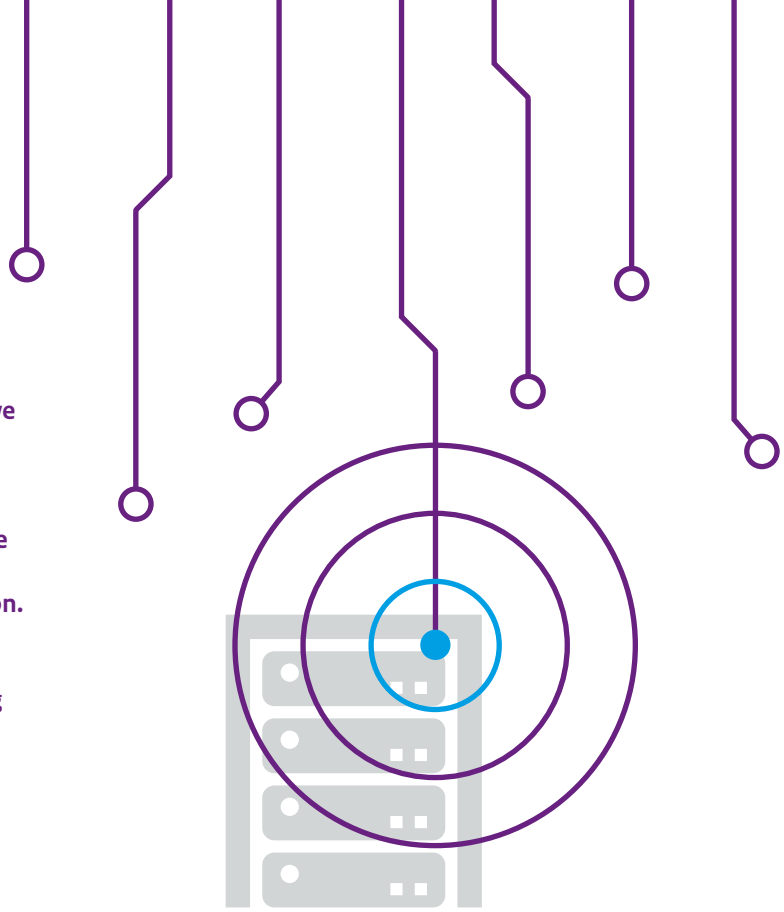
Dutch Authority for Digital Infrastructure
Ministry of Economic Affairs and Climate Policy

Network and Information Systems Security Act

This brochure contains general information on the European Directive on Security of Networks and Information Systems (NIS), the Network and Information Systems Security Act (*Wet Beveiliging Netwerk- en Informatiesystemen, Wbni*) and additional laws and regulations.



Introduction

It all seems so natural: electricity powers our homes, we can safely travel by train, water comes out of our taps and we can buy and sell anything we like over the Internet. All these things that we take for granted depend on network and information technology. These services can all be delivered reliably through properly functioning networks and correct, available information. However, networks and information are vulnerable. Organisations that provide essential services or digital services must reduce their vulnerability by maintaining sufficient resilience to threats.

The Dutch Authority for Digital Infrastructure supervises compliance with the Network and Information Systems Security Act (Wbni) for the energy sector, digital infrastructure and digital service providers. These organisations report security incidents in their network and information systems to the Dutch Authority for Digital Infrastructure.

The NIS Directive

The Directive on security of Network and Information Systems (2016/1148) (NIS Directive) was adopted at European level. The Dutch translation of the NIS Directive is the 'Richtlijn Netwerk- en informatiebeveiliging' (NIB). The NIS Directive requires countries in the European Union to increase the resilience of their networks and information systems. This includes robust risk management, organisational and technical security measures (duty of care) and reporting any incidents (notification obligation).

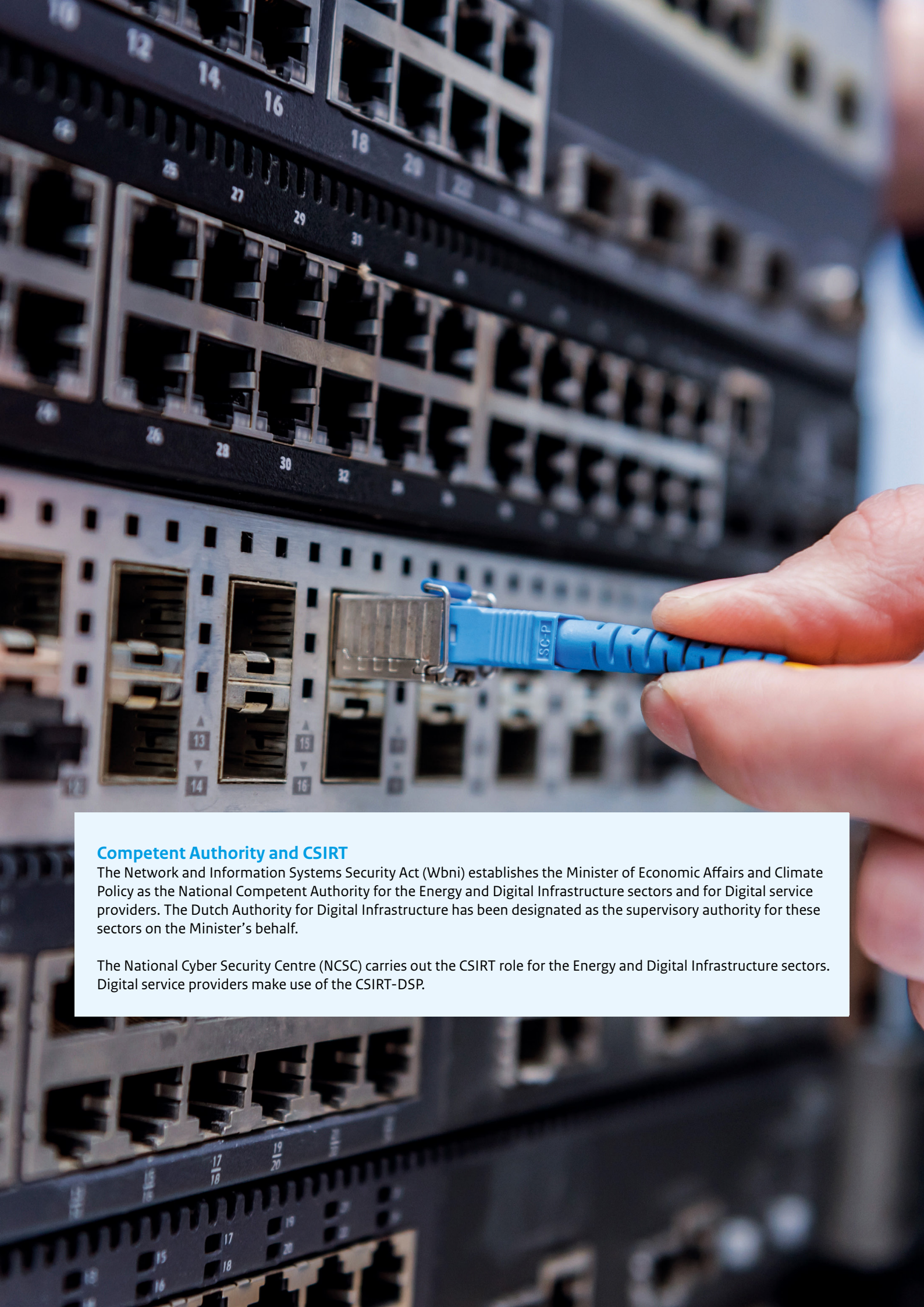
The NIS Directive encourages national and international cooperation, which is taken up by the EU Member States through the sharing of information, participation in collaborative groups and by sharing the approach to increasing resilience. National Competent Authorities (NCAs) and Computer Security Incident Response Teams (CSIRTs) within individual Member States are also required to work together and share relevant knowledge and information. A CSIRT is a team that is responsible for issuing early warnings with regard to information security risks and providing support and assistance in the event of an incident.

The NIS Directive requires that each Member State:

- Designate a national point of contact for cooperation in relation to international incidents
- Designate at least one National Competent Authority
- Designate at least one CSIRT

This ensures that it is clear where organisations who are subject to regulatory compliance can turn to with any questions and incident notifications and which governmental organisation acts as the regulatory and enforcement agency.

The NIS Directive will be revised in the near future. The new Directive will define a clear scope, harmonise the designation of operators of essential services by Member States, streamline the enforcement regime, improve information sharing between Member States and strengthen cyber security policies across the European Union.



Competent Authority and CSIRT

The Network and Information Systems Security Act (Wbni) establishes the Minister of Economic Affairs and Climate Policy as the National Competent Authority for the Energy and Digital Infrastructure sectors and for Digital service providers. The Dutch Authority for Digital Infrastructure has been designated as the supervisory authority for these sectors on the Minister's behalf.

The National Cyber Security Centre (NCSC) carries out the CSIRT role for the Energy and Digital Infrastructure sectors. Digital service providers make use of the CSIRT-DSP.

The Network and Information Systems Security Act

The Network and Information Systems Security Act (Wbni) is the Dutch implementation of the European NIS Directive into national law. The Wbni requires operators of essential services (OES) and digital service providers (DSPs) to put in place appropriate and proportionate technical and organisational measures to secure their ICT resources and to take appropriate measures to prevent incidents and to mitigate the impact of any incidents as much as possible. The Network and Information Systems Security Act came into force on 9 November 2018.

At the same time as the Wbni, the 'Network and Information Systems Security Decree' (*Besluit Beveiliging Netwerk- en Informatiesystemen, Bbni*) also came into force. The Bbni fleshes out the provisions of the Network and Information Systems Security Act, for example, providing further specification regarding the designation of operators of essential services and defining the duty of care in greater detail. The most current decisions are set out in the Bbni; the Decree was amended in June 2021.

The European Implementing Regulation 2018/151 – which is a regulatory supplement to the NIS Directive and thereby to the Wbni – applies to digital service providers, additional to the Wbni.

This Regulation specifies the elements to be taken into account for risk management and the parameters to determine whether an incident has a substantial impact. The Regulation is available in full on the eur-lex.europa.eu website – simply search '2018/151' and select 'Regulation'.

Risk management at the core

Management of information security risks in network and information systems forms the basis of the NIS Directive. Only if there is a deep understanding of those risks can an organisation put appropriate technical and organisational measures in place. Risks can be assessed by looking at the probability of an event occurring and examining the impact that that such an event would have.

Confidentiality and integrity, as well as the availability and authenticity of network and information systems can be adversely affected. If this impacts the continuity of an organisation's essential services, this is classified as an incident.

No organisation is the same as the next and what may be an appropriate measure for one organisation need not qualify as one for another organisation. That is why the Dutch Authority for Digital Infrastructure does not prescribe measures, but rather focuses on monitoring the risk management of processes.

Operators of essential services and digital service providers

The NIS Directive distinguishes between operators of essential services and digital service providers.

Operators of essential services are public or private entities that provide a service that is essential to maintaining critical economic or social activities. Incidents that affect network and information systems can have a substantial impact on the continuity of essential services and service provision.

Digital service providers are not designated. Using the flowchart below, digital service providers are able to assess whether they fall under the Network and Information Systems Security Act (Wbni) or not.

Operators of essential services
Provides essential services as referred to in Annex II of the NIS Directive
Is designated by the national government
Proactive monitoring of compliance
Takes appropriate and proportionate technical and organisational measures based on a thorough risk assessment
Reports incidents to the national CSIRT and the regulator
Demonstrates security policies and security measures through documentation
Demonstrates actual implementation of security policy and security measures

Digital service provider
Provides digital services as referred to in Annex III of the NIS Directive
Is defined in the NIS Directive; please see the flowchart below for more information
Reactive monitoring of compliance
Takes appropriate and proportionate technical and organisational measures based on a thorough risk assessment
Reports incidents to the national CSIRT-DSP and the regulator
Has the appropriate documentation to be able to demonstrate security measures

Notification obligation under the Wbni

Operators of essential services in the Energy and Digital Infrastructure sectors are obliged to report all incidents that exceed the threshold value(s) and/or have a substantial impact on the continuity of services to the Dutch Authority for Digital Infrastructure and the National Cyber Security Centre (NCSC) without delay. The Ministry of Economic Affairs and Climate Policy will be announcing the threshold value(s) to the relevant organisations within the Energy and Digital Infrastructure sectors.

→ For more information on the procedure governing the reporting of incidents, please refer to the 'Notification obligation for operators of essential services' brochure. Available for download from: www.rdi.nl/wbni-brochure-OES

Digital service providers are required to report all incidents that exceed the threshold value(s) and/or have a substantial impact on the continuity of services to the Dutch Authority for Digital Infrastructure and the CSIRT-DSP without delay. The thresholds that determine whether an incident has a substantial impact have been set out in the European Implementing Regulation for digital service providers (2018/151).

→ For more information on the thresholds and the procedure governing the reporting of incidents, please refer to the 'Notification obligation for digital service providers' brochure. Available for download from: www.rdi.nl/wbni-brochure-DSP

All sectors may also voluntarily report incidents even if they do not (yet) fall under the notification obligation. We equally stand to learn a lot from incidents with a smaller impact. That is why we explicitly invite you to report these incidents to us as well.

As a supervisory authority, we will always attempt to gain a balanced picture of the background to an incident. Following a notification of an incident, the Dutch Authority for Digital Infrastructure will conduct an in-depth investigation aimed at increasing the quality of network and information security and stimulating the learning capacity of the relevant sectors. The Dutch Authority for Digital Infrastructure will assess incidents and threats relating to network and information systems security in a broader sense. We will also include incidents in our assessment that remain below the thresholds and incidents that have received media attention.

This information will allow us to work with the sectors in a constructive manner to increase the digital resilience of essential services and digital services in the Netherlands.

Monitoring and enforcement

Operators of essential services are subject to an active monitoring policy that includes regular inspections aimed at assessing the design, implementation and operation of the risk management process and the putting in place of appropriate and proportionate control measures. In addition, thematic inspections will be carried out that focus on specific topics and on particular themes in the context of the Wbni. In terms of our monitoring remit, our approach is to establish an open dialogue at an early stage to ensure that mutual expectations are clearly defined and that supervised organisations are aware of the relevant rules.

Digital service providers, by contrast, are subject to reactive monitoring, with inspections only taking place based on indicators and on incidents.

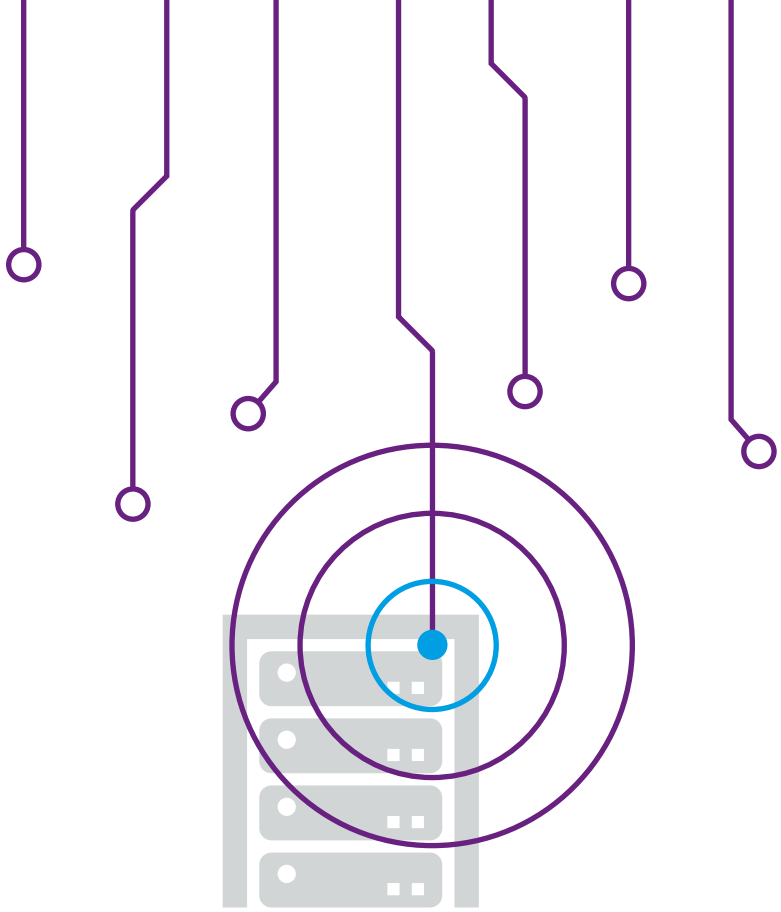
The Dutch Authority for Digital Infrastructure has several powers in relation to implementation its supervision remit. If the Dutch Authority for Digital Infrastructure concludes that an operator of essential services or a digital service provider is not in compliance with the applicable laws and regulations, the law provides for several ways to take enforcement action, including imposing binding instructions. This means that an organisation may be required to put in place specific measures or to cease or refrain from a certain type of conduct. The Dutch Authority for Digital Infrastructure also has the power to impose fines, as applicable.

Data processing

The Dutch Authority for Digital Infrastructure will only disclose confidential information relating to your organisation to third parties to the extent permitted by law. This will only be done if confidentiality is sufficiently guaranteed and where there are adequate safeguards to ensure that the information will not be used for any other purpose. The Public Access to Government Information Act (*Wet openbaarheid van bestuur,* Wob) does not apply to this confidential information.

If public awareness should be required to prevent or control an incident, the Dutch Authority for Digital Infrastructure may inform the general public about the reported incident. You will always be consulted in advance of this taking place. Your organisation may likewise be asked to inform the public.

In the event that the incident should affect an essential service in another Member State of the European Union, the Dutch Authority for Digital Infrastructure will be able to request that the NCSC refer your report to the dedicated point of contact in that Member State.



Find out more / Questions
Please go to **www.rdi.nl/wbni**
or send an e-mail to **wbni@rdi.nl**

October 2021