PROCUREMENT RECOMMENDATIONS FOR SUBSTATION GATEWAYS

Proposal of the TSOs, with the assistance of the ENTSO for Electricity, in cooperation with the EU DSO entity, for a non-binding cybersecurity procurement recommendations on gateways used for substation automation in accordance with Article 35 of the Commission Regulation (EU) 2024/1366 of 11 March 2024 establishing a network code for cybersecurity aspects of cross-border electricity flows

Table of Contents

TSOS, WITH THE ASSISTANCE OF ENTSO FOR ELECTRICITY AND IN COOPERATION WITH THE EU DSO ENTITY, TAKING INTO ACCOUNT THE FOLLOWING:

Whereas

(1) This document provides a non-binding cybersecurity procurement recommendation on gateways used for substation automation (hereafter referred to as "the recommendation") in accordance with Article 35, of Commission Regulation (EU) 2024/1366 establishing a network code for cybersecurity aspects of cross-border electricity flows (hereafter referred to as 'NCCS Regulation').

(2) The recommendation takes into account the general principles and goals set in the:

a) NCCS Regulation;
b) 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 (hereafter referred to as 'NIS 2 Directive');
c) Regulation (EU) 2019/941 of the European Parliament and of Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/ (hereafter referred to as the 'Risk Preparedness Regulation'); as well as
d) Regulation (EU) 2019/943 of the European Parliament and of Council of 5 June 2019 on the Internal Market for Electricity (recast) (hereafter referred to as the 'Electricity Regulation').

(3) TSOs, with the assistance of the ENTSO for Electricity, in cooperation with the EU DSO entity and following a consultation with the NIS Cooperation Group shall submit proposal for non-binding procurement recommendations in accordance with Article 18 of the NCCS Regulation.

SUBMIT THE FOLLOWING PROPOSAL FOR THE NON-BINDING CYBERSECURITY PROCUREMENT RECOMMENDATION ON GATEWAYS USED FOR SUBSTATION AUTOMATION

TITLE 1
General provisions

Article 1
Subject matter and scope

(1) This document provides non-binding procurement recommendations that high-impact and critical-impact entities may use as a basis for the procurement of gateways or remote terminal units (RTUs) used for substation automation in high-voltage electricity grids. The recommendations do not cover distribution automation gateways or RTUs used in medium-voltage electricity grids.

Article 2
Definitions

(1) For the purposes of this methodology for procurement recommendations on gateways, the terms used shall have the meaning given to them in Article 3 of the NCCS Regulation, Article 6 of the NIS 2 Directive, Article 2 of the Risk Preparedness Regulation and Article 2 of the Electricity Regulation.

(2) In this methodology for procurement recommendations on gateways, unless the context clearly indicates otherwise:

(a) the singular also includes the plural and vice versa;

(b) the table of contents and headings are inserted for convenience only and do not affect the interpretation of this methodology for procurement recommendations on gateways;

(c) any reference to legislation, regulations, directives, orders, instruments, codes, or any other enactment shall include any modification, extension, or re-enactment of it when in force; and

(d) any reference to an Article without an indication of the document shall mean a reference to this methodology for procurement recommendations on gateways.

TITLE 2
Procurement recommendation for substation automation gateways

Article 3
Procurement recommendation

(1) When procuring gateways for substation automation projects, it is recommended that entities use the gateway cybersecurity profile provided in Annex I. The profile includes technical security requirements for the gateway, and requirements for secure software development.

(2) When applying the profile, entities should verify that the profile can be used in their specific situation by verifying that:

(a) the scope in the profile matches the procurement scope;

(b) the intended use and intended operational environment are applicable to the entity's situation;

(c) the threats considered in the profile include all threats relevant to the entity, as determined by the entity level risk assessment;

(d) the assets, users, and functions cover all uses by the entity.

(3) Entities may use the profile as a baseline for their procurement requirements. They may add requirements to their individual procurement requirements. It is recommended not to change or delete requirements.

(4) Entities and suppliers may use the conformance statement included in the profile to more efficiently communicate about the implementation of the requirements in the profile.

(5) When selecting the supplier, entities must assess the risk profile of the supplier.