

# Overview of the EU's draft NIS 2 Directive

#### Anticipating stronger security requirements

The EU Commission recently proposed a revision to its Directive on Security of Network and Information Systems (NIS). The existing NIS Directive ("NIS 1") requires EU Member States to enact security safeguards for critical infrastructure-like entities and large digital services. The proposed revision - nicknamed "NIS 2" - would replace NIS 1 and require EU Member States to implement stronger security safeguards and stricter enforcement. This post provides an analysis of the NIS 2 proposal and comparison with the existing NIS Directive.

- Here is the NIS 2 proposal and annex. (See link at bottom of the page, after the public statement.)
  - Here is the NIS 1 document. (See link at top of the public statement.)
  - Here is the EU implementing regulation for NIS 1.

At the present time, the NIS 2 proposal will likely be subject to months of negotiation among EU lawmakers, and the text will likely change somewhat before enactment. However, by reviewing the NIS 2 proposal, we can at least anticipate the direction of changes that regulated organizations may be subject to under a revamped NIS Directive.

Rapid7 is supportive of efforts to ensure critical infrastructure security is strengthened in proportion to the risks, and there are a number of elements in the NIS 2 proposal we view as beneficial. These include recognition of the importance of coordinated vulnerability disclosure, and the need for a central coordinating body in the EU that will align with, and participate in, international programs and practices. We are also in strong agreement regarding the usefulness of Recital 69 (more details below) in clarifying allowable security activity under GDPR. However, there are also elements of the current NIS 2 proposal that appear overbroad, such as potentially applying to all cloud computing services simply because they are cloud-based. Likewise, the incident notification requirements would see regulated entities notify authorities of "any significant cyber threat" that "could have potentially resulted in a significant incident," which risks a large number of unnecessary threat reports.

We look forward to continuing to work with EU officials to make NIS 2 streamlined, clear, and effective.

1

#### **Background**

The 2016 Network and Information Systems Directive (NIS 1) was the first EU-wide cybersecurity law. The EU Member states (and the UK, an EU Member State at the time) issued local regulations to implement the Directive. In 2018, the EU also issued an implementing regulation for NIS 1 to provide additional specifics on security elements that are expected of "digital service providers." (Note: EU Directives tell a Member State the broad outcome, but leave the details open to the State to "transpose" into national laws. EU Regulations issue more detailed requirements that bind Member States.)

The NIS 2 Directive is one of a trio of cybersecurity documents the EU Commission proposed in Dec. 2020. The other two are the EU Cybersecurity Strategy (which calls for updates to NIS, among other things), and a directive on critical infrastructure resilience (which defers to NIS 2 on cybersecurity issues, and reminds critical infrastructure and Member States to follow NIS 2 cybersecurity requirements).

While this post focuses on proposed changes in requirements for regulated entities, it's worth noting that the NIS 2 Directive would do many other things as well. For example, the proposal would establish a framework for EU-wide coordinated vulnerability disclosure and set up an ENISA-operated vulnerability registry. Recital 69 of the NIS 2 proposal would also explicitly confirm that cybersecurity info-sharing, vulnerability disclosure, and awareness activities are within the scope of legitimate interest for security under GDPR - a welcome clarification.

## **Regulated Sectors**

The NIS 1 Directive applies to two categories of sectors, with the NIS 1 Directive's Annex listing types of entities that fall within these sectors. The proposed NIS 2 Directive, <u>as detailed in its Annex</u>, would rename those categories, expand the number of regulated sectors, and significantly expand the types of entities that fall within these sectors. One area that needs clarity is the scope of application to cloud computing services, as the language presently reads as though *all* cloud-based services are covered, which would be out of step with the concept of these as "essential" entities. The sector categories are important in relation to how the Directive is to be enforced - see the "Enforcement, and penalties" section below.

Under NIS 1, Member States designated the specific organizations as being regulated based on how strategically important the entities are to the State (i.e., market size, national security, economic impact, etc.). [NIS 1, Art. 6] However, under NIS 2, the Member States do not need to designate a specific organization as regulated. Instead, NIS 2 would require all essential and important entities to register with ENISA, and ENISA would notify Member States of entities in their jurisdiction. [NIS 2, Art. 25]

Below is a comparison of the sectors from their respective annexes, however please note that the NIS 2 directive expands on the types of entities as well.

Sectors covered by NIS 1	Sectors covered by NIS 2 proposal
"Operators of essential services" category	"Essential entities" category
	All sectors from NIS 1
Healthcare providers	Additional health-related services - including pharma, some medical device manufacturers, researchers
Digital infrastructure - IXPs, DNS services, TLD registries)	Additional digital infrastructure services - cloud computing services, data centers, CDNs, network providers
Drinking water	Waste water
Transport	Space
Financial market infrastructure	Public Administration
Energy	
Banking	
"Digital service providers" category	"Important entities" category
Online marketplaces	Online marketplaces
Online search services	Online search services
Cloud services	Social networking services
	Food production & distribution
	Postal services
	Waste management
	Chemical manufacturers
	Manufacturing - medical devices, electronic products and equipment, machinery, vehicles and transport equipment

#### **Security requirements**

The NIS 1 Directive requires all EU Member States to adopt a national strategy for network and information system security, and requires Member States to establish security and reporting requirements for essential services and digital service providers. [NIS 1, Art. 1.2, 14, 16] The EU Commission also issued an <u>implementing regulation</u> to provide additional specifics on how Member States should regulate digital service providers, though not essential services.

The NIS 2 Directive would empower Member States to require essential and important entities to certify ICT products, services, and processes under specific EU cybersecurity certification schemes. [NIS 2, Art. 21] The proposed NIS 2 Directive would also expand on the security outcomes required under NIS 1, with a notable new section on supply chain security and a burdensome expansion of requirements to report any potential cyber threat that could cause a disruption.

Here is a high level breakdown of the changes:

	NIS 1 Directive	NIS 1 Implementing Regulation for digital service providers	NIS 2 proposal
Security program	Essential and digital services must take appropriate technical and organizational measures to manage risks to the security of networks and information systems.  [NIS 1, Art. 14.1, 16.1]		Same overarching security risk management requirement as NIS 1. [NIS 2, Art. 18.1]
	Essential and digital services must take appropriate measures to prevent and minimize the impact of security incidents. [NIS 1, Art. 14.2, 16.2]		This clause does not appear.
Risk assessment	Measures taken for the security of networks and information systems		Same as NIS 1, but risk analysis would also be a required security

	must be appropriate to the risks and reflect the state of the art. [NIS 1, Art. 14.1, 16.1]		measure. [NIS 2, Art. 18.2(a)]
Security safeguards	Virtually no detail on security requirements for essential services.  Digital services' measures must include - Security of systems and facilities, - Incident handling, - Business continuity, - Monitoring and testing, - Compliance with international standards. [NIS 1, Art. 16.1]	Much more detail on requirements for digital services' security measures, including  - Asset management,  - Secure system lifecycle management,  - Encryption where applicable,  - Access controls,  - Identifying system vulnerabilities,  - Incident detection.  [Implementing Reg., Art. 2]	Security measures for essential and important services shall include at minimum:  - Incident prevention, detection, and response, - Business continuity and crisis management, - Secure network and systems acquisition and maintenance, including vuln handling and disclosure, - Testing and auditing safeguard effectiveness, - Use of cryptography. [NIS 2, Art. 18.2]
Supply chain			Essential and important services must include supply chain in their security measures. [NIS 2, Art. 18.2(d)] They must consider specific suppliers' vulnerabilities and cybersecurity practices. [NIS 2, Art. 18.3] Supply chain includes network and systems acquisitions, data storage and processing services, and managed security services. [NIS 2, Art. 18.2(d)-(e)]
Workforce			The management of

and personnel		essential and important entities must approve their respective cybersecurity risk management measures, and follow regular cybersecurity training. [NIS 2, Art. 17]
Incident reporting	Essential and digital services must notify authorities of incidents having significant impact on services. [NIS 1, Art. 14.3-4, 16.3-4]	Notify the relevant competent authority and, where applicable, their customers of "any significant cyber threat" that "could have potentially resulted" in a substantial disruption or loss. [NIS 2, Art. 20.1-3]

## **Enforcement and penalties**

The NIS 1 Directive requires EU Member States to empower their supervisory authorities and to create penalties for noncompliance. The specific powers and penalties were left up to the EU Member States. For example, the UK (a Member State at the time) <u>announced</u> fines of up to £17 million or 4% of a company's global revenues, depending on the severity.

The NIS 2 Directive would continue to require EU Member States to work out the specifics, but would give much greater detail on the enforcement powers authorities must have, and a GDPR-like civil fine for noncompliance, with the intention to have stricter supervision as well as more consistent enforcement and penalties across Member States.

Here is a summary of the proposed changes:

NIS 1 enforcement	Proposed NIS 2 enforcement
Powers: EU Member State authorities must have powers to assess compliance and compel evidence from regulated entities. [NIS 1, Art. 15, 17] Member State authorities must have powers to issue binding instructions to regulated entities to remedy deficiencies. [NIS 1, Art. 15.3, 17.2(b)]	Powers: Essentially the same as NIS 1, but with much greater detail on what the authorities' powers must entail, such as security audits and scans based on risk assessments, and designating a monitoring officer to oversee compliance, etc. [NIS 2, Art. 29-30]

Supervision: Member State authorities shall supervise essential services at any time, even without evidence of noncompliance. [NIS 1, Art. 15] Authorities shall supervise digital services "ex post" - when aware of evidence of noncompliance. [NIS 1, Art. 17]	<b>Supervision:</b> Similar structure as NIS 1 - ongoing supervision for essential entities, and supervision for important entities when aware of noncompliance. [NIS 2, Art. 30.1-2]
Jurisdiction: Digital service providers are under the jurisdiction of the Member State where they have their "main establishment." [NIS 1, Art. 18, Recital 64] Little information on jurisdiction for essential services is provided.	Essential and important entities are under the jurisdiction of Member States where they provide services. Certain entities, like cloud computing service providers and other digital services, are under the jurisdiction of where they have their main establishment. [NIS 2, Art. 24] Member States must cooperate on cross-border cases. [NIS 2, Art. 34]
NIC 1 nanakina	B A NIO O It'
NIS 1 penalties	Proposed NIS 2 penalties
EU Member States must issue rules on penalties. Penalties must be effective and proportionate. [NIS 1, Art. 21] No further specifics.	Member States shall ensure imposition of fines are effective and proportionate for noncompliance. [NIS 2, Art. 31] These fines are in addition to the "binding instructions to remedy deficiencies, which may be issued by Member State authorities as part of their supervision, described above.

## **Next steps for NIS 2**

The proposed NIS 2 Directive is now subject to negotiations between the EU Council and the EU Parliament. There is no official public deadline for these negotiations, but it's likely a matter of months, not years. The text of the NIS 2 Directive will likely change before the final version is adopted, but it is unclear how much.

Under the current proposal, EU Member States would have 18 months to transpose the NIS 2 Directive after it is enacted. [NIS 2, Art. 38] The proposed NIS 2 Directive also expresses

willingness to issue additional implementing guidance on the security requirements at some point after enactment. [NIS 2, Art. 18.5]

## **Further reading**

- o <u>EU Commission NIS 2 Fact Sheet</u>
- o ENISA "NIS Investments" report on cybersecurity investment and NIS implementation
- o EU Commission "NIS Toolkit"
- o <u>UK National Cyber Security Centre Cyber Assessment Framework</u>

\* \*

For more information on how Rapid7 can help your organization comply with security requirements, please visit https://www.rapid7.com/solutions/compliance/