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

These impact criteria are set:

- Impact criteria according to Section 1 of Governmental order No 432/2010 Coll., as amended by No 315/2014 Coll.
- More than 250 casualties or more than 2,500 people who needed hospitalisation for longer than 24 hours
- Economic impact with threshold value of economic loss greater than 0.5 % of GDP or
- Impact on society with threshold value of a large limitation of necessary service provision or another serious intervention into the daily life of more than 125,000 people

The following sectoral criteria are set within the field of cyber security:

- Sectoral criteria according to Governmental order No 432/2010 Coll., as amended by No 315/2014 Coll - sector VI: field G

a) Does your IS or CS significantly or fully influences the activity of a state
b) Does your IS or CS cause at the same time replacement only if excessive costs are incurred or in longer period of time than 8 hours
c) Does your IS or CS cause at the same time replacement only if excessive costs are incurred or in longer period of time than 8 hours
d) Does your IS or CS significantly or fully influences the activity of a state

The government of the Czech Republic shall decide in the form of a resolution and identify the IS or CS on the list which shall be fulfilled these criteria is necessary to ensure cyber security.

The following sectoral criteria are set (Sector VI. Communication and information systems)

A. Technological elements of a wired electronic communications network:
- A centre for network control and support
- A transit central office
- A control centre
- A data centre

B. Technological elements of a mobile electronic communications network:
- A centre for network control and support
- A mobile network central office
- A mobile network central office
- A data centre

C. Technological elements of networks for radio and television broadcasting:
- Transmitters for broadcasting television or radio signals allocated for notifying citizens in situations of crisis with a transmitted power of at least 1 kW to secure radio and television broadcasting of a public broadcaster
- An operation control centre
- A data centre
- The network for radio and television broadcasting to secure the operation of radio and television broadcasting of a public broadcaster

D. Technological elements for satellite communication:
- The main terrestrial satellite receiver and transmitter stations
- The European global satellite-based navigation system
- A terrestrial communication and control centre
- A terrestrial connection network

E. Technological elements for the postal services:
- A central and regional computer centre, a centre for central recording and data storage
- A collection transportation hub
- Management and international post
- Post transport infrastructure

F. Technological elements of Information systems:
- A control centre
- A data centre
- An electronic communications network
- A technological element securing the operation of the domain name system with “.cz” and the protection of the operation of the top-level domain “.cz”
- The field of cyber security: see the previous section on the left

Your IS or CS are not a critical information infrastructure at this moment but it can be an important information system (if you are a public authority that execute public powers); see the diagram on important information systems available at www.GovCERT.cz.

Can breach in the security of information (related to confidentiality, availability, integrity) of your IS or CS cause AT LEAST ONE of the above mentioned impact criteria?

Your IS or CS is not a critical information infrastructure. If you have other infrastructure systems available at www.GovCERT.cz.

CRITICAL INFORMATION INFRASTRUCTURE

For state organizational units

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: 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.

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, CS – 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

NCISA shall submit a proposal to the Ministry of the Interior to put your IS or CS as a CII by issuing a measure of general nature. According to Section 2, letter b) of Act No 181/2014 Coll., your IS or CS shall become an element of critical information infrastructure.

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.