of infrastructures subject to the Law on IT security. In particular, these systems are classified as 'systems to connect to an interbank payment system' which are allocated to the categories of 'infrastructures for the supply of cash' and 'conventional payment transactions' under part 1(1) of Annex 6 to the draft regulation.

1.6 The Law on IT security exempts from its scope operators of critical infrastructures that are subject to legal provisions which are either comparable to or go beyond the requirements of the Law on IT security[7].

2. General observations

2.1 As previously noted[8], the ECB supports the aim of Directive (EU) 2016/1148 to ensure a high common level of network and information security (NIS) across the Union and to achieve 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 cyber-security incidents.

2.2 While the draft regulation seeks to enhance the overall resilience of critical infrastructures by identifying infrastructures that have key functions for society in different areas, it should be ensured that the provisions of the draft regulation do not encroach on the Eurosystem's competences. This could be done by explicitly exempting from its scope of application payment and securities settlement systems overseen and/or operated by the ECB and the Eurosystem in general, including the Deutsche Bundesbank, as these are subject to comparable or more stringent

3 Regulation (EU) No 2015/751 of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions (OJ L 123, 19.05.2015, p. 1).

4 Regulation (EU) No 260/2012 of the European Parliament and of the Council of 14 March 2012 establishing technical and business requirements for credit transfers and direct debits in euro (OJ L 94, 30.03.2012, p. 22).

5 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).

6 See Opinion CON/2014/58. All ECB opinions are published on the ECB's website at www.ecb.europa.eu.

7 Sections 8c(2) no. 5 and 8c(3) no. 5 of the Law on IT security.

8 See paragraph 2.1 of Opinion CON/2014/58.

requirements. Essentially, it must be ensured that implementation of the requirements of Directive (EU) 2016/1148 does not conflict with Regulation (EU) No 795/2014 of the European Central Bank (ECB/2014/28)[9] and the Eurosystem's oversight policy framework. An extension of the scope of the Law on IT security to infrastructures operated and/or overseen by the ECB and the Eurosystem in general, including the Deutsche Bundesbank, would raise severe concerns regarding the principle of primacy of Union law as well as regarding the principle of central bank independence pursuant to Article 130 of the Treaty.

2.3 Notwithstanding the above, the ECB stands ready to cooperate with the BSI to ensure that best practices with regard to NIS are established and followed.

2.4 Finally, to qualify the infrastructures operated and overseen by the ECB and the Eurosystem, including the Deutsche Bundesbank, as subject to the Law on IT security, seems to lack a sufficient legal basis under the draft regulation itself. First, contrary to the intended application of the Law on IT security to Eurosystem-operated infrastructures, there are doubts as to whether the definition of critical infrastructures provided for in Section 2(10) of the Law on IT security captures these infrastructures. While this provision generally refers to the 'financial and insurance sector', the explanatory memorandum to the parliamentary draft of the Law on IT security sets out a comprehensive list of sub-sectors relevant to this area, which should form a basis for secondary legislation applicable to banking, financial service providers, stock exchanges and insurance companies. Central banks are not part of this list. Following the principle established by the Court of Justice of the European Union that provisions of national law must be interpreted in conformity with the directive that they implement[10], it is noteworthy that Annex II to Directive (EU) 2016/1148 does not list central banks as operators of essential services. Central banks are also not to be qualified as credit institutions, referred to in the definition of 'banking', as credit institutions are defined by reference to Article 4(1) of Regulation (EU) No 575/2013 of the European Parliament and of the Council[11]. Regulation (EU) No 575/2013 lays down uniform rules concerning general prudential requirements with which credit institutions and investment firms subject to Directive 2013/36/EU of the European Parliament and of the Council[12] must comply. 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 Deutsche Bundesbank falls within the scope of the banking sector, in accordance with point (3) of Annex II to Directive (EU) 2016/1148.

2.5 The ECB and the Bundesbank do not fall within the scope of the 'financial market infrastructures' referred to in point (4) of Annex II to Directive (EU) 2016/1148 since they do not operate trading venues within the meaning of Article 4(24) of Directive 2014/65/EU of the European Parliament and

---

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

10 *Amministrazione delle Finanze dello Stato v Simmenthal SpA*., C-106/77, ECLI:EU:C:1978:49; *Marleasing SA v La Comercial Internacional de Alimentacion SA.*, C-106/89, ECLI:EU:C:1990:395.

11 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).

12 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).

of the Council[13], being excluded from the scope of this Directive under Article 2(1)(h) thereof. The members of the European System of Central Banks (ESCB) also do not qualify as central counterparties within the meaning of Article 2(1) of Regulation (EU) No 648/2012[14] since ESCB members are excluded from the scope of this Regulation under Article 1(4)(a) thereof.

3. Impact of the draft regulation on payment systems overseen by the ECB and the Eurosystem

3.1 The ECB takes particular note of the fact that the explanatory memorandum to the draft regulation explicitly lists TARGET2, EURO1 and STEP2-T as examples of infrastructures subject to the Law on IT security[15]. These payment systems have been identified, pursuant to Decision ECB/2014/35 of the European Central Bank[16] and Decision ECB/2014/36 of the European Central Bank[17] respectively, as systemically important payment systems (SIPS) and are overseen by the ECB as competent authority under Regulation (EU) No 795/2014 (ECB/2014/28). Among the listed SIPS, TARGET2 plays a distinct role, as it is owned and operated by the Eurosystem, and subject to strict regulation and oversight.

3.2 The draft regulation incorrectly classifies TARGET2, EURO1 and STEP2-T as examples of 'systems to connect to an interbank payment system'. In fact, they are payment systems which should be classified as systems for carrying out conventional payment transactions. With regard to conventional payment transactions, due to the draft regulation's reference in Section 7(4) to Regulation (EU) No 260/2012 of the Parliament and the Council[18], which contains provisions on retail payment systems, all payments are exempted from the scope of conventional payment transactions which are carried out on a large-value payment system like TARGET2 and EURO1.

3.3 According to the fourth indent of Article 127(2) of the Treaty, promotion of the smooth operation of payment systems is one of the core tasks of the ESCB. Furthermore, pursuant to Article 22 of the Statute of the European System of Central Banks and of the European Central Bank (hereinafter the 'Statute of the ESCB'), the ECB and the national central banks may provide facilities, and the ECB may make regulations, to ensure efficient and sound clearing and payment systems within the Union. Thus, the ECB and the Eurosystem as a whole have a particular interest in an enhanced level of NIS in respect of payment systems, as it fosters confidence in the euro and the smooth functioning of the economy in the Union.

---

13 Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.6.2014, p. 349).

14 Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ L 201, 27.7.2012, p. 1).

15 STEP1, which is also identified by the draft regulation as a critical infrastructure, is primarily a payment service for commercial transactions and has been designed to process single cross-border payments in euro. STEP1 benefits from the technical and legal infrastructure of EURO1; participants in the STEP1 service can make full use of the EURO1 platform and are directly connected to all EURO1 and STEP1 participants.

16 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).

17 Decision ECB/2014/36 of the European Central Bank of 13 August 2014 on the identification of EURO1 and STEP2-T as systemically important payment systems pursuant to Regulation (EU) No 795/2014 on oversight requirements for systemically important payment systems.

18 Regulation (EU) No 260/2012 of the European Parliament and of the Council of 14 March 2012 establishing technical and business requirements for credit transfers and direct debits in euro and amending Regulation (EC) No 924/200 (OJ L 94 of 30.3.2012, p. 22).

3.4 Within the euro area, SIPS are subject to the requirements of Regulation (EU) No 795/2014 (ECB/2014/28). This Regulation implements the Principles for financial market infrastructures published by the Committee on Payment and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO) (CPMI-IOSCO) (hereinafter 'the CPMI-IOSCO Principles')[19] in a legally binding manner and covers both large-value and retail payment systems of systemic importance, operated either by a Eurosystem central bank or a private entity. Thus, SIPS are subject to regular assessment against the requirements of Regulation (EU) No 795/2014 (ECB/2014/28) related to operational risk, which allows the designated competent authority to verify that the systems are in compliance. In cases of non-compliance, the competent authority has the power to impose sanctions or corrective measures to ensure compliance.

3.5 In line with the ECB's recommendation[20], recital 14 of Directive (EU) 2016/1148 states that the Directive does not affect the Eurosystem's oversight of payment and settlement systems. While Article 3 of the Directive clarifies that the Directive lays down minimum harmonisation measures, such that Member States may adopt or maintain provisions with a view to achieving a higher level of security of network and information systems, it also states that this is without prejudice to Member States' obligations under Union law. In this respect, it is important to emphasise that there are already applicable effective provisions in place on the security of SIPS within the Union legal framework on oversight of payment systems. More specifically, Regulation (EU) No 795/2014 (ECB/2014/28) imposes a number of legal requirements on SIPS, which also address operational risk, including the obligation to (a) establish comprehensive physical and information security policies that adequately identify, assess and manage all potential vulnerabilities and threats, and (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.[21] Finally, recital 13 of Directive (EU) 2016/1148 acknowledges that the operational risk requirements in respect of financial market infrastructures (such as SIPS) under Union legal acts often exceed the requirements provided for under the Directive and should thus be considered as *lex specialis,* and therefore prevail over national measures implementing Directive (EU) 2016/1148.

3.6 There are plans to enhance the existing Union legal framework on oversight of payment systems. In particular, Regulation (EU) No 795/2014 (ECB/2014/28) is currently subject to a general review of its application, and public consultation in respect of a revised draft of Regulation (EU) No 795/2014 (ECB/2014/28) was carried out in December 2016[22]. The proposed regulation amending Regulation (EU) No 795/2014 (ECB/2014/28) seeks to further strengthen operational risk and NIS requirements, taking into account, inter alia, the CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures[23]. It introduces a number of new requirements addressing operational and cyber risks, such as imposing an obligation on SIPS operators to take the following steps: (a) review, audit and test systems, operational policies, procedures and controls periodically and after significant changes; (b) establish an effective cyber resilience framework with appropriate

19 Available on the Bank for International Settlement's (BIS) website at www.bis.org.
20 See paragraph 3.1 of Opinion CON/2014/58.
21 See Article 15 of Regulation (EU) No 795/2014 (ECB/2014/28).
22 Published on the ECB's website at www.ecb.europa.eu.
23 Available on the BIS' website at http://www.bis.org.

governance measures in place; (c) 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; (d) regularly test the established measures; and (e) have a sound level of situational awareness of cyber threats, including through a process of continuous learning[24]. The proposed new arrangements will therefore also qualify as Union sector-specific legislation of at least equivalent effect within the meaning of Article 1(7) of Directive (EU) 2016/1148, and should thus prevail over national measures implementing the Directive. As a result, the abovementioned SIPS should be excluded from the scope of application of the draft regulation.

3.7 In line with the requirements set out in Directive (EU) 2016/1148[25], Regulation (EU) No 795/2014 (ECB/2014/28) already provides competent authorities 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[26]. Additionally, the proposed regulation amending Regulation (EU) No 795/2014 (ECB/2014/28) further enhances competent authorities' powers to conduct onsite inspections and request independent reviews of and investigations into the functioning of the systems[27].

3.8 Similarly to SIPS that are governed by Regulation (EU) No 795/2014 (ECB/2014/28), the other two categories of non-SIPS, namely prominently important retail payment systems (PIRPS) and other retail payment systems (ORPS), are subject to comparable oversight standards. According to the Eurosystem Revised Oversight Framework for retail payment systems[28], both PIRPS and ORPS are subject to the CPMI-IOSCO Principles, in particular Principle 17 on operational risk[29].

3.9 While the objective of the draft regulation is to implement Article 5(1) of Directive (EU) 2016/1148 by identifying the operators of essential services with an establishment within the territory of Germany, it is questionable whether the identified payment systems can be considered as having 'effective and real exercise of activity through stable arrangements' within Germany[30]. While it is acknowledged that the critical infrastructures identified are subject to German law, the governing law should not be considered as a determining factor in assessing their critical nature with regard to German territory, as in many cases the physical infrastructure is to a relevant extent located outside the jurisdiction of Germany[31].

4. Impact of the draft regulation on TARGET2-Securities

4.1 In light of the abstract criteria set out in the draft regulation referred to in paragraph 1.3, the ECB understands that TARGET2-Securities (T2S) may also fall within the scope of the draft regulation.

---

24 See Article 1(9)(a) and (b) of the proposed regulation amending Regulation (EU) No 795/2014 (ECB/2014/28).

25 See Article 14(3).

26 See Article 21 of Regulation (EU) No 795/2014 (ECB/2014/28).

27 See Article 1(12)(b) and (c) of the proposed regulation amending Regulation (EU) No 795/2014 (ECB/2014/28).

28 Published on the ECB's website at www.ecb.europa.eu.

29 This includes Key Considerations 1, 3 and 5 from Principle 17.

30 See recital 21 of Directive (EU) 2016/1148.

31 With regard to TARGET2, this is only true for the TARGET2-ECB and TARGET2-Deutsche Bundesbank components. It should also be noted that EURO1 and STEP2-T are operated by a legal entity incorporated in France.

4.2 T2S is a service set up by the Eurosystem to support securities settlement in central bank money, to be provided to central securities depositories (CSDs) as part of the Eurosystem's tasks in accordance with Articles 17, 18 and 22 of the Statute of the ESCB. T2S is based on a single technical platform integrated with central bank real time gross settlement systems[32]. It is systemically important, as it provides critical core settlement services to CSDs.

4.3 In line with the Governing Council decision in its Eurosystem Oversight Policy Framework of July 2011, T2S falls under the Eurosystem oversight competences under Articles 127(2) of the Treaty and Article 3(1) and Article 22 of the Statute of the ESCB[33]. These competences are exercised in accordance with the CPMI-IOSCO Principles. The Eurosystem oversight function over T2S is similarly recognised in the T2S Framework Agreement, which is the core T2S contractual document that sets out the rules governing the provision of T2S services by the Eurosystem to CSDs[34]. In addition, in conducting the oversight of T2S, the Eurosystem cooperates with national authorities responsible for the oversight and supervision of CSDs connected to T2S on the basis of a memorandum of understanding between the ECB and those authorities. To consider T2S as falling under the scope of the draft regulation would interfere with the Eurosystem competences stemming from the Treaty, and the draft regulation should be amended in order to clearly exclude T2S from its scope.

5. Impact of the draft regulation on payment instruments overseen by the Eurosystem

5.1 Card-based transactions and conventional payment transactions should not fall under the scope of the draft regulation as this would interfere with the Eurosystem's existing supervisory and oversight competences.

5.2 While infrastructures related to card-based transactions and conventional payment transactions, e.g. credit transfers and direct debits may fall within the scope of the draft regulation, it should be noted that the Eurosystem Oversight Policy Framework identifies payment instruments, such as cards, credit transfers, direct debit and e-money, as an 'integral part of payment systems', and thus includes these within the scope of its central bank 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 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.

5.3 While payment service providers (PSPs) that provide payment services via payment instruments are supervised by competent authorities, the underlying critical financial market infrastructures are overseen by the Eurosystem. With regard to ensuring a high level of NIS, PSPs are subject to Directive (EU) 2015/2366 of the European Parliament and of the Council[35], which is applicable as of January 2018. The Directive sets out stringent guidelines on major incident reporting under

32 See Article 1(1) of Guideline ECB/2012/13.

33 See Section 4.4 of the Eurosystem oversight policy framework, revised version (July 2016), available on the ECB's website at www.ecb.europa.eu.

34 See Article 18 thereof.

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).

Article 96, on security measures for operational and security risk under Article 95, and on regulatory technical standards on strong customer authentication and secure communication under Article 98. These guidelines were drafted by the European Banking Authority in cooperation with the ECB.

6. Impact of the draft regulation on critical service providers

6.1 Contrary to the explanatory memorandum to the draft regulation, which explicitly lists the Society for Worldwide Interbank Financial Telecommunication (SWIFT) as an infrastructure subject to the Law on IT security, the draft regulation should exclude SWIFT from its scope. It supplies secure messaging services in a vast number of countries, and is a limited liability cooperative company established in Belgium whose infrastructure hubs are not located within the territory of Germany. Nationale Bank van België / Banque Nationale de Belgique acts as the lead overseer of SWIFT, and conducts, on the basis of a cooperative oversight arrangement, oversight in respect of SWIFT in cooperation with the other G10 central banks, including the ECB and the Deutsche Bundesbank.

6.2 The G10 overseers recognise that the main focus of oversight is SWIFT's operational risk, as this is considered to be the primary risk category through which SWIFT could pose a systemic risk to the financial system in the Union. In this regard, the SWIFT Cooperative Oversight Group has developed a specific set of principles and high level expectations that apply to SWIFT, such as risk identification and management, information security, reliability and resilience, technology planning and communication with users. The G10 overseers subject SWIFT to an intense form of oversight, and expect that SWIFT specifically adheres to the CPMI-IOSCO Guidance on cyber resilience and other international standards on IT Security, which exceed the requirements set out in Directive (EU) 2016/1148.

7. Impact of the draft regulation on other types of financial market infrastructures

7.1 While central clearing counterparties (CCPs) and CSDs may fall within the scope of the draft regulation, it is noteworthy that such financial market infrastructures are already strictly regulated and supervised by different authorities under Regulation (EU) No 648/2012 and Regulation (EU) No 909/2014 of the European Parliament and of the Council[36], which set out requirements pertaining to operational risk. Furthermore, both types of financial market infrastructures should take note of the CPMI-IOSCO Cyber Guidance, which is applicable to all financial market infrastructures.

7.2 In addition to the supervisory competences entrusted to national competent authorities under Regulation (EU) No 648/2012 and Regulation (EU) No 909/2014, it should be noted that national authorities, in particular the members of the ESCB, may be entrusted with oversight competences in relation to those financial market infrastructures. In this regard, recital 11 of Regulation (EU) No 648/2012 clarifies that one of the basic tasks to be carried out through the ESCB is to promote the smooth operation of payment systems. In this respect, the members of the ESCB execute oversight by ensuring efficient and sound clearing and payment systems, including CCPs. Further, Regulation (EU) No 648/2012 is without prejudice to the responsibilities of the ECB and the NCBs

36 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).

to ensure efficient and sound clearing and payment systems within the Union and with other countries.

7.3 In the same vein, as regards CSDs, recital 8 of Regulation (EU) No 909/2014 states that the Regulation should be without prejudice to the responsibilities of the ECB and the NCBs to ensure efficient and sound clearing and payment systems within the Union and other countries and that the Regulation should not prevent the members of the ESCB from accessing information relevant for the performance of their duties, including the oversight of CSDs and other financial market infrastructures.

7.4 Therefore, the ECB considers that the potential coverage of CCPs and CSDs within the scope of the draft regulation could interfere with the existing supervisory and oversight competences. Thus, the draft regulation should be amended in order to (a) clarify that the BSI's responsibilities under the draft regulation are without prejudice to and are aligned with the tasks of the competent authorities, including the members of the ESCB responsible for the supervision and oversight of the CCPs and CSDs, and (b) avoid the application to those financial market infrastructures of any requirements stemming from the draft regulation that could overlap with the *lex specialis* requirements applicable to CCPs and CSDs under their respective supervisory and oversight frameworks.

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

Done at Frankfurt am Main, 6 April 2017.

[*signed*]

The President of the ECB

Mario DRAGHI