EUROPEAN
COMMISSION

Brussels, 4.10.2017
COM(2017) 476 final/2

CORRIGENDUM

This document corrects document COM(2017)476 final of 13.09.2017

Concerns the English language version.

Correction of errors of a clerical and formatting nature, as well as correction of cross-references and the use of certain defined terms.

The text shall read as follows:

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union

Introduction

The Directive (EU) 2016/1148 on the security of network and information systems across the Union[1] (hereinafter referred to as "NIS Directive" or the "Directive") adopted on 6 July, 2016 is the first EU horizontal legislation addressing cybersecurity challenges and a true game changer for cybersecurity resilience and cooperation in Europe.

The Directive has three main objectives:

- Improving national cybersecurity capabilities;
- Building cooperation at EU level; and
- Promoting a culture of risk management and incident reporting among key economic actors, notably operators providing essential services (OES) for the maintenance of economic and societal activities and Digital Service Providers (DSPs).

The NIS Directive is a cornerstone of the EU's response to the growing cyber threats and challenges which are accompanying the digitalisation of our economic and societal life, and its implementation is therefore an essential part of the cybersecurity package presented on 13 September, 2017. The effectiveness of the EU's response is inhibited as long as the NIS Directive is not fully transposed in all EU Member States. This was also recognized as a critical point in the Commission's 2016 Communication on Strengthening Europe's Cyber Resilience System.[2]

The novelty of the NIS Directive and the urgency of tackling a fast evolving cyber-threat landscape warrant particular attention to the challenges faced by all actors in ensuring the timely and successful transposition of the Directive. In view of the transposition deadline of 9 May, 2018, and the deadline for the identification of operators of essential services of 9 November, 2018, the Commission has been supporting the Member States' transposition process and their work in the Cooperation Group to this end.

The present Communication with its annex is based on the Commission's preparatory work and analysis related to the implementation of the NIS Directive thus far, on the input of the European Agency for Network and Information Security (ENISA) and on the discussions held with Member States in the transposition phase of the Directive, notably within the Cooperation Group.[3] This Communication complements the considerable efforts taken so far, in particular through:

- The intensive work of the Cooperation Group, which has agreed to a working plan focusing predominantly on the transposition of the NIS Directive, and in particular on the question of identification of operators of essential services and their obligations concerning security requirements and incident notifications. While the Directive

[1] 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. The Directive entered into force on 8 August, 2016.
[2] COM(2016) 410 final.
[3] A mechanism for strategic cooperation between Member States under the NIS Directive, Article 11.

provides for discretion in transposing provisions related to operators of the essential services, Member States recognised the importance of a harmonised approach in this respect[4].

- The establishment and swift operation of the Network composed of Computer Security Incident Response Teams (CSIRTs) in accordance with Article 12(1) of the Directive. Since then, this network has started to lay the foundations for structured operational cooperation at European level.

For both the policy and the operational levels represented by these two structures, the full engagement of all Member States is essential to achieve the goal of a high common level of security of network and information systems in the Union.

The present Communication with its annex will reinforce these efforts by bringing together and comparing best practices from the Member States which are relevant for the implementation of the Directive, by providing further guidance on how the Directive should be implemented and through more detailed explanations on specific provisions. The overarching goal is to support Members States to achieve an effective and harmonised implementation of the NIS Directive across the EU.

This Communication will be further complemented by the upcoming Commission's Implementing Regulation on further specification of elements and parameters related to the security and incident notification requirements for digital service providers, pursuant to Article 16(8) of the NIS Directive. The Implementing Regulation will facilitate the implementation of the Directive with respect to obligations concerning digital service providers.[5]

The Communication presents the key conclusions of the analysis of the issues which are seen as important points of reference and potential inspiration from the point of view of the transposition into national law. Here the primary focus is on provisions related to Member States' capabilities and obligations concerning entities that are within the scope of the Directive. The annex provides a more detailed examination of those areas where the Commission sees the greatest value in providing practical transposition guidance through the explanation and its interpretation of certain Directive's provisions, and through presentation of best practices and accumulated experience with the Directive so far.

Towards the effective implementation of the NIS Directive

The objective of the NIS Directive is to achieve a high common level of security of network and information systems within the EU. This means improving the security of the Internet and

[4] The Cooperation Group is currently working on reference guidance documents concerning among others: the criteria defining the criticality of an operator pursuant to Article 5(2) of the Directive; the circumstances in which operators of essential services are required to notify incidents based on Article 14(7) of the Directive; and the security requirements for operators of essential services, in line with Articles 14(1) and 14(2).

[5] The draft of the Implementing Regulation is made available for public consultation at https://ec.europa.eu/info/law/better-regulation/have-your-say_en

private networks and information systems underpinning the functioning of our society and economy. The first important element in this regard is the Member States' preparedness which should be ensured by having national cybersecurity strategies in place, as described in the Directive, by the work of the CSIRTS, and by that of the competent national authorities.

Comprehensiveness of national strategies

It is important that Member States seize the opportunity of the transposition of the NIS Directive to review their national cybersecurity strategy in the light of the gaps, best practices and new challenges addressed in the Annex.

While the Directive understandably focuses on those companies and services that are of particular critical importance, it is the cybersecurity of the economy and society as a whole that needs to be addressed in a wholistic and consistent manner, given the ever increasing reliance on ICT. Therefore, the adoption of comprehensive national strategies which go beyond the minimum requirements of the NIS Directive (i.e. covering more than the sectors and services listed respectively in the Directive's Annex II and III) would increase the overall level of security of network and information systems.

As cybersecurity is still a relatively new and rapidly expanding area of public policy, new investments are required in most cases, even if the overall situation in public finances calls for cuts and savings. Taking ambitious decisions to secure adequate financial and human resources which are indispensable for the effective implementation of national strategies, including the sufficient resourcing of national competent authorities and CSIRTs, is therefore fundamental for the achievement of Directive's objectives.

Effectiveness of implementation and enforcement.

The need to designate respective national competent authorities and single points of contacts is outlined in the Directive's Article 8 and is a key element to ensure an effective implementation of the NIS Directive and cross-border cooperation. Here both more centralised and decentralised approaches have emerged in Member States. When Member States adopt a more decentralised approach with regard to the designation of national competent authorities, ensuring strong cooperative arrangements between numerous authorities and the single point of contact has proved to be of essence (*see Table 1 of section 3.2. of the Annex*). This would increase effectiveness of implementation and facilitate enforcement.

Drawing on previous experience in relation to Critical Information Infrastructure Protection (CIIP) may help to design an optimal model of governance for Member States, ensuring both effective sectoral implementation of the NIS Directive, as well as a coherent horizontal approach (*see section 3.1. of the Annex*).

Enhanced national CSIRTs' capabilities

Without effective and adequately resourced national CSIRTs across the EU, as laid out in Article 9 of the NIS Directive, the EU will remain too vulnerable to cross-border cyber threats. Member States could therefore consider extending the scope of CSIRTs beyond sectors and services that are included in the scope of the Directive (*see section 3.3 of the Annex*). This would enable national CSIRTs to provide operational support to cyber incidents that occur in companies and organisations which are not in the scope of the Directive but are also important for the society and economy. In addition, Member States could make full use of additional funding opportunities offered by the Cybersecurity Digital Service Infrastructures (DSI) programme of the Connecting Europe Facility (CEF), designed to enhance capabilities of national CSIRTs and cooperation among them (*see section 3.5 of the Annex*).

Consistency of the identification process of OES

In accordance with Article 5 of the NIS Directive Member States are required to identify the entities that will be considered operators of essential services by 9 November, 2018. In relation to this task, Member States could consider using consistently the definitions and guidance included in this Communication in order to ensure that similar type of entities playing a similar role in the internal market would consistently be identified as operators of essential services in other Member States. Member States could also consider extending the scope of the NIS Directive to public administrations, given the role they play for society and the economy as a whole (*see sections 2.1. and 4.1.3 of the Annex*).

Aligning national approaches to the identification of operators of essential services to a maximum extent, notably by following guidance developed by the Cooperation Group (*see section 4.1.2 of the Annex*) would be very useful, as it would lead to a more harmonised application of the Directive's provisions and thus reduce the risk of market fragmentation. In cases where operators of essential services provide essential services in two or more Member States, striving to reach an agreement between Member States in the context of the consultation process under Article 5(4)) on the consistent identification of entities, (*see section 4.1.7 of the Annex*) is essential, as this would avoid a different regulatory treatment of the same entity under different Member State jurisdictions.

Submission of information on identification of OES to the Commission

In accordance with Article 5(7), Member States are requested to provide to the Commission information on national measures allowing for the identification of OES, the list of essential services, the number of identified OES and the relevance of those operators for the sector. Furthermore, Member States are requested to provide thresholds, where such exist, used in the identification process to determine the relevant supply level or the importance of the particular operator for maintaining a sufficient level of supply. Member States could also consider sharing with the Commission the lists of identified operators of essential services and

if necessary on a confidential basis, as this would help to improve the accuracy and quality of the Commission's assessment (*see sections 4.1.5. and 4.1.6. of the Annex*).

Aligned approaches concerning security and incident notification requirements for OES

In relation to obligations concerning security requirements and incident notifications for operators of essential services (Article 14(1), (2) and (3)), an aligned approach regarding the security requirements and incident notifications in order to facilitate the compliance of OESs across EU Member State borders, would promote to the greatest extent possible a single market effect. The reference here remains the work on a guidance document within the Cooperation Group (*see sections 4.2. and 4.3. of the Annex*).

In case of a large scale cyber incident affecting several Member States, it is very likely that a mandatory incident notification is submitted by an OES or DSP pursuant to article 14(3) and 16(3) or by another entity which is not in the scope of the Directive on a voluntary basis pursuant to article 20(1). In line with the Commission Recommendation on Coordinated Response for Large-Scale Cybersecurity incidents and crises, Member States could consider aligning their national approaches so that they can provide as soon as possible, relevant information based on those notifications to the competent authorities or the CSIRT of other Member States concerned. Accurate and actionable information would be vital for reducing the number of infections or addressing vulnerabilities before they are exploited.

In the spirit of partnership in making the most from the NIS Directive, the Commission intends to extend support under the Connecting Europe Facility to all relevant stakeholders under this legislation. While the focus has been on CSIRT capacity building and on an enabling platform for swift and effective operational co-operation, thereby re-enforcing the CSIRT Network, the Commission will now explore how funding under Connecting Europe Facility can also benefit national competent authorities as well as operators of essential services and digital service providers.

Conclusion

In view of the impending deadline for the transposition of the NIS Directive into national legislation by 9 May, 2018, and in view of the deadline for the identification of operators of essential services by 9 November, 2018, Member States should take appropriate measures to ensure that the provisions and the cooperation models of the NIS Directive can provide the best possible EU-level tools to achieve a high common level of security of network and information systems across the Union. The Commission invites Member States to consider in this process the relevant information, guidance and recommendations contained in this Communication.

This Communication may be further supplemented by other actions, including those generated through ongoing work within the framework of the Cooperation Group.