CER

The Voice of European Railways

POSITION PAPER

CER comments on the Commission's Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union (COM(2013) 48 final)

COMMUNITY OF EUROPEAN RAILWAY AND INFRASTRUCTURE COMPANIES - COMMUNAUTÉ EUROPÉENNE DU RAIL ET DES COMPAGNIES D'INFRASTRUCTURE - GEMEINSCHAFT DER EUROPÄISCHEN BAHNEN UND INFRASTRUKTURGESELLSCHAFTEN

CER aisbl Avenue des Arts, 53 B-1000 Bruxelles Tel: +32 2 213 08 70 Fax: +32 2 512 52 31 contact@cer.be www.cer.be

ABOUT CER

The Community of European Railway and Infrastructure Companies (CER) brings together more than 80 European railway undertakings, infrastructure companies and vehicle leasing companies, including long-established bodies, new entrants, and both private and public-sector organisations. In EU, EFTA and EU accession countries, CER members represent about 75% of the rail network length, more than 85% of the rail freight business and over 90% of rail passenger operations, with 1.2 million jobs directly created by CER members. CER promotes a strong rail industry that can form the basis of a long-term sustainable European transport system.

BACKGROUND

As part of the 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace', the European Commission (EC) adopted in February 2013 the proposal for a 'Directive concerning measures to ensure a high common level of network and information security across the Union' (COM(2013)048). The goal of the proposed directive should be achieved by requiring the Member States (MS) to increase their preparedness to handle incidents and improve their cooperation with each other, and by requiring, inter alia, operators of critical infrastructure (e.g. transport) to adopt appropriate steps to manage security risks and report serious incidents to the national authorities.

CER'S POSITION

CER welcomes the Commission's proposal and the efforts made to ensure a high level of network and information security in all MS. Although we realise the importance of this issue, CER expresses concerns about some of the aspects of the proposed directive that need to be further clarified.

In particular we call for the following aspects to be taken into account:

- In general, the proposal reflects a new way of delivering information from market operators to competent authorities. However, it takes little or no account of the existing data flows to a range of different (national and international) authorities. CER would welcome the EC first investigating the existing data streams to identify any gaps. In particular, in the case of cargo transport under customs and excise supervision, the data streams customers-railway-authorities is comprehensive and already within the scope of security interests. CER considers it is important to avoid any unnecessary duplication of data streams.

- Compared to other (cargo) transport modes, the existing available data (in particular based on the consignment note and the procedures/manuals/systems behind it) are quite comprehensive. These (which also function well from a security perspective) data management and related procedures and systems must not be overruled or undermined by new European initiatives.

- Even though the introduction of delegated acts may make the legislative process more efficient, MS, the European Parliament (EP) but also market players have very little ability to influence it. Thus, CER is in favour of a more open and consultative approach. (Art. 9.2, Art. 10.5, Art 14.5 and Art. 18)

- To avoid overlaps, a clear separation of responsibilities between authorities involved, such as competent authorities, law enforcement national authorities and data protection authorities, should be specified more precisely. (Art. 6.5, Art. 15.4 and Art. 15.5)

- The level of network and information security is very uneven across the Union. Thus, it is essential that a minimum set of security standards be defined and implemented, by the MS. The operational guidelines to be followed by the MS should also be further specified. The alignment of security levels of network and information systems across the EU has to be carried out in view of fair as well as anti-discriminatory competition.

- To ensure an 'effective, efficient and secure cooperation of the competent authorities via the network referred to in Article 8' (Art. 6.3) the different systems in each MS would also have to be brought in line with some common standards, e.g. for storing, transmitting and receiving of information regarding risks and incidents affecting network and information systems. These should also be defined.

- The cooperation network would deal with very sensitive data. It should be clear from the beginning who would be in charge of this network and how and for whom the collected data would be accessible. The proposal should not only take into account and safeguard data protection but also the business interests of market operators. (Art. 8)

- Especially exchange of non-confidential information and best practices (Art. 8.3.g) as well as participation in NIS exercises at Union level (Art. 8.3.i) are activities that would be not only

profitable for competent authorities but also for market operators. Thus it is necessary to involve market operators in some of the activities of the cooperation network.

- While market operators already have some measures to secure their network and information systems, since it is also in their interest to ensure a high level of network and information security in order to prevent potential incidents, it is vital to know their suitability to the new requirements set out in the proposal as complying with this requirement may imply some investments. The EC should consider measures that could help reduce the costs as well as additional administrative burden.

- The requirements placed on market operators are generally decided on by the MS (through the competent authority). This is very welcome as it provides flexibility and supports a risk based approach rather than imposing prescriptive EU-wide requirements. (Art. 14, Art. 15). As stated in the proposal, Member States shall ensure that 'market operators take appropriate technical and organisational measures to manage the risks posed to the security of the networks and information system' (Art. 14.1) and also 'investigate cases of non-compliance of market operators' with, inter alia, this obligation (Art. 15.1). However, how is it possible to define and set up 'appropriate' measures responding to very quickly evolving and very dynamic cyber-threats? Market operators are equally at risk as society and economy when facing cyber-attacks that have the potential to very seriously damage a company's reputation and credibility and hence the public's confidence in its ability to manage its services. The security requirements should be welcome as long as they help to raise awareness and increase the knowledge about potential risks and how to mitigate them as well as serve to highlight weaknesses which leave market operators vulnerable to cyber-attacks.

- In the event of an incident, it is important that the decision to publicly disclose, or not, aspects relating to this event must be under the responsibility of the local authority or the operator. Police forces should be also involved in the evaluation of such cases. Namely, the requirement to report incidents and make this information publicly available raises a potential concern as it could lead to reputational damage. The question is whether making information on successful cyber-attacks public would lead to a decrease of cyber-attacks per se. CER would like to express concerns that publishing data about successful attacks might give an incentive to amateur hackers as it will bring them publicity. (Art. 14.4)

- The proposal should also take into consideration that there are many companies having outsourced their IT servers thus relying on information from cloud computing service providers. Consequently, these companies will not always be able to report incidents.

- The benefits of reporting security breaches are unclear. Simply requiring market operators to comply with reporting requirements will result in minimal reporting (in terms of numbers of reports made and their content). The aim should instead be to encourage a culture of voluntary sharing. Market operators should be incentivised to report, for example by receiving practical assistance and a flow of information from as well as to the national competent authorities. Care is also needed to ensure that those organisations with robust security in place – and which are hence more likely to be aware of and therefore report security breaches – are not penalised while those companies without such protection and which therefore may be unaware of attacks go unnoticed.

SUGGESTIONS FOR AMENDMENTS

Amendment 1

EC proposal	*Amendment*
Article 1 – paragraph 7 (new)	
	(7) Where information is considered confidential in accordance with Union and national rules on business confidentiality, such confidentiality shall be ensured when carrying out the activities and fulfilling the objectives set by this Directive.

Justification

A lot of information provided by market operators is sensitive and commercially confidential and should be treated accordingly.

Amendment 2

EC proposal	*Amendment*
Article 6 – paragraph 7 (new)	
	(7) All persons who require access to information classified as confidential shall be appropriately cleared before such access is authorised.

Justification

A lot of information provided by market operators is sensitive and commercially confidential and should be treated accordingly.

Amendment 3

EC proposal	*Amendment*
Article 6 – paragraph 8 (new)	
	(8) The competent authority shall provide assistance to market operators in case of incidents.

Justification

Market operators are equally at risk as society and economy. The competent authority should assist market operators in resolving incidents.

Amendment 4

EC proposal	*Amendment*
Article 8 – paragraph 2	
(2) The cooperation network shall bring into permanent communication the Commission and the competent authorities. When requested, the European Network and Information Security Agency ("ENISA") shall assist the cooperation network by providing its expertise and advice.	(2) The cooperation network shall bring into permanent communication the Commission and the competent authorities. When requested, the European Network and Information Security Agency ("ENISA") shall assist the cooperation network by providing its expertise and advice. ***Market operators shall also participate to the cooperation network referred to in paragraphs 3(g)-(i).***

Justification

The involvement of market operators in these activities will be profitable for competent authorities as well as market operators. Exchange of experience and best practices will help to raise awareness and increase the knowledge about potential risks.

Amendment 5

EC proposal	*Amendment*
Article 8 – paragraph 4	
(4) The Commission shall establish, by means of implementing acts, the necessary modalities to facilitate the cooperation between competent authorities and the Commission referred to in paragraphs 2 and 3. Those implementing acts shall be adopted in accordance with the consultation procedure referred to in Article 19(2).	(4) The Commission shall establish, by means of implementing acts, the necessary modalities to facilitate the cooperation between competent authorities, ~~***and***~~ the Commission and ***market operators*** referred to in paragraphs 2 and 3. Those implementing acts shall be adopted in accordance with the consultation procedure referred to in Article 19(2).

Justification

The involvement of market operators in these activities will be profitable for competent authorities as well as market operators. Exchange of experience and best practices will help to raise awareness and increase the knowledge about potential risks.

Amendment 6

EC proposal	*Amendment*
Article 9 – paragraph 2	
(2) The Commission shall be empowered to adopt delegated acts in accordance with Article 18 concerning the definition of the criteria to be fulfilled for a Member State to be authorized to participate to the secure information-sharing system, regarding: (a) the availability of a secure and resilient communication and information infrastructure at national level, compatible and interoperable with the secure infrastructure of the cooperation network in compliance with Article 7(3), and (b) the existence of adequate technical, financial and human resources and processes for their competent authority and CERT allowing an effective, efficient and secure participation in the secure information-sharing system under Article 6(3), Article 7(2) and Article 7(3).	***deleted***

Justification

The European Parliament, the Council but also market operators should have the ability to influence the legislative procedure. Time limit for invoking right of opposition and revocation is too short.

Amendment 7

EC proposal	*Amendment*
Article 10 – paragraph 5	
(5) The Commission shall be empowered to adopt delegated acts in accordance with Article 18, concerning the further specification of the risks and incidents triggering early warning referred to in paragraph 1.	***deleted***

Justification

The European Parliament, the Council but also market operators should have the ability to influence the legislative procedure. Time limit for invoking right of opposition and revocation is too short.

Amendment 8

EC proposal	*Amendment*
Article 14 – paragraph 4	
(4) The competent authority may inform the public, or require the public administrations and market operators to do so, where it determines that disclosure of the incident is in the public interest. Once a year, the competent authority shall submit a summary report to the cooperation network on the notifications received and the action taken in accordance with this paragraph.	(4) The competent authority may inform the public, ***~~or require the public administrations and market operators to do so~~***, where it determines that disclosure of the incident is in the public interest. ***Publicity of incidents reported to the competent authorities should duly balance the interest of the public in being informed about threats with possible reputational and commercial damages for the market operators reporting incidents. In the implementation of the notification obligations, competent authorities should pay particular attention to the need to maintain information about product vulnerabilities strictly confidential prior to the release of appropriate security.*** Once a year, the competent authority shall submit a summary report to the cooperation network on the notifications received and the action taken in accordance with this paragraph.

Justification

The competent authority should disclose only information that can help to prevent incidents. Publicity of incidents should not be associated with any market operator. Much of information provided by market operators is sensitive and commercially confidential and should be treated accordingly.

Amendment 9

EC proposal	*Amendment*
Article 14 – paragraph 5	
(5) The Commission shall be empowered to adopt delegated acts in accordance with Article 18 concerning the definition of circumstances in which public administrations and market operators are required to notify incidents.	***deleted***

Justification

The EP, the Council but also market operators should have the ability to influence the legislative procedure. Time limit for invoking right of opposition and revocation is too short.

Amendment 10

EC proposal	*Amendment*
Article 14 – paragraph 6	
(6) Subject to any delegated act adopted under paragraph 5, the competent authorities may adopt guidelines and, where necessary, issue instructions concerning the circumstances in which public administrations and market operators are required to notify incidents.	(6) ~~***Subject to any delegated act adopted under paragraph 5, t***~~The competent authorities may adopt guidelines and, where necessary, issue instructions concerning the circumstances in which public administrations and market operators are required to notify incidents.

Justification

Delegated acts were removed in Article 14.5.

Amendment 11

EC proposal	*Amendment*
Article 18	
Exercise of the delegation (1) The power to adopt the delegated acts is conferred on the Commission subject to the conditions laid down in this Article. (2) The power to adopt delegated acts referred to in Articles 9(2), 10(5) and 14(5) shall be conferred on the Commission. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the five-year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period. (3) The delegation of powers referred to in Articles 9(2), 10(5) and 14(5) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the powers specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated act already in force. (4) As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council. (5) A delegated act adopted pursuant to Articles 9(2), 10(5) and 14(5) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.	***deleted***

Justification

The EP, the Council but also market operators should have the ability to influence the legislative procedure. Time limit for invoking right of opposition and revocation is too short.

Disclaimer

Community of European Railway and Infrastructure Companies (CER) AISBL

Avenue des Arts 53
B-1000 Brussels
Belgium

Tel +32 2 213 08 70
Fax +32 2 512 52 31
contact@cer.be