FEASIBILITY STUDY ON COMMON TOOL

ENTSO-E's and EU DSO entity's feasibility study to assess the possibility and the financial cost necessary to develop a common tool enabling all entities to share information with relevant national authorities in accordance with Article 37(9) of the Commission Regulation (EU) 2024/1366 of 11 March 2024 establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows

13 June 2026

DSO Entity
Rue Belliard 35
1000 Brussels Belgium

info@eudsoentity.eu
www.eudsoentity.eu

ENTSO-E aisbl
Rue de Spa 8
1000 Brussels Belgium

info@eudsoentity.eu
www.eudsoentity.eu

TABLE OF CONTENTS

DSO Entity
Rue Belliard 35
1000 Brussels Belgium
info@eudsoentity.eu
www.eudsoentity.eu

ENTSO-E aisbl
Rue de Spa 8
1000 Brussels Belgium
info@eudsoentity.eu
www.eudsoentity.eu

1. INTRODUCTION

This document provides a feasibility study to assess the possibility and the financial costs necessary to develop a common tool enabling all entities and national authorities to share information, hereafter referred to as the "common information sharing tool". Article 37(9) of the Commission Regulation (EU) 2024/1366 of 11 March 2024 establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows, hereafter referred to as the "NCCS Regulation", states that the ENTSO for Electricity, in collaboration with the EU DSO entity, shall perform such a study.

According to Article 37(10) of the NCCS Regulation, the feasibility study shall address the possibility for such a common tool to:
Support critical-impact and high-impact entities with relevant security related information for operations of cross-border electricity flows, such as near real-time reporting of cyber-attacks, early alerts related to cybersecurity matters and undisclosed vulnerabilities on equipment in use in the electricity system.
Be maintained in a suitable and highly trustable environment.
Allow for data collection from critical-impact and high impact entities and facilitate removal of confidential information and anonymisation of the data and their prompt dissemination to critical-impact and high-impact entities.

The feasibility study reviews existing tools used for information sharing and concludes in a recommendation for a common tool to share information about cyber-attacks, early alerts related to cybersecurity, and undisclosed vulnerabilities.
According to Article 37(11), ENTSO-E and DSO Entity shall present the results of the feasibility study to ACER and the NIS Cooperation Group.

2. REQUIREMENTS FOR THE COMMON TOOL

2. 1. Purpose and requirements

The purpose of the common information sharing tool is to share information between entities (high-impact and critical-impact entities) and the national competent authorities. It is also desirable that the tool enables the information exchange among entities, among national authorities, and between national authorities and other European stakeholders as described in the NCCS Regulation. This information is highly sensitive, so the tool must be trusted, it must protect security and ensure anonymisation capabilities.

The common tool will have to meet the following requirements defined in Article 37 of the NCCS Regulation. The common tool must allow for:

- near real-time reporting of cyber-attacks
- reporting of early alerts related to cybersecurity
- reporting of undisclosed vulnerabilities
- secure data collection (encryption at rest, communication integrity and confidentiality)
- data anonymisation
- prompt dissemination to critical-impact and high-impact entities
- being maintained in a suitable and highly trustable environment

Moreover, the common tool will have to meet the following requirements, implicitly derived from the NCCS Regulation or to allow for synchronisation with other reporting obligations. The common tool should provide:

- Role-based access control with support for different parties (SPOCs from entities, NCAs, CSIRTs, etc.)
- Availability
- Usability
- Compatibility with other existing tools used by national authorities
- A single-entry point to avoid double reporting due to other regulations

On 19 November 2025, the European Commission published the Digital Omnibus Regulation Proposal, which includes amendments to regulations that require information sharing and reporting to introduce a single-entry point that will allow to report all information for different regulations in a single platform. This feasibility study also considers this proposal.

2.2. Data in scope

The tool needs to enable the above-described communication to share information on cyber-attacks, early alerts related to cybersecurity matters and undisclosed vulnerabilities on equipment in use in the electricity system.

In the paragraphs below, these types of information are further defined. The base definitions are the ones stated on article 3 of the NCCS Regulation.

- Information on cyber-attacks corresponds to the information on reportable cyber-attacks as defined in the Cyber-Attack Classification Scale Methodology (hereby CACS Methodology).
- Early alerts related to cybersecurity matters can include different types of information, such as threats. These early alerts constitute the information exchange described on article 42 of the NCCS Regulation.
- Undisclosed vulnerabilities on equipment in use in the electricity system include mainly:
    - Unpatched actively exploited vulnerabilities according to Article 38(5) of the NCCS Regulation.
    - Unpatched vulnerability, without evidence of yet being actively exploited according to Article 37(4) of the NCCS Regulation

2.2.1. Reportable cyber-attacks

The data that must be exchanged in the context of cyber-attacks according to the NCCS Regulation are:

- Estimation of root cause
- Potential impact
- Estimation of severity
- Cyberattack gravity classification (based on the CACS Methodology)

Additional information such as the date of the incident, information on measures taken to mitigate the cyber-attack, Tactics, Techniques, and Procedures (TTPs) used in the attack or Indicators of Compromise (IoCs) could also on a voluntary basis be shared through the tool.

2.2.2. Early alerts related to cybersecurity matters

The data that can be exchanged on a voluntary basis in the context of early alerts are:

- Identified TTPs or IOCs used in an attack to contextualise and correlate the attack.
- Relevant information for other entities for preventing, detecting, responding, or mitigating the impact of the threat:
    - potential targets,
    - impact, and
    - geographical/industrial scale

2.2.3. Undisclosed vulnerabilities

The data that can be exchanged in the context of undisclosed vulnerabilities are:

- Evidence that execution of malicious code was performed without permission of the system owner
- List of affected ICT products or ICT services
- Severity of vulnerability
- Description of how the vulnerability could be exploited or IoCs.

2.2.4. Data classification

Based on ACER dissemination guidelines, information sharing is restricted to generating situational awareness purposes. Dissemination is therefore, under the NCCS, limited to other entities that may be affected. Any information not required or related to identify similar cyber-attacks, threats, or vulnerabilities shall be removed.

Such information includes, but is not limited to:

- Employee or customer personal data
- Specific details of impact, where such information brings further risk to the affected entity
- Confidential business information
- IP address of impacted entity (if logs are shared as part of disseminating cyber-attack information, such logs should be sanitised)
- Any confidential information that could conflict with national laws and regulations or could damage the national security

For information flows within a Member State, national classification schemes take precedence. For cross-border information flows, the TLP marking according to ACER's *Guidelines on Information Exchange Mechanisms* should apply.

2.3. Users of the common tool

The main intended users of the common tool are mandated employees of high-impact and critical-impact entities and representatives from the national authorities.

- **High-impact and Critical-impact entities:** they can send information to the competent authorities and to other entities upon approval of the competent authority. They have to receive information concerning events that could have an effect on their own infrastructure
- **National authorities (i.e., NCAs, CSIRTs):** according to Article 37, they can receive information from entities, anonymise it, and further disseminate it to entities or other parties. They can also ask entities to share the information.
- **ENISA:** they receive certain information pursuant to Article42., enrich it and share it.
- **National Single Points of Contact (SPOC):** according to Article 37(1)(d), the NCAs need to share the information about cyber-attacks with the national SPOCs no later than 24 hours after receiving the information.
- **API clients:** for integration with other systems from the competent authorities, CSIRTs or entities.
- **Operator of the tool:** for the administration of the tool (i.e., tool configuration, maintenance, and development, user management, etc.)
- **ACER:** dedicated view of statistics for monitoring purposes pursuant to Art. 12 of the NCCS Regulation

3. DEVELOPING A NEW TOOL

When evaluating solutions to meet our operational and compliance requirements, there is the option to develop a new tool. While technically and operationally, it is possible to develop a tool that meets all the requirements from the NCCS Regulation. This approach would require:

- **A trusted hosting environment** to ensure data security and regulatory compliance. All stakeholders should agree on the hosting organisation.
- **A dedicated development team** with expertise in the required technologies.
- **A substantial budget and long delivery timeline** for development, testing, and ongoing maintenance. The CRA Single Reporting Platform, which is currently under development, has a foreseen budget of over 10 million euros over four years[1], and the proposal from the Commission for the updated Cybersecurity Act foresees a budget of 8 million euros over 5 years for ENISA to develop and maintain the single-entry point[2], It is also unclear where the budget to develop a new tool would come from.
- **A long implementation timeline** that would require intermediate solutions for information sharing under the NCCS Regulation.
- **Double reporting,** entities and competent authorities would need to share information on different platforms for different regulations, increasing the reporting overhead.

[1] *https://www.enisa.europa.eu/procurement/implementation-of-the-single-reporting-platform*
[2] *COM(2026) 11 - Proposal for a Regulation for the EU Cybersecurity Act*

4. EXISTING TOOLS FOR INFORMATION SHARING

There are already existing tools, either open source or developed in line with other European regulations that are aimed at information sharing. This feasibility study has reviewed three tools that could be leveraged for the reporting under the NCCS Regulation as the common tool, namely NIS CIRAS, ENISA MISP instance, and the CRA Single Reporting Platform under development.

4.1. NIS Directive's CIRAS

Under the NIS (and NIS2), national authorities in Member States send summary reports of the significant incidents received during the year to ENISA. ENISA then collects, anonymises, aggregates and analyses the data. This is done through the Cybersecurity Incident Reporting and Analysis System (CIRAS)[3].

This platform is hosted by ENISA, and Single Point of Contacts (SPOCs) from the national authorities have accounts to access the platform. They can submit cross-border incident reports through the platform, but they can also receive notifications about significant incidents. The information is sent over the internet via HTTPS, but the data stored in the platform is not encrypted as no sensitive data is stored.

4.2. Cyber Resilience Act's Single Reporting Platform (SRP)

Under the Cyber Resilience Act (CRA), ENISA is developing a Single Reporting Platform (SRP)[4] to report vulnerabilities and incidents. This platform is expected to be implemented by 11 September 2026. This platform needs to meet the needs of the CRA, and therefore it must support manufacturers notifying actively exploited vulnerabilities and severe incidents having impact on the security of their products as well as the voluntary reporting of any vulnerability and cyber threats. Additionally, it should also support the CSIRT receiving and sharing these notifications.

The requirements for the platform were published on ENISA's website during the procurement call for the implementation of the tool. Basic security requirements were listed as core features, such as secure storage against unauthorised access, data retention, maintaining an audit trail, separation of environments, and available as open source.

While there is no decision yet, the amendment proposal of the commission to (EU)2022/2555 under the Digital Omnibus proposal, mentions that ENISA may ensure that the single-entry point builds on the single reporting platform.

[3] https://ciras.enisa.europa.eu/

[4] https://www.enisa.europa.eu/procurement/implementation-of-the-single-reporting-platform

4.3. ENISA MISP instance

The Malware Information Sharing Platform (MISP)[5] is a tool dedicated to collecting, storing, distributing, and sharing cyber security indicators and threats. Organisations can set up their own MISP instance and share events amongst the instances. Based on its documentation, the following capabilities are listed:

Collaboration

- Synchronisation feature allowing real-time information exchange between different MISP instances, or between an instance and a feed
- Offers capability of creating custom sharing groups

Data sharing

- Possibility of sharing data with different levels of granularity
- Use of tags to label events, attributes, and TLP level
- Adjustable taxonomies to follow custom classification schemes with possibility of sharing these taxonomies across instances
- Use of advanced filtering functionalities to align with organisation sharing policies
- Customisable RBAC

[5] https://www.misp-project.org/

5. ANALYSIS OF EXISTING TOOLS

This section includes an analysis of whether the tools considered meet the requirements for the NCCS common tool at the time of writing.

The features and assumptions included for each of the tools are valid and accurate at the time of writing this feasibility study. Due to the agile development of software applications, especially for the ones that are not implemented yet, the assessment of the features included in this report remains subject to change over time.

In the table below, the tick (✓) means the tool meets the requirements, the cross (✗) means it does not meet the requirements, both a tick and cross means it partially meets the requirements, and a question mark (?) means unknown or dependent of the way the tool is implemented.

Requirements	NIS-CIRAS	CRA-SRP	ENISA MISP
Near real-time reporting of cyber-attacks	✓	✓	✗ ✓
Reporting of early alerts	✗	✓	✓
Reporting of undisclosed vulnerabilities	✗	✓	✗ ✓
Allow for secure data collection (encryption at rest)	✗	✓	✓
Allow for secure data collection (communication integrity and confidentiality)	✓	✓	✓
Allow for data anonymisation	✓	✗	?
Allow for prompt dissemination to entities	✗	✓	✓
Trustable environment	✓	✓	?
Role based access control with support for different parties (SPOCs from entities, NCAs, CSIRTs, etc)	✗ ✓	✓	✓
Availability	✓	✓	?
Compatibility with other existing tools used by NCAs through APIs	✓	?	✗ ✓
Digital Omnibus – Single Entry Point	✗	?	✗

It is also important to note that usability of the tool by all the user groups is an essential requirement for the selected tool. Due to the state of development of the CRA SRP and the need to assess this requirement with the users of the tool, this requirement has not been analysed in this Chapter.

5.1. CIRAS

CIRAS is a reporting platform for national authorities; high-impact and critical-impact entities, as defined in Article 2 of the NCCS regulation, do not currently participate in it. Therefore, as is, it supports quarterly reporting of cyber-attacks among national authorities. It is not meant for real-time reporting, even though it could technically support it, or reporting of early alerts or undisclosed vulnerabilities. While it supports communication integrity and confidentiality, the data at rest is not encrypted. The data that goes into the CIRAS is anonymised, and it is hosted by ENISA in a trustable environment, however, it does not allow for a prompt dissemination to high-impact and critical-impact entities, as these entities are not part of the foreseen user group for the CIRAS platform, thus, the CIRAS platform does not currently support all the user groups for the NCCS common tool. ENISA has a service level agreement to maintain the availability of the tool.

As for the requirements coming to align with other regulations, an API for the CIRAS platform is being implemented and should be available by the second half of 2026. It is not known if the CIRAS would be used as the Single-Entry Point, but with the current functionality it is not expected that it will be the chosen tool for the Single-Entry Point proposed in the Digital Omnibus proposal.

Therefore, to use CIRAS for cyber-attack reporting under the NCCS Regulation, updates to the tool would need to be implemented:

- Enable real time communication
- Expand the number of users and roles to the ones defined in 0
- Implement encryption at rest of the data stored by CIRAS

5.2. CRA-SRP

The CRA-SRP is currently under development by ENISA. However, in the procurement requirements for the tool and the requirements laid out in the regulations there is detailed information about the functionality of the tool. From the CRA, the SRP needs to support the voluntary reporting of vulnerabilities, cyber threats, or incidents or near misses that might impact a product under the CRA. Therefore, in the context of the NCCS Regulation, the platform could support the reporting of cyber-attacks, early alerts, and undisclosed vulnerabilities. The requirements for the platform explicitly ask for availability and protection of the data both at rest and in transit. As the tool is hosted by ENISA, the environment is trustable. However, since the main objective of the tool is sharing vulnerabilities, the current plan for the tool would not allow for data anonymisation, which is required for disseminating cyber-attack information pursuant to Art. 37(1) of the NCCS Regulation. For the CRA-SRP to be used as the NCCS common tool, anonymisation capabilities should be implemented.

For the CRA, CSIRTs need to disseminate the information received about the vulnerabilities. Therefore, the tool needs to allow for prompt dissemination of data. It also supports a more diverse number of roles on the tool, as it foresees manufacturers, CSIRTs, and voluntary legal persons to use the platform.

The Single-Entry Point could build on the SRP as stated in the Digital Omnibus proposal from the European Commission, although this proposal is still subject to updates stemming from the proposals of the European Council and Parliament. The requirements for it include already the compatibility to other tools via an API, although it is not clear which tools and how they will be compatible.

5.3. ENISA's MISP

The final tool being considered is ENISA's MISP instance. The MISP's main purpose is to share cyber threats or early alerts between different parties. Therefore, even if technically possible, its main objective is not to share cyber-attacks or vulnerabilities nor to report to authorities.

The MISP allows for secure data collection, both at rest and in transit, and it allows for prompt dissemination of the information to the parties that are subscribed to a feed or synchronised between instances. The ENISA MISP is not hosted by ENISA on premises, therefore, it is difficult to determine the security level of the solution used without further investigation. The tool does allow for role-based access control and supports different types of parties. It is not clear whether data anonymisation can be performed.

For the requirements coming to align with other regulations, the MISP is compatible with other MISP instances, but not with any tool. It is not expected that the MISP will be used as the Single-Entry Point for the Digital Omnibus proposal.

6. CONCLUSIONS

This report has analysed the requirements and implications to develop a new common tool and has assessed and compared existing tools that could be used as the common tool under the NCCS Regulation.
While creating a new common tool for information sharing would be a possibility, the analysis of the different options and existing tools shows that leveraging an existing solution provided by a trusted host is the most efficient and cost-effective option. This approach offers several advantages:

- Immediate compliance with security and regulatory standards.
- Reduced time-to-market, as the tool is already developed and tested.
- Lower costs, avoiding the need for a full development cycle and long-term maintenance overhead.
- Increased efficiency by using just one tool to meet multiple reporting obligations. Stakeholders will receive more relevant information in a single place.

By choosing an existing solution, the effort can be focused on integration and customisation, ensuring that all obligations are met quickly and effectively.

Out of the evaluated existing tools, the CIRAS is currently better suited for periodical reporting from the competent authorities to ENISA. The MISP is useful for peer-to-peer voluntary information sharing, via trusted MISP instances such as the ones from ENISA or ENTSO-E. The CRA SRP, as it is currently being implemented by ENISA, would meet most of the requirements. However, it does not meet the requirements for anonymisation, and it is not yet clear whether it would integrate with the platforms used by the National Competent Authorities.

Therefore, the CRA SRP could be considered to be used as the NCCS common tool to meet the information exchange obligations under the NCCS Regulation, but it would require additional work to ensure the integration with existing national platforms and processes and the implementation of the anonymisation capabilities. If the Single Reporting Platform were to be chosen for information sharing under the NCCS Regulation, the ENTSO-E and the DSO Entity could collaborate with ENISA to further define the use cases and ensure that the tool meets all the requirements of the NCCS Regulation and the relevant usability needs for critical-impact and high-impact entities and national authorities.

Nevertheless, this report proposes that, once the single-entry point proposed by the Digital Omnibus is available, it is used to fulfil the reporting obligations of the NCCS and to leverage existing national reporting platforms and processes, ensure alignment with other cybersecurity regulations and to avoid double reporting.

7. INFORMATION SHARING WITHOUT A COMMON TOOL

The deployment of the tools outlined in this report may require several months or even years. Nevertheless, the NCCS Regulation mandates the timely exchange of information for high-impact and critical-impact entities. To ensure that the information sharing obligations are met while the recommended tools are not yet available, this section proposes a series of interim measures.

In the short term, to facilitate compliance with the NCCS Regulation's information sharing obligations (particularly Articles 37 and 38 of the NCCS Regulation), information may be shared via encrypted email or via existing secure channels and platforms available in each Member State.

To enable efficient and secure communication, it is essential to clearly identify the designated recipients in each country. Accordingly, it is proposed that:

- Each high-impact and critical-impact entity is aware of the channels to contact their NCCS-NCA.
- Each Member State's NCCS-NCA maintains an up-to-date registry of national authorities and relevant high-impact and critical-impact entities in their own country.
- At the European level, an institution — either ENISA, the European Commission, ACER or the ENTSO-E with DSO Entity — be assigned the responsibility for maintaining the consolidated list of NCCS-NCAs across all Member States and other European stakeholders involved in the information sharing flows under the NCCS Regulation (e.g., CSIRTs, ENISA, etc.).

These registries should be adequately protected and continuously updated to support information sharing obligations under the NCCS Regulation and to ensure that accurate information can be shared promptly with authorised stakeholders on a need-to-know basis.

NCCS-NCAs could choose to use the CIRAS platform to share anonymised information about cyber-attacks, threats or vulnerabilities among each other. Information exchanged via CIRAS should then be shared with high-impact and critical-impact entities and other stakeholders in conformance with Article 37 of the NCCS Regulation.

For EU Member States, these interim measures would support compliance to the NCCS Regulation. Third countries may voluntarily participate in information sharing arrangements through bilateral or multilateral agreements as foreseen under Article 14 of the NCCS Regulation.