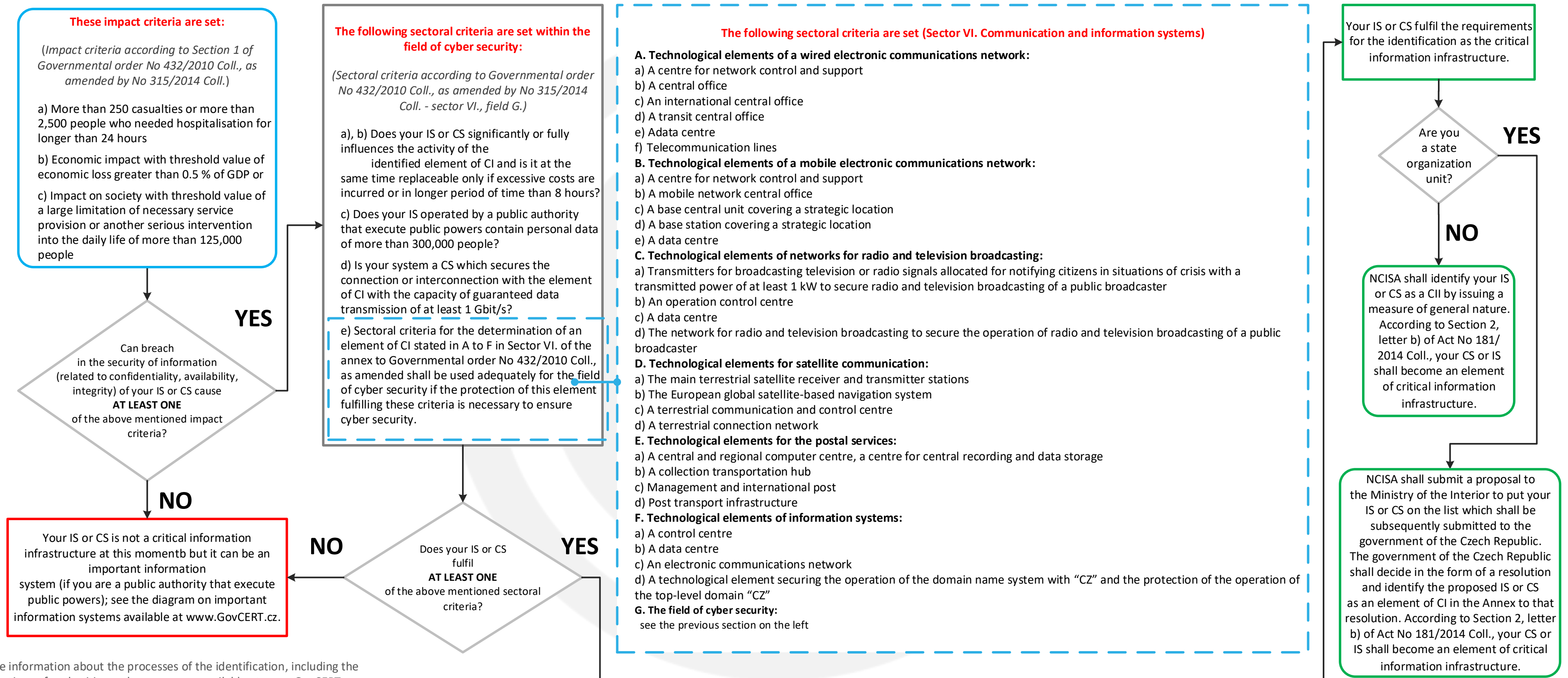


CRITICAL INFORMATION INFRASTRUCTURE

The process of the identification according to the Act No 240/2000 Coll., on Crisis Management and on the Amendment of Certain Acts (the Crisis Act) and Governmental Order No 432/2010 Coll. on the Criteria for the Identification of a Critical Infrastructure Element as amendment



More information about the processes of the identification, including the obligations of authorities and persons, are available at www.GovCERT.cz

Abbreviations: IS – information system, CB – cyber security, CI – critical infrastructure, CII – critical information infrastructure, CS – communication system, NCISA – National Cyber and Information Security Authority, MGN – measure of general nation

version 2.0, March 2018

Note:

NCISA shall cooperate with the concerned entities within the process of the determination of the critical information infrastructure (CII), even before the identification itself. The identification then shall be done after bilateral discussions. For state organizational units, the identification of CII elements is done by issuing the resolution of the government of the Czech Republic. For public authorities or legal or natural persons which are not state organizational units, the identification is done by issuing a measure of general nature (MGN) which is issued by NCISA. NCISA is available for potential discussions and for the provision of methodological help in the process of the assessment of fulfilling the determinative criteria.

Note:

This document is only a supporting guide and does not replace any act or implementing legislation. The right to make changes to this document reserved. This document is non-binding English translation.