ACER

European Union Agency for the Cooperation of Energy Regulators

Guidelines for the entities on information exchange mechanisms

Pursuant to the network code for cybersecurity aspects of cross-border electricity flows

25 April 2025

Guidelines for the entities on information exchange mechanisms

Pursuant to the network code for cybersecurity aspects of cross-border electricity flows

25 April 2025

Find us at:

ACER

E press@acer.europa.eu
Trg republike 3
1000 Ljubljana
Slovenia

www.acer.europa.eu

Table of contents

1. Scope of these guidelines 4
1.1. Entities listed in Article 2(1) of the NCCS 4
1.2. Principles of information exchanges applicable to these guidelines 5
2. Entity information flows foreseen under the NCCS 7
3. Recommended approach to information sharing 12
3.1. Information flows confined to a Member State 12
3.2. Cross-border information flows 13
3.3. Information flows to ACER, ENISA and the Commission 15
3.4. Information flows between ENTSO-E and EU DSO entity 16
4. Application of information markings 17
4.1. Application of the TLP marking 17
4.2. Combined application of the TLP and SENSITIVE markings 17
5. Anonymisation and aggregation in the context of exchanges under the NCCS 19
5.1. Anonymisation of originators and sensitive information 19
5.2. Information aggregation 21
5.3. Recommendations for the entities 22
5.3.1. Disseminating information on cyber-attacks by the entities 23
5.3.2. Reporting on the risk assessment at entity level 23
5.3.3. Provision of Article 12(2)(a) monitoring information to ACER by the ENTSO-E and the EU DSO Entity 23
5.3.4. Sharing of Article 12(5) operational reliability performance indicators with ACER 24
5.3.5. Regional and comprehensive cybersecurity risk assessment reports 24
5.3.6. Benchmarking and cost assessment related to cost recovery 25
6. Summary grid of entity information flows and recommendations 26
7. List of tables 29

1. Scope of these guidelines

Pursuant to Article 47(7) of the Commission Delegated Regulation (EU) 2024/1366 establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows[1] (the '**NCCS**'), ACER shall issue guidelines addressing mechanisms for all entities listed in Article 2(1) (the '**entities**'[2]) to exchange information, and in particular envisaged communication flows, and methods to anonymise and to aggregate information for the purpose of implementation of Article 47.

These guidelines therefore focus on information that is to be exchanged in the context of the NCCS, as well as the process of exchanging it. Consequently, these guidelines:

- outline the information flows involving the entities as foreseen under the NCCS, with references to its relevant provisions;
- recommend an approach to information marking and provide a rationale behind it;
- advise on how information marking should be applied;
- discuss how information could be anonymised and aggregated in the context of exchanges under the NCCS; and
- summarise the above to provide an overview of recommended mechanisms for the entities to exchange information.

These guidelines do not provide detailed recommendations on tools, solutions and processes to exchange information. This choice is left to the entities, as long as they apply all necessary measures of organisational and technical nature to safeguard and protect information confidentiality, integrity, availability and non-repudiation and as long as they are aligned with the principles of the protection of exchanged information pursuant to Article 46 of the NCCS. Furthermore, the entities should ensure the compatibility of selected tools, solutions and processes.

Thus, for example, these guidelines do not recommend cybersecurity controls that entities should apply to protect the information exchanged. Such controls shall be included in the proposal for minimum cybersecurity controls developed by the TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO Entity, pursuant to Article 29(5) of the NCCS.

1.1. Entities listed in Article 2(1) of the NCCS

The rules on protection of information outlined in Chapter VII of the NCCS as well as these guidelines apply to the following entities involved in information exchanges under the NCCS, irrespective of whether or not they have been identified as high-impact and critical-impact entities pursuant to Article 24(1) of the NCCS:

- electricity undertakings as defined in Article 2(57) of Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity[3]; namely, undertakings carrying out at least one of the following functions: generation, transmission, distribution, aggregation, demand response, energy storage, supply or purchase of electricity, and who is responsible for the commercial, technical or maintenance tasks related to those functions;

[1] OJ L, 2024/1366, 24.5.2024.

[2] For the purpose of these guidelines, the singular and plural forms shall be used interchangeably.

[3] OJ L 158, 14.6.2019.

- nominated electricity market operators ('**NEMOs**') as defined in Article 2(8) of Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity ('**Regulation 2019/943**')[4];
- organised market places or 'organised markets' as defined in Article 2(4) of Commission Implementing Regulation (EU) No 1348/2014 of 17 December 2014 on data reporting implementing Article 8(2) and Article 8(6) of Regulation (EU) No 1227/2011 of the European Parliament and of the Council on wholesale energy market integrity and transparency[5] that arrange transactions on products relevant to cross-border electricity flows;
- critical ICT service providers as referred to in Article 3, point (9) of the NCCS;
- the ENTSO for Electricity established pursuant to Article 28 of Regulation 2019/943;
- the EU DSO entity established pursuant to Article 52 of Regulation 2019/943;
- balancing responsible parties as defined in Article 2, point (14) of Regulation 2019/943;
- operators of recharging points as defined in Annex I to Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union ('**Directive 2022/2555**');
- regional coordination centres (the '**RCCs**') as established pursuant to Article 35 of Regulation 2019/943;
- managed security service providers (the '**MSSPs**') as defined in Article 6(40) of Directive 2022/2555;
- any other entity or third party to whom responsibilities have been delegated or assigned pursuant to the NCCS.

1.2. Principles of information exchanges applicable to these guidelines

Article 47(7) of the NCCS stipulates that the guidelines shall address mechanisms for all entities to exchange information for the purpose of implementation of Article 47 of the NCCS. This article establishes the following principles applicable to the entities:

- any information provided, received, exchanged or transmitted for the purposes of implementing the NCCS, shall be protected, considering the confidentiality level of the information applied by the originator (Article 47(1));
- obligation of professional secrecy (Article 47(2));
- information received subject to the NCCS in the course of duty may not be disclosed to any other entity or authority, without prejudice to cases covered by national law, other provisions of the NCCS or other relevant Union legislation (Article 47(5));
- without prejudice to national or Union legislation, an authority, entity or natural person who receives information pursuant to the NCCS may not use it for any other purpose than carrying out its duties under the NCCS (Article 47(6)); and

[4] OJ L 158, 14.6.2019.

[5] OJ L 363, 18.12.2014.

- any information received, exchanged or transmitted for the purposes of implementing Article 23 on the comprehensive cross-border electricity cybersecurity risk assessment report, shall be anonymised and aggregated (Article 47(4)).

In addition, Article 46 stipulates that the entities shall ensure that information provided, received, exchanged or transmitted under the NCCS is:

- accessible only on a need-to-know basis and in accordance with relevant Union and national rules on security of information (Article 46(1));
- handled and tracked during its entire life-cycle and that it may be released at the end of its life-cycle only after being anonymised (Article 46(2));
- is limited to individuals who fulfil the criteria of Article 46(5) of the NCCS; and
- provided to a third party falling outside the scope of the NCCS only subject to the written agreement of the natural or legal person that originally created or provided the information (Article 46(6)).

2. Entity information flows foreseen under the NCCS

To provide appropriate context prior to discussing recommended information markings and approach to information anonymisation and aggregation, this section outlines the information flows involving the entities as foreseen under the NCCS, with references to its relevant provisions.

For the purposes of displaying an entire information flow, the information flows outlined in this section include the authorities referred to in Article 2(2), such as ACER, the competent authorities, NRAs, CSIRTs or ENISA, as recipients of the information.

Descriptions of the information exchanged are only indicative, **non-exhaustive**, and should not be relied on with regards to the implementation of the NCCS. Furthermore, unless the provisions of the NCCS and other relevant legal acts stipulate otherwise, not all parts of the description may be applicable.

Table 1: Non-exhaustive list of entity information flows foreseen under the NCCS

Type of information	NCCS articles	Indicative description of entity-related information flows and information exchanged
Cyber-attacks	38(3)	**Entity to national CSIRT and competent authority** This information includes the level of the reportable cyber-attack according to the cyber-attack classification scale methodology referred to in Article 37(8) of the NCCS, with the following information: • an estimation of the root cause; • determination of the potential impact of the cyber-attack; • estimation of the severity of the cyber-attack; and • cyber-attack gravity classification. In addition, pursuant to Article 23(4)(d) of Directive 2022/2555, the entity shall, amongst others, provide a final report with a detailed description of the incident, including: • its severity and impact; • the type of threat or root cause that is likely to have triggered the incident; • applied and ongoing mitigation measures; and • where applicable, the cross-border impact of the incident.
	37(1)(f)	**Entity to entities in the same Member State or to entities in other Member States** If requested by the competent authority, the entity further disseminates the reportable cyber-attack information to other entities that may be affected. The contents of this information should generate situational awareness in the electricity sector and prevent the materialisation of a risk that may escalate in a cross-border cybersecurity electricity incident.
Threats	38(6)	**Entity to national CSIRT**

Type of information	NCCS articles	Indicative description of entity-related information flows and information exchanged
		Any information related to a reportable cyber threat that may have a cross-border effect, including: • relevant information for other entities for preventing, detecting, responding or mitigating the impact of the risk; and • the identified tactics, techniques and procedures used in the context of an attack lead to information such as compromised URL or IP addresses, hashes or any other attribute useful to contextualise and correlate the attack.
Unpatched actively exploited vulnerabilities	38(5)	**Entity to national CSIRT** Information describing the vulnerability, including: • evidence that execution of malicious code was performed by an actor on a system without permission of the system owner; • the affected ICT products or ICT services; and • the severity of the vulnerability (description of how it could be exploited).
Union-wide risk assessment	19	**Exchanges between ENTSO-E and EU DSO Entity** Union-wide risk assessment information including: • Union-wide processes that could affect the operational security of the electricity system; • assessment of possible consequences of a cyber-attack compromising these processes, considering intentional compromises, indirect consequences (including cascading effects), effect of mitigating controls and possible impact of trends in the electricity sector on the consequences; and • resulting Union-wide high-impact and critical-impact processes. **ENTSO-E and EU DSO Entity to ACER, Commission, ENISA and the competent authorities** Union-wide risk assessment report including the information above, as well as a list of the types of entities involved in the process.
Entity risk assessment	27	**Entity to competent authority** Risk assessment report, including: • a list of controls selected for the entity-level risk mitigation plan pursuant to Article 26(5) of the NCCS, with the implementation status of each control; • for each Union-wide high-impact or critical-impact process, an estimate of the risk of a compromise of the confidentiality, integrity, and availability of information and relevant assets; and • a list of critical ICT service providers for their critical-impact processes. Additionally, risk assessment report may contain:

Type of information	NCCS articles	Indicative description of entity-related information flows and information exchanged
		• an estimate of duration of impact on availability; • cyber threats causing the risk; • residual risk after implementing the controls.
Regional risk assessments	21	**Exchanges between ENTSO-E, EU DSO Entity and the RCCs** **Provision of draft reports by ENTSO-E and EU DSO Entity to NIS Cooperation Group for consultation[6]** Regional risk assessments will be based on the Union-wide risk assessment report and on Member State risk assessment reports, the latter of which will be submitted by the competent authorities to the ENTSO-E and EU DSO Entity pursuant to Article 20 of the NCCS. The ENTSO-E and EU DSO Entity will aggregate the Member State risk assessment results to System Operation Region level to that end. Such aggregated Member State risk assessment reports will include the following information for each high-impact and critical-impact business process: • the implementation status of the minimum and advanced cybersecurity controls pursuant to Article 29 of the NCCS; • a list of all cyber-attacks reported in the previous three years pursuant to Article 38(3) of the NCCS; • a summary of the cyber threat information reported in the previous three years pursuant to Article 38(6) of the NCCS; and • for each Union-wide high-impact or critical-impact process, an estimate of the risks of a compromise of information and relevant assets.
Comprehensive cross-border risk assessment report	23	**Exchanges between the TSOs, ENTSO-E and EU DSO Entity** **Exchanges between the TSOs, ENTSO-E, EU DSO Entity and other Article 2(1) entities** **Provision of draft report by the TSOs, ENTSO-E and EU DSO Entity to the NIS Cooperation Group for consultation** **TSOs, ENTSO-E and EU DSO Entity provide the report to the Electricity Coordination Group[7], including national authorities and ACER** **ENTSO-E and EU DSO Entity shall release a sanitised public version** The comprehensive cross-border risk assessment report will include:

[6] Once the NIS Cooperation Group establishes its procedures on handling external communications, these guidelines may be amended to take them into account.

[7] https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&do=groupDetail.groupDetail&groupID=2735

Type of information	NCCS articles	Indicative description of entity-related information flows and information exchanged
		• the list of Union-wide high-impact and critical-impact processes (Article 19(2)(a)), including the likelihood and impact of cybersecurity risks evaluated during the regional risk assessments (Article 21(2) and Article 19(3)(a)); • current cyber threats; • cyber-attacks for the previous period at Union level, providing a critical overview of how such cyber-attacks may have had an impact on electricity cross-border flows; • overall status of implementation of the cybersecurity measures; • status of implementation of the cyber-attack, threat and vulnerability information flows pursuant to Articles 37 and 38; • list of information or specific criteria for classification of information pursuant to Article 46; • identified risks that may derive from insecure supply chain management; • results of regional and cross-regional cybersecurity exercises organised pursuant to Article 44; • analysis of the development of the overall cross-border cybersecurity risks in the electricity sector since the last regional cybersecurity risk assessments; and • aggregated and anonymised information on derogations from cybersecurity controls granted pursuant to Article 30(3).
Monitoring by ACER	12(2)(a) 12(5) 17(1)	**Art. 12(2)(a) Implementation of risk management measures** **Entities to their competent authority, to be subsequently aggregated and shared with ACER** **ENTSO-E and EU DSO Entity to ACER (aggregated subset)** **Entity to ACER** The information flow entity to ACER is mentioned for completeness. ACER will determine the information related to the status of implementation of the applicable cybersecurity risk management measures in accordance with Article 12(2)(a) of the NCCS in collaboration with the competent authorities. This could include the implementation status of: • the cybersecurity controls pursuant to Article 29(6) of the NCCS; • the entity-level risk assessments pursuant to Article 26(4) of the NCCS; • the entity-level risk treatment plan pursuant to Article 26(5) of the NCCS; • the cybersecurity management system pursuant to Article 32 of the NCCS; • the CSOC capabilities pursuant to Article 38(1)(a) of the NCCS; • the capabilities to handle detected cyber-attacks pursuant to Article 39(a) of the NCCS;

Type of information	NCCS articles	Indicative description of entity-related information flows and information exchanged
		• the entity-level crisis management plan pursuant to Article 41(6) of the NCCS; • the entity- or Member-State level cybersecurity exercises pursuant to Article 43 of the NCCS; and • participation in regional cybersecurity exercises pursuant to Article 44 of the NCCS. The information would be the same or very similar regardless of the information flow at the beginning of this section. The difference would relate to the aggregation level. **Art. 12(5) Operational reliability performance indicators** **Entities to the CSIRT and competent authority, to be subsequently aggregated and shared with ACER** **Entity to ACER** Performance indicators referred to in Article 12(5) for the assessment of operational reliability that are related to cybersecurity aspects of cross-border electricity flows.
Benchmarking by the NRAs	13	**Entities to their NRAs** Information required by the NRAs to carry out the benchmarking analysis referred to in Article 13, such as the expenditure on cybersecurity investments and their effectiveness.
Recovery of costs	11	**TSOs and DSOs to their NRAs** • Processes (technical and organisational), products, services, systems and solutions implemented to comply with the NCCS, including the cybersecurity risk management measures. • Their costs.
Development of proposals for the terms and conditions or methodologies or plans (the '**TCMPs**')	6	**Exchanges between ENTSO-E, EU DSO Entity and the entities** **Provision of drafts and proposals to ACER, ENISA and other authorities encapsulated in Article 2(2) of the NCCS** Some documents will be based on risk assessments, such as the minimum and advanced cybersecurity controls developed pursuant to 29(1) of the NCCS.

3. Recommended approach to information sharing

The purpose of marking information is to ensure its sufficient level of confidentiality. For example, by indicating that the information in question is sensitive and thus must be protected, considering the confidentiality level of the information applied by the originator. To such information, the principles of information exchanges outlined in Section 1.2 of these guidelines would apply.

In all cases, the information originator has the freedom and the responsibility to apply an appropriate classification scheme or distribution protocol, as well as a respective mark or label, based on the principles of information exchanges outlined in Section 1.2, and any relevant national legislation.

3.1. Information flows confined to a Member State

In the context of information flows under the NCCS, the general recommendation is to use the existing classification schemes and distribution protocols. This is particularly appropriate for information flows confined to a Member State-level. In such cases, where available, existing confidentiality markings aligned with national laws as well as existing distribution protocols should be used.

In the absence of existing national distribution protocols or confidentiality markings applicable to company security or business secrets, the Traffic Light Protocol discussed in Section 3.2 should be applied.

Entity information flows confined to a Member State could be allocated to the following four broad categories, with non-exhaustive examples:

Cyber-attacks, threats and unpatched actively exploited vulnerabilities

- entities providing information on cyber-attacks to their national CSIRT and their competent authority;
- entities disseminating reportable cyber-attack information to other entities in the same Member State, if requested by the competent authority;
- entities providing information related to a reportable cyber threat to their national CSIRT;
- entities providing information related to unpatched actively exploited vulnerabilities to their national CSIRT;

Entity risk assessments

- entities providing risk assessment reports and any ancillary information to their competent authority, as well as any subset thereof for the purposes of monitoring;

Benchmarking and cost assessment related to cost recovery

- entities providing information to their NRAs relating to cybersecurity benchmarking pursuant to the NCCS;
- entities providing information to their NRAs relating to cost recovery pursuant to the NCCS; and

TCMPs

- each entity providing proposals for the terms and conditions or methodologies or plans to their authorities encapsulated in Article 2(2) of the NCCS. In particular, to the competent authorities.

3.2. Cross-border information flows

Entity cross-border entity information flows under the NCCS could be allocated to the following three broad categories, with non-exhaustive examples:

Cyber-attack information dissemination

- entities disseminating reportable cyber-attack information to entities in other Member States, if requested by the competent authority;

Union-wide and regional risk assessments, and comprehensive cross-border risk assessment report

- ENTSO-E and EU DSO Entity providing the Union-wide risk assessment report, including any related need-to-know information, to the competent authorities designated pursuant to Article 8 of Directive 2022/2555 (the '**NIS Competent Authorities**');
- exchanges between the ENTSO-E, the EU DSO Entity and the Regional Coordination Centres in the context of regional risk assessments;
- ENTSO-E and EU DSO Entity provide draft regional risk assessment reports to the NIS Competent Authorities for consultation;
- exchanges between the ENTSO-E, EU DSO Entity and the TSOs and other Article 2(1) entities in the context of the comprehensive cross-border risk assessment report;
- TSOs, ENTSO-E and EU DSO Entity consulting the NIS Competent Authorities on draft comprehensive cross-border risk assessment report;
- TSOs, ENTSO-E and EU DSO Entity provide the comprehensive cross-border risk assessment report to the national authorities within the Electricity Coordination Group; and

Benchmarking

- ENTSO-E and EU DSO Entity provide aggregated and averaged Article 13(3)(b) price data to the NRAs for the purposes of system operation region benchmarking.

TRAFFIC LIGHT PROTOCOL

The Traffic Light Protocol (v2, FIRST)[8], or the '**TLP**', is a widely used standard for exchanging cybersecurity-related information. It is most commonly used in the context of incident response, digital forensics and cyber threat intelligence, making it a natural reference for exchanging information on cyberattacks, threats and unpatched actively exploited vulnerabilities under the NCCS. However, by virtue of its universality and simplicity, it is also used for sharing many other types of sensitive information.

Therefore, the TLP marking could be used for most cross-border information flows under the NCCS, including those described in Section 3.3 below (Information flows to ACER, ENISA and the Commission).

The TLP uses the following four colours to give an indication about the sensitivity of cybersecurity-related information and specify the sharing restrictions associated with this information:

[8] https://www.first.org/tlp/.

Table 2: The TLP markings

TLP marking	Definition
TLP:RED	For the eyes and ears of individual recipients only, no further disclosure. Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organisations involved. Recipients may therefore not share TLP:RED information with anyone else.
TLP:AMBER+STRICT	Recipients can share this information **on a need-to-know basis** within their organisation **only**.
TLP:AMBER	Recipients can only share this information **on a need-to-know basis** within their organisation and its clients. TLP:AMBER may be used when information requires support to be effectively acted upon, yet carries operational risk if shared outside of the organisations involve
TLP:GREEN	Recipients may share TLP:GREEN information with peers and partner organisations within their community, but not via publicly accessible channels. When 'community' is not defined, cybersecurity community is assumed. Sources may use TLP:GREEN when information is useful to increase awareness within their wider community.
TLP:CLEAR	Recipients can spread this to the world, there is no limit on disclosure (subject to standard copyright rules). Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.

While the TLP is not a formal classification scheme, its colour coding does provide an implicit indication of the information sensitivity level. Furthermore, while the TLP itself is not legally binding, the confidentiality provisions under the NCCS and the relevant national laws are.

As noted in Section 3.1, the TLP could also be used in the context of information flows confined to a Member State in the absence of existing national distribution protocols or confidentiality markings applicable to company security or business secrets.

National classification schemes take precedence

Since the TLP is not a formal marking, it is inapplicable when national legislation and national schemes stemming from it apply to the information in question. Some Member States may apply default classifications to certain information, even at 'classified' level, indicating a risk to national interests. Sharing such information, even marked as TLP:RED, would be illegal in these Member States.

This rule must also be observed during cross-border information exchanges to the extent that the information shared by the originator is subject to national legislation and national schemes stemming from it.

Thus, in the context of the entities disseminating reportable cyber-attack information to the entities in other Member States if requested by the competent authority pursuant to Article 37(1)(f) of the NCCS, the entity concerned shall use any applicable national scheme instead of the TLP. In such cases, this entity will need to put the recipient entities on notice and explain to them how to apply the scheme in question. In particular, the allowed distribution.

For example, the originating entity would need to include a stipulation that, based on its national scheme, the information in question may **only** be shared within the recipient's entity and strictly on a need-to-know basis.

The TLP contains usage instructions, which are provided in Section 4 of this document.

ACER will monitor the application and the updates of the TLP in the context of information flows pursuant to the NCCS, as part of Article 10 potential improvement proposals related the implementation of the NCCS.

3.3. Information flows to ACER, ENISA and the Commission

Entity information flows under the NCCS to ACER, ENISA and the Commission could be allocated to the following three broad categories, with non-exhaustive examples:

Union-wide and regional risk assessments, and comprehensive cross-border risk assessment report

- ENTSO-E and EU DSO Entity providing the Union-wide risk assessment report, including any related need-to-know information, to ACER, ENISA and the Commission;
- ENTSO-E and EU DSO Entity providing draft regional risk assessment reports, including any related need-to-know information to ENISA and the Commission;
- TSOs, ENTSO-E and EU DSO Entity provide draft comprehensive cross-border risk assessment report, including any related need-to-know information, to ENISA (as the submission shall be made to the NIS CG) for consultation;
- TSOs, ENTSO-E and EU DSO Entity provide the comprehensive cross-border risk assessment report, including any related need-to-know information, to ACER (as the submission shall be made to the Electricity Coordination Group);

Monitoring

- ENTSO-E and EU DSO Entity providing risk assessment information aggregated to system operation region-level to ACER to monitor the status of implementation of the applicable cybersecurity risk management measures in accordance with Article 12(2)(a) of the NCCS;
- entities reporting on the operational reliability performance indicators to ACER. This information flow is mentioned for completeness (please refer to the description in Section 2); and

Proposals for TCMPs

- provision of drafts and proposals for the terms and conditions or methodologies or plans to ACER and ENISA.

The TLP marking discussed in Section 3.2 should also be used in the context of entity information flows to ACER, ENISA and the Commission, with the respective application instructions provided in Section 4 of this document.

‘SENSITIVE’ MARKING

When sharing information with ACER, ENISA or the Commission classified as TLP:AMBER or above, the entities should **additionally** apply the ‘SENSITIVE’ marking and share the information in accordance with the practices provided in Section 4 of these guidelines. The use of the SENSITIVE marking will put ACER, ENISA and the Commission on notice that the information must be handled accordingly.

SENSITIVE marking is used in the context of sensitive non-classified information, defined in Article 9(5)(b) of Commission Decision 2015/443 of 13 March 2015 on Security in the Commission as:

‘(…) information or material the Commission must protect because of legal obligations laid down in the Treaties or in acts adopted in implementation thereof, and/or because of its sensitivity. Sensitive non-classified information includes, but is not limited to, information or material covered by the obligation of professional secrecy, as referred to in Article 339 TFEU, information covered by the interests protected in Article 4 of Regulation (EC) No 1049/2001 of the European Parliament and of the Council (12) read in conjunction with the relevant case-law of the Court of Justice of the European Union or personal data within the scope of Regulation (EC) No 45/2001.’

3.4. Information flows between ENTSO-E and EU DSO entity

Information flows between ENTSO-E and EU DSO Entity under the NCCS could be allocated to the following four broad categories:

- performance Union-wide and regional risk assessments;
- development of the Comprehensive cross-border electricity cybersecurity risk assessment report;
- development of proposals for the terms and conditions or methodologies or plans; and
- development of guidance.

Exchange of documents developed by ENTSO-E in collaboration with the EU DSO entity fall under the ENTSO-E and DSO entity non-disclosure agreement pursuant to their respective Memorandum of Understanding (the ‘**MoU**’).

Any interaction or exchange of information between the ENTSO-E and the EU DSO Entity shall be done in compliance with their obligations not to disclose commercially sensitive information and to protect personal and operational data.

4. Application of information markings

This section advises how to apply the TLP marking in practice. It also advises how to apply the TLP and SENSITIVE markings together, when sharing information classified as TLP:AMBER or above with ACER, ENISA or the Commission.

4.1. Application of the TLP marking

In messaging, such as emails: the TLP label must be inserted directly prior to the information itself. In case of emails, the TLP label should be in the subject of the email.

Example of a subject line: 'TLP:AMBER | Regional risk assessment results'

In addition, when sharing information classified as TLP:AMBER or above, it is advisable to insert the TLP label in the email body, at the beginning of it. For example:

TLP:AMBER

'Dear George,

I enclose the results of this year's regional risk assessment (…).'

Table 3: The TLP colour-coding in RGB

TLP marking	RGB font		
	R	G	B
TLP:RED	255	43	43
TLP:AMBER	255	192	0
TLP:GREEN	51	255	0
TLP:CLEAR	255	255	255

In documents: the TLP label must be included in the header and footer of each page (including Word, Excel, PDF and PowerPoint), all capital letters in at least font size 12 and right-justified. There is no space between the 'TLP:' and the indication of colour.

4.2. Combined application of the TLP and SENSITIVE markings

When combined, the SENSITIVE marking should come first, to give an immediate indication that ACER, ENISA or the Commission need to handle the information appropriately. It should then be followed by an appropriate TLP distribution label, for example:

SENSITIVE: *TLP:AMBER*

SENSITIVE: ***TLP:AMBER***

In messaging, such as emails: as before, the combined TLP and SENSITIVE markings must be inserted directly prior to the information itself. In case of emails, the TLP and SENSITIVE markings should be in the subject of the email.

Example of a subject line: 'SENSITIVE: TLP:AMBER | Regional risk assessment results'

In addition, when sharing information classified as TLP:AMBER or above, it is advisable to insert the SENSITIVE and TLP markings in the email body, upfront, as the first line of the email.

The security markings should be in bold and the distribution markings in italics. Both should be in capital letters, at least font size 12, and in any event not smaller than the main text. For example:

SENSITIVE: *TLP:AMBER*

'Dear George,

I enclose the results of this year's regional risk assessment (…).'

Encryption: when sharing information with ACER, ENISA or the Commission classified as SENSITIVE (TLP:AMBER or above), emails must be signed and encrypted by secure tools and algorithms, such as PGP[9] or S/MIME.

In documents: as seen at the beginning of this section, the SENSITIVE markings must be inserted upfront, bolded, at least in font size 12. Furthermore, the TLP label should be in italics as seen above.

As in Section 4.1, the SENSITIVE and the TLP markings must be right-justified, and included in the header and footer of each page.

The TLP label must be placed in the same line as the SENSITIVE label, and may also continue in the following line if there is insufficient space in the first line. In any event, the marking should not extend past the centre of the page.

[9] https://www.openpgp.org/

5. Anonymisation and aggregation in the context of exchanges under the NCCS

This section discusses the rationale and general approach to information anonymisation and aggregation, as well as their application in the context of information flows under the NCCS. It also provides illustrative examples of how data can be anonymised to fulfil the principles of information exchanges applicable to these guidelines outlined in Section 1.2. Most specifically, to limit the information exchanged under the NCC to a need-to-know basis.

Section 6 of this guideline, which constitutes the summary section, includes anonymisation and, if relevant, aggregation proposals for each information type identified in Section 2.

5.1. Anonymisation of originators and sensitive information

Limiting the information exchanged to a need-to-know basis should not only be interpreted as limiting the number of its recipients, but also as limiting the scope of the information exchanged. In other words, removing certain data from the dataset based on the principles of information exchanges outlined in Section 1.2, including the need-to-know of the recipients.

The term anonymisation is usually used in the context of modifying sensitive and typically low-granularity information so that the natural or legal persons can no longer be identified. However, for the purposes of information exchanges under the NCCS, it will also be understood as modifying sensitive information to limit the exposure of any sensitive assets this information relates to. Such sensitive assets could be internal business processes of the entities and the systems supporting them.

In the context of the NCCS, non-perturbative anonymisation techniques are recommended, as they can be used to remove sensitive information without modifying the rest of the dataset.

Some of the most basic non-perturbative anonymisation techniques are:

- **information removal**, which amounts to removing information of a certain type from the entire dataset. It is most commonly used to remove direct identifiers from the dataset, such as names of natural or legal persons;
- **local suppression**. Instead of removing information of a certain type from the entire dataset, it is only removed from specific data records, where it could otherwise allow identifying specific natural or legal persons due to a very uncommon combination of their properties;

Table 4: Example of basic local suppression

Entry	Before local suppression			After local suppression		
ID	Entity type	Region	Impact	Entity type	Region	Impact
1	DSO	A	Critical	DSO	A	N/A
2	TSO	A	Critical	TSO	A	Critical
3	TSO	A	Critical	TSO	A	Critical
4	TSO	A	Critical	TSO	A	Critical
5	DSO	A	High	DSO	A	N/A

6	DSO	A	High	DSO	A	N/A
7	DSO	A	High	DSO	A	N/A

- **global recoding**, which is similar to aggregation, with one key difference. Namely, as seen in the table below, only one information type is aggregated, where it would otherwise allow identifying certain entries due to their uncommon combination of properties. In the example presented in the table below, there is only one DSO in country A, which makes it easily identifiable. However, once the countries are aggregated into regions, the country A DSO is no longer identifiable.

  Global recoding is different from aggregation described in Section 5.2, as it does not aggregate the data entries themselves. In other words, the data entries retain their individuality;

Table 5: Example of global recoding

Entry	Before local suppression			After local suppression		
ID	Country	Entity	ICT supplier	Region	Entity	ICT supplier
1	A	DSO	Bugs4Us	North	DSO	Bugs4Us
2	B	DSO	Bugs4Us	North	DSO	Bugs4Us
3	B	DSO	Bugs4Us	North	DSO	Bugs4Us
4	C	DSO	Perf-KPI	Central	DSO	Perf-KPI
5	C	Generator	Perf-KPI	Central	Generator	Perf-KPI
6	C	DSO	Perf-KPI	Central	DSO	Perf-KPI
7	C	Generator	Perf-KPI	Central	Generator	Perf-KPI
8	D	Generator	Makeshift	South	Generator	Makeshift
9	D	Generator	Makeshift	South	Generator	Makeshift
10	E	Generator	Makeshift	South	Generator	Makeshift

- **local recoding**, which is similar to global recoding, except it is applied only to records posing a higher risk. Using the example above, it could only be applied to countries A and B by aggregating them into region ‘North’, while leaving other countries unaggregated.

  While local recoding preserves more information than global recoding, it may be of much less utility for statistical and reporting purposes as a result of the inconsistency it introduces into the datasets; and

- **top and/or bottom recoding**, which is a type of recoding where, firstly, top and bottom thresholds are defined and, secondly, the values which cross these thresholds are recoded into the value of the threshold itself.

5.2. Information aggregation

Information aggregation involves collecting lower-granularity information, such as individual entries, and combining it to create higher-level information. Such aggregated information can provide summaries or overviews, for example with regards to the implementation of cybersecurity risk management measures, which can advise decisions on policy development and implementation.

At the same time, when properly aggregated, this higher-level information should no longer permit identification of the entities the information relates to and limits the exposure of any sensitive assets.

There are a number of ways to aggregate information, depending on the aim of the data analysis and presentation. For example:

- **summarising** the individual values;
- **averaging,** also referred to as calculating the mean. Averaging could be based on weighted or unweighted data. In case of the former, the averaging process takes into account the significance of the data point, such as its frequency;
- **grouping (generalising) based on a condition met**. This, for example, could involve pre-defined values, such as <10, 10-20, 20-30 and >30. Subsequently, occurrences falling within each group could be counted; and
- **minimums and maximums**, where only the minimum and maximum values in the dataset are taken into account for the aggregation purposes.

Table 6: Example of basic information aggregation

Region	Entities designated	Risk assessments notified	Ratio of controls implemented
A	42	30	90%
B	65	41	84%
C	34	15	73%
D	18	10	85%
Avg.[1]	40	24	83%

Note 1 – In this case, the averages assume four regions. They are also rounded and unweighted.

Once the information is aggregated, depending on its specific nature, it may need to be further anonymised. For example, by removing the outliers. In such case, depending on the number of removed outliers, the totals may need to be removed as well in order to prevent cross-identification.

Table 7: Example of an outlier low count

Type of certified ICT product	Region		Total
	A	B	
X	15	7	22
Y	10	3	13
Total	25	10	35

Table 7-A: Example where both the outlier low count and the totals have been removed

Type of certified ICT product	Region	
	A	B
X	15	7
Y	10	N/A

Table 7-B: Example with ranges instead of counts and without the totals

Type of certified ICT product	Region	
	A	B
X	15-19	5-9
Y	10-14	<5

In all cases, the resulting dataset needs to be reviewed based on the context and the resulting values to ensure that no sensitive information is inadvertently disclosed.

5.3. Recommendations for the entities

In most cases, basic anonymisation and aggregation techniques could be used to protect the information exchanged under the NCCS. For example, removing information of a certain type from the entire dataset, or aggregating the data based on summarising it and, where appropriate, averaging.

Nevertheless, this aggregation and anonymisation needs to operate within the confines of the entities' obligations under the NCCS. For example, to report specific cyber-attack related information to the national CSIRT and the competent authority.

Therefore, the entities need to firstly, identify the information which could prejudice their interests either directly, because the information itself is sensitive, or indirectly, because disclosing this information could permit identifying other otherwise confidential information. For example, by way of cross-referencing.

Secondly, once this sensitive information is identified, bearing in mind their obligations under the NCCS, the entities shall apply appropriate aggregation or anonymisation steps to ensure this information's confidentiality. If the entities are not obligated to provide specific sensitive information at all, they shall not provide it in order to fulfil the need-to-know principles. If the entities are obligated to provide specific sensitive information, yet their obligation could be discharged by providing the information in an appropriately aggregated format, then they shall adopt such a format.

Certain guidelines under the NCCS will provide recommendations to that end. For example, the ACER monitoring guidance pursuant to Article 12(3) of the NCCS.

Based on the list of the information flows by the entities foreseen under the NCCS and provided in Section 2, this subsection:

- outlines the information exchanged in some of these flows; and
- discusses how sensitive information could be anonymised or aggregated in a manner consistent with the provisions of the NCCS.

5.3.1. Disseminating information on cyber-attacks by the entities

Pursuant to Article 37(1)(f) of the NCCS, *'If a competent authority receives information related to a reportable cyber-attack, that competent authority (…) may request the reporting high-impact or critical-impact entity to further disseminate the reportable cyber-attack information in a secure manner to other entities that may be affected, with the aim to generate situational awareness by the electricity sector and to prevent the materialisation of a risk that may escalate in a cross-border cybersecurity electricity incident (…)'.*

This provision indicates the purpose of information sharing, namely generating situational awareness amongst other entities that may be affected. Two restrictions on information sharing are thus implicit.

Firstly, this provision limits the dissemination to other entities that may be affected, meaning that the originator should follow an appropriate distribution protocol, as recommended in Section 4 of this guideline. While it may not always be possible to define a closed group of entities that may be affected, the information sharing pursuant to this provision should not result in this information being communicated to the attackers or other unauthorised parties.

Secondly, the entities should remove any information that is not needed for other entities to identify similar cyber-attacks, threats or vulnerabilities. This includes:

- any personal data within the meaning of Article 4(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data related to their employees or customers[10], such as names, e-mail addresses or phone numbers;
- specific details of the impact, to the extent that sharing them could bring further risk to the entity;
- any confidential business information; and
- IP address of the entity impacted.

If the entities share logs as part of the dissemination of cyber-attack information, the entities should consider sanitising such logs. For example, by way of hiding specific IP addresses and domains.

5.3.2. Reporting on the risk assessment at entity level

The entities should only report on the information required by Article 27 of the NCCS at the highest possible aggregation level.

For example, in the context of Article 27(2) of the NCCS, the entities should report the risks in accordance with the risk impact matrix established pursuant to Article 19(2)(b) of the NCCS relating to the Union-wide high-impact and critical-impact processes developed in accordance with Article 19(2)(a) of the NCCS. The entity should not report the risks at the level of the underlying internal business processes supporting these Union-wide processes.

The ENTSO-E and the EU DSO Entity may issue non-binding guidance on entity-level risk assessments, including reporting.

5.3.3. Provision of Article 12(2)(a) monitoring information to ACER by the ENTSO-E and the EU DSO Entity

Pursuant to Article 12(2)(a), ACER shall *'review the status of implementation of the applicable cybersecurity risk management measures with regard to the high-impact and critical-impact entities (…)'.*

[10] OJ L 119, 4.5.2016.

In addition to the cooperation with the competent authorities referred to in Article 17(1) of the NCCS, ACER may request support from the ENTSO-E and the EU DSO Entity pursuant to Article 12(1) of the NCCS. This support would primarily consist of the ENTSO-E and the EU DSO Entity providing to ACER the Member State cybersecurity risk assessment information submitted by the competent authorities pursuant to Article 20(2) of the NCCS.

Such Member State risk assessment results will be reported as the risk of a compromise of the confidentiality, integrity or availability of each Union-wide high-impact and critical-impact process using the risk assessment methodologies developed by the ENTSO-E and the EU DSO Entity pursuant to Article 18(1) of the NCCS. The ENTSO-E and the EU DSO entity shall then aggregate the results of the Member States' cybersecurity risk assessments at a level of System Operation Regions ('**SOR**') in order to carry out regional risk assessments pursuant to Article 21 of the NCCS.

Thus, in the context of the Article 12(1) cooperation with ACER, the ENTSO-E and the EU DSO Entity could provide the results of the Member States' cybersecurity risk assessments to ACER at the same SOR-level of aggregation.

Provision of Article 12(2)(a) information to ACER by the competent authorities in the context of Article 17(1) or, once the Member State Cybersecurity Risk Assessments are completed, by the ENTSO-E and the EU DSO Entity, fulfils the need-to-know principle and avoids double notification, as prescribed by Recital 24 of the NCCS.

5.3.4. Sharing of Article 12(5) operational reliability performance indicators with ACER

Similarly to the above, provision of the aggregated annual results of the Article 12(5) operational reliability performance indicators to ACER by the CSIRTs in collaboration with the competent authorities would be optimal from the perspective of the need-to-know principle.

In any event, the operational reliability performance indicators should not contain any confidential information that could be useful to threat-actors. For example, they should not contain any information relating to risk assessments, high-impact or critical-impact processes, or assets.

5.3.5. Regional and comprehensive cybersecurity risk assessment reports

In order to carry out regional risk assessments and draw up a regional cybersecurity risk assessment report for each SOR pursuant to Article 21 of the NCCS, the ENTSO-E and the EU DSO entity will aggregate the results of the Member States' cybersecurity risk assessments at the SOR level. The aggregated information should not contain any information on the entities or the Member States. This same aggregation level should be applicable to the comprehensive cybersecurity risk assessment report pursuant to Article 23 of the NCCS.

Specifically, only SOR-level statistics should be provided on the following aspects, without any information connected to the related entities or the Member States:

- cyber threats;
- cyber-attacks;
- the implementation status of the minimum and advanced cybersecurity controls, as well as other cybersecurity measures; or
- information of derogations granted pursuant to Article 30(3) of the NCCS.

For completeness, the same protection in terms of anonymisation and aggregation must be afforded to the entities contributing the development of the comprehensive cross-border electricity cybersecurity risk assessment report pursuant to Article 23(3).

In addition to the removal of any information permitting direct identification of the entities or the Member States, the ENTSO-E and the EU DSO Entity shall ensure that none of the reports contains

any descriptions, comments or otherwise any other quantitative or qualitative information, which could risk cross-identification of the entities or the Member States.

5.3.6. Benchmarking and cost assessment related to cost recovery

This category pursuant to Article 11 and Article 13 contains the following information flows related to the entities:

- entities providing information to their NRAs relating to cybersecurity benchmarking pursuant to the NCCS;
- entities providing information to their NRAs relating to cost recovery pursuant to the NCCS; and
- ENTSO-E and EU DSO Entity providing aggregated pricing data to the NRAs for the purposes of system operation region benchmarking.

To the extent possible, the information exchanged in the context of these provisions should limit the presence of any data that could be useful to threat actors. Furthermore, any data should be provided at the highest possible aggregation level which permits the required cost or performance assessment by the NRAs.

Thus, for example, while the benchmarking analysis pursuant to Article 13(2)(a) necessitates a causal link between current investments in cybersecurity and mitigating risks having an impact on cross-border electricity flows, providing such a link should neither extend to information on vulnerabilities addressed, nor provide detailed descriptions of the internal business processes.

The cybersecurity benchmarking guide ACER will establish pursuant to Article 13(1) will include recommendations on the data the NRAs could request to provide them with the requisite information for the fulfilment of their benchmarking analysis task pursuant to Article 13(2) and Article 13(3), consistently with the need-to-know principle.

6. Summary grid of entity information flows and recommendations

Table 8: Non-exhaustive summary grid

Information flow	Within a Member State	Cross-border	Cross-border to an EU body
Entities (companies)			
Attacks to CA and CSIRT	National scheme Otherwise, TLP		
Attack info disseminated to other entities	National scheme Otherwise, TLP Remove confidential security, business and personal data	National scheme with explanation Otherwise, TLP Remove confidential security, business and personal data	
Threat information to CSIRT	National scheme Otherwise, TLP		
Unpatched actively exploited vulnerabilities to CSIRT	National scheme Otherwise, TLP		
Entity-level RA to CA	National scheme Otherwise, TLP Report risks at the highest level in accordance with risk impact matrix		
Benchmarking and cost recovery information to NRA	National scheme Otherwise, TLP		

Information flow	Within a Member State	Cross-border	Cross-border to an EU body
Art. 12(5) performance indicators to ACER			National scheme, if applicable SENSITIVE TLP:AMBER, if at least TLP:AMBER Only statistical data. No data useful to threat actors, such as risk assessment data
TCMP proposals to CAs	National scheme Otherwise, TLP		
ENTSO-E and EU DSO Entity			
Exchange draft TCMP information		TLP and MoU	
Exchange RA information		TLP and MoU	
TCMP proposals to ACER and ENISA			SENSITIVE TLP:AMBER, if at least TLP:AMBER
Draft Union-level RA to NIS Cooperation Group and ACER			SENSITIVE TLP:AMBER, if at least TLP:AMBER
Union-level RA submission to CAs, ACER, ENISA and Commission		TLP	SENSITIVE TLP:AMBER, if at least TLP:AMBER
Draft regional RA to NIS Cooperation Group			SENSITIVE TLP:AMBER, if at least TLP:AMBER Aggregate data at SOR level Only statistical data

Information flow	Within a Member State	Cross-border	Cross-border to an EU body
Draft Comprehensive cross-border RA to NIS Cooperation Group			SENSITIVE TLP:AMBER, if at least TLP:AMBER Aggregate data at SOR level Only statistical data
Comprehensive cross-border RA to NRAs and ACER		TLP Aggregate data at SOR level Only statistical data	SENSITIVE TLP:AMBER, if at least TLP:AMBER Aggregate data at SOR level Only statistical data
Benchmarking pricing information to NRAs		TLP Aggregate data at SOR level	
Art. 12(2)(a) monitoring information to ACER			SENSITIVE TLP:AMBER, if at least TLP:AMBER Aggregate data at SOR level Only statistical data

7. List of tables

Table 1: Non-exhaustive list of entity information flows foreseen under the NCCS 7
Table 2: The TLP markings 14
Table 3: The TLP colour-coding in RGB 17
Table 4: Example of basic local suppression 19
Table 5: Example of global recoding 20
Table 6: Example of basic information aggregation 21
Table 7: Example of an outlier low count 21
Table 7-A: Example where both the outlier low count and the totals have been removed 22
Table 7-B: Example with ranges instead of counts and without the totals 22
Table 8: Non-exhaustive summary grid 26