Cross-border Dependencies

Guidelines for the Member States on voluntary information exchange on cross-border dependencies

CG Publication 01/2019

NIS Cooperation Group

January 2019

Glossary

Cross-border dependency – a critical reliance on a network or information system that is located in another member state and without which an essential service is unable to function;

Operator of Essential Services (OES) - A public or private entity of a type referred to in Annex II of the NIS Directive, which meets the criteria laid down in Article 5(2);

SPOC - national single point of contact on the security of network and information systems referred to, inter alia, in NISD Articles 8, 11 and 12;

Affected Member State (AMS) – Member State which is potentially affected by the loss of an essential service as a result of a cross-border dependency;

Originating Member State (OMS) – a Member State whose territory the operator and/or network and information system on which an essential service in another Member State is dependent upon, is located on;

Maximum Tolerable Downtime (MTD) - The amount of time critical network or information system without which a AMS essential service is unable to function, can be disrupted without causing significant harm to the Affected Member State essential service;

Recovery Time Objective (RTO) - The overall length of time a network or information system that is located in another Member State (OMS) can be in the recovery phase before negatively impacting the AMS essential service(s).

Introduction

The free provision and supply of services across borders is at the heart of the EU Single Market resulting in better availability for customers as well as opportunities and economies of scale for service providers. This has proven as true in all sectors covered by the NIS Directive. The cost of such openness, however, are inherent cross-border risks and dependencies that fundamentally affect the availability, integrity and confidentiality of such services and therefore could potentially fracture the public trust in the Digital Single Market. Cooperation and relevant information exchange between Member States would help to identify and mitigate such risks.

Target audience

This document addresses national competent authorities and/or single points of contact in the EU tasked with cyber risk management or implementing the NIS Directive.

Objective

The aim of these guidelines is to help Member States gather information on and map their cross-border dependencies and risks related to those dependencies which can eventually help them in applying nationally any risk mitigation measures deemed appropriate. They do not apply to information exchanges on such dependencies covered by the non-binding reference document on modalities of the consultation process in cases with cross-border impact as laid down in Article 5(4) to facilitate the assessment of the critical nature of operators of essential services.

Background and context

The problem related to cross-border dependencies in EU has quite a wide scope, as dependencies exist across borders of Member States and both along and across different sectors in which services are provided. The need to manage the risks to the essential services emanating from the cross-border provision of services within the EU is at the core of the NIS Directive starting from rec. 3 of the Directive. More specifically, article 5(4) of the NIS Directive creates a consultation process between Member States in order to exchange information in case of identified operators of essential providing services in more than one Member States, for which Cooperation Group already has endorsed a reference document. Member States who have received information about their dependencies through the consultation process of Article 5(4) should therefore take that as a basis in further discussions on their dependencies.

Additionally, articles 11 and 12 divide the relevant work on cross-border dependencies and impacts between Cooperation Group and CSIRTs Network. Articles 14 and 16 give further guidance related to the notification of cross-border impacts and to the need to understand the geographical spread of the impacts of incidents as part of

determining their significance. In particular, at the request of the competent authority or the CSIRT, the competent authority or the CSIRT shall inform the other affected Member State(s) if the incident has a significant impact on the continuity of essential services in that Member State.

While Member States may get information about their dependencies from the consultation process under article 5(4), understanding about existing dependencies across borders can also be developed through processes related to cyber risk analysis and management, both clearly national prerogatives and the substance of which are out of the scope of the given guidelines. In this case, Member States should use the present guidelines for their consultations on those dependencies with other Member States.

Sensitivity of Member States to the problem of cross-border dependencies and their tolerance of risks resulting from them can be quite different, depending on differences in national risk assessments or levels of digitalization in economies. These guidelines aim to keep that in mind while trying to offer a framework to use for all Member States if deemed necessary. Some Member States contributing to the process proposed to approach the problem differently in different sectors. The aim of these guidelines is not to do that, while clearly acknowledging that differences could exist between sectors. The aim is to provide guidelines that are general enough to be used across sectors. A cross-border dependency in the given guidelines is defined as a critical reliance of an essential service of an EU Member State on a network or information system that is located in another Member State, without which the given essential service is unable to function.

There are several benefits for knowing about cross-border dependencies[1] or mapping them, all of which are part of managing the risks related to essential services and protecting the population of Member States against the disruptions of essential services.

The aim of these guidelines is to help Member States gather information on and map their cross-border dependencies and risks related to those dependencies which can eventually help them in applying nationally any risk mitigation measures deemed appropriate. Therefore these guidelines try to establish a basic voluntary framework recommended for Member States' Single Point of Contacts (SPOC)[2]for communication and information sharing on cross-border dependencies. Because of the sector-specific nature of the information to be shared on cross-border dependencies, the SPOC may invite the relevant competent authorities under the NIS Directive to collaborate in this task and apply the same basic principles in that or Member States can use the given guidelines within their national respective framework as appropriate.

Voluntary nature of the Guidelines

[1] Member States can voluntarily ask for guidance from ENISA in categorizing cross-border dependencies.

[2] Definition of SPOC comes from NIS directive whereby each Member State shall designate a national single point of contact on the security of network and information systems ('single point of contact').

NIS Directive states voluntary notification shall not result in the imposition upon the notifying entity of any obligations to which it would not have been subject had it not given that notification. Therefore the given guidelines are voluntary for Member States to follow, on a best effort basis. More specifically, when an Affected Member State (AMS) has identified a cross-border dependency and decides to turn to Originating Member State (OMS) based on the given guidelines, neither side shall not be under any obligation to give out sensitive information about their services.

Framework for the information exchange on cross-border dependencies between the Member States:

First step – who should start the dialogue and why

The given guidelines can be used once any Member State has information about some cross-border dependencies of services that it has designated as essential services under the NIS Directive. Information about the cross-border dependencies can be acquired via national risk management efforts or process deriving from Council Directive 2008/114/EC, details of which are both beyond the scope of the given guidelines. Any Member State can also receive information about its dependencies based on the consultation process deriving from NIS Directive Article 5(4), for which Cooperation Group has already adopted relevant guidelines[3].

Although both AMS and OMS have potentially information about dependencies, only AMS is affected as a result of any unmitigated dependencies and therefore bears all responsibility for managing the risks from those. Therefore AMS is more likely interested to start the dialogue on dependencies between Member States and even if it chooses not to do it itself, can have no expectation towards OMS to do so. Information exchange[4] on cross-border dependencies shall be conducted by SPOCs of Member States as responsible authorities for coordinating issues related to security of network and information systems[5] as the SPOC designated under the NIS Directive is considered as a key national entity to undertake the information exchange and liaison function on behalf of each Member State[6]. However this does not preclude any Member State to use the given guidelines and principles as appropriate in their national context.

[3] CG Publication 07/2018

[4] It is important to take into account that Member States can have special requirements around information sharing and they therefore might require assurances for channels of information sharing, which may also be be delayed due to internal clearance processes.

[5] NIS Directive, rec.31

[6] According to article 8(4) of the Directive, the single point of contact shall exercise a liaison function to ensure cross-border cooperation of Member State authorities and with the relevant authorities in other Member States and with the Cooperation Group and the CSIRTs network. However, this does not preclude a Member State from choosing national authorities other than SPOCs and national competent authorities under the Directive to undertake this task.

Dialogue on cross-border dependencies takes place on a best effort basis from both OMS and AMS and with respect to the need-to-know principle in order to avoid unnecessary sharing of information amongst different national SPOCs or other national authorities.

Second step – content of the dialogue

Information to be provided and required by the AMS:

When the AMS has information about a cross-border dependency of any of its essential services, it may wish to turn to OMS under whose jurisdiction is the service or network and information system covered by the NIS Directive, upon which the given service is dependent on. In order to create a basis for clear information exchange, the AMS will need to provide the following information to OMS:

- **Description of the service or network and information system in OMS, upon which an essential service in AMS is dependent upon.**
- **Description of the service provider (Operator of essential service) in AMS**
- Questions related to **network and information security of the service in OMS that the essential service of AMS is dependent upon** and that AMS needs more information about in order to support its national risk management process. These questions may notably include **information about security measures or requirements of network and information security that are in place for the given service or network and information system. For example about possible measures or requirements related to service continuity like Maximum Tolerable Downtime (MTD) or Recovery Time Objective (RTO).**

The OMS SPOC should on a best effort basis evaluate the questions received, provide an answer or gather further details from other national or relevant sectoral authorities with the aim of providing a response to the AMS as soon as possible. OMS SPOC should also indicate to AMS as soon as possible if any of the questions can not be answered or if more time would be required to answer the given questions.

Third step - Based on the received information the AMS can:

- **Establish further discussion with the OMS SPOC on possibilities for mitigating identified dependencies**
- **Establish additional risk mitigation measures within AMS, taking into account the results of the dialogue.**

Non-disclosure and Data Protection measures applicable in the management of cross-border risks between SPOCs

Same principles as in NIS directive states for information sharing between Member States will apply to information exchange established by these guidelines:

This Directive should be without prejudice to the possibility for each Member State to take the necessary measures to ensure the protection of the essential interests of its security, to safeguard public policy and public security, and to allow for the investigation, detection and prosecution of criminal offences. In accordance with Article 346 of the Treaty on the Functioning of the European Union (TFEU), no Member State is to be obliged to supply information the disclosure of which it considers to be contrary to the essential interests of its security. In this context, Council Decision 2013/488/EU and non-disclosure agreements, or informal non-disclosure agreements such as the Traffic Light Protocol, are of relevance.

Annex - explanatory diagram on the voluntary information exchange between Member States on cross-border dependencies