Government Decree 65/2013 (III.8.) on the implementation of Act CLXVI of 2012 on the identification, designation and protection of critical systems and facilities

On the basis of the authorisation set out in section 14 a)-i) of Act CLXVI of 2012 on the identification, designation and protection of critical infrastructures and facilities,

as regards section 4(2) on the basis of the authorisation set out in section 174/A(1) of Act CXL of 2004 on the general rules of public administrative procedures and services,

as regards section 11(6) on the basis of the authorisation set out in section 80b) of Act CXXVIII of 2011 on disaster control and on the modification of certain related acts,

acting within its powers defined in Article 15(1) of the Fundamental Law, the Government orders the following:

1. Interpretative provisions

Section 1[1] For the purposes of this decree

1. *identification*: means the process during which the potential critical infrastructures are determined on the basis of risk analysis and sectoral and horizontal criteria,

2. *identification test*: means the process as a result of which the operator – as regards itself – makes a proposal in its identification report on its designation, on the revocation or maintenance of designation as a national or European critical infrastructure by analysing and assessing the possible fulfilment of the sectoral and horizontal criteria,

3. *risk analysis*: means the test of threat and risk factors for the purpose of assessing the consequences caused by the vulnerability, disruption or destruction of infrastructures.

2. Identification of possible critical infrastructures[2]

Section 2 (1)[3] The operator of the possible critical infrastructure prepares an identification report on the result of the identification test.

(2) The identification test contains:

a) the name of the possible critical infrastructure tested, the risk analysis and its result, the proposal on the designation as a national or European critical infrastructure, or the proposal on the revocation or maintenance of such designation,

b) the declaration of the operator on the completeness of the identification report, and

[1] Declared by Government Decree 375/2020 (VII.30.) section 37. Effective from: 31.07.2020

[2] Modified by Government Decree 375/2020 (VII.30.) section 52a)

[3] Modified by Government Decree 375/2020 (VII.30.) section 52b)

c)[1] the commencement and closing date of the identification test,

d)[2] the analysis of the criteria set out in section 2/A(2) of Act CLXVI of 2012 on the identification, designation and protection of critical infrastructures and facilities (hereinafter Hungarian CIP Act) if it may be established as regards the possible infrastructure that it belongs to the sub-sector defined in Annexes 1-3 to the Hungarian CIP Act which on the basis of Annex 4 is equivalent to any of the sectors or sub-sectors set out in Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union,

e)[3] the name, registered seat, mailing address, company registration number, statistical code and tax identification number of the operator, the name, phone number and e-mail address of its representative,

f)[4]name and address of the national critical infrastructures, services, and the names and addresses of those European critical infrastructures and services where Hungary is a party involved.

(3) If the operator fails to meet its obligation to prepare and submit an identification report, the designating authority appointed by the Government in a decree having sectoral responsibility (hereinafter designating authority) calls upon the operator by setting a deadline to prepare and submit the identification report.

(4) If the operator did not identify any infrastructure as critical infrastructure following the notification of the designating authority set out in paragraph (3) above, the operator shall even in this case submit the identification report, applying as regards its content the prescriptions set out in paragraph (2) mutatis mutandis.

(5) The identification report shall be sent for opinion to the sectoral advisory authority appointed by the Government in a decree (hereinafter advisory authority) by the designating authority. The advisory authority examines the identification report within 30 days following its receipt and sends its proposals regarding the risk analysis to the designating authority.

(6)[5] The advisory authority may initiate that the designating authority adopts a decision on obligating the operator pursuant to paragraph (3).

(7) The operator shall notify the designating authority in writing within 8 days on any change in its activities that affects the identification of the critical infrastructure.

(8)[6] Following the designation as national critical infrastructure the operator of the designated critical infrastructure shall prepare a new identification report, which shall be submitted to the designating authority within 15 days following the lapse of 5 years after the submission of the previous identification report to the designating authority.

Section 3[7] With consideration to public order, public safety, civil defence, constitutional protection, national security, counter-terrorism the Government designates the central body

---

[1] Modified by Government Decree 375/2020 (VII.30.) section 52b)

[2] Added by Government Decree 394/2017 (XII.13.) section 2(1). Effective from 10.05.2018

[3] Added by Government Decree 375/2020 (VII.30.) section 38(1). Effective from: 31.07.2020

[4] Added by Government Decree 375/2020 (VII.30.) section 38(1). Effective from: 31.07.2020

[5] Declared by Government Decree 441/2015 (XII.28.) section 194. Effective from: 01.01.2016, See: Government Decree 441/2015 (XII.28.) section 263

[6] Declared by Government Decree 375/2020 (VII.30.) section 38(2). Effective from: 31.07.2020

[7] Declared by Government Decree 375/2020 (VII.30.) section 39. Effective from: 31.07.2020

of the national disaster management to be the general advisory authority as regards designation as national critical infrastructures. Following the date on which the general advisory authority sends its case initiating proposal pursuant to section 10(2) of the Hungarian CIP Act, the sectoral designating authority conducts the designating procedure and the procedure for the revocation of the designation ex officio as regards the critical infrastructure, services, operators set out in the case initiating proposal.

3. Rules on designation as national critical infrastructure and revocation of the designation

Section 4[1] (1)[2] The designating authority adopts a decision on the designation as a national critical infrastructure or the revocation of such designation with the involvement of the relevant administrative authority – with the exceptions of the special rules concerning the procedure of designating non-sectoral critical infrastructures for national defence. If the central, regional or local body of the national disaster management acts as designating authority, the fulfilment of the horizontal criteria is tested by the designating authority in the administrative procedure.

(2) In the procedure for designating as national critical infrastructure or for the revocation of such designation, preliminary administrative opinion shall not be permitted.

(3) In its decision, the designating authority:

a) approves the identification report of the operator and designates the infrastructure as national critical infrastructure and orders its registration - provided that the possible fulfilment of at least one of each horizontal criterion defined in Annex 1 exits, from among the sectoral criteria and on the basis of the opinion of the administrative authority, and in the case set out in paragraph (1) on the basis of the decision of the authority,

b) approves the identification report of the operator and revokes the designation, and orders the deletion from the registry,

c) rejects the proposal on the designation, revocation of the designation or prescribes the submission of a new identification report by setting a deadline of 90 days at most and providing itemized indication of the defects and deficiencies identified,

d) approves that the operator did not identify any infrastructure as possible critical infrastructure,

e)[3] simultaneously with those set out in point a) above, it orders the registration of the operator in the list of operators of essential services, provided that those set out in section 2/A(2) of the Hungarian CIP Act are fulfilled as regards the national critical infrastructure, and it provides the essential service described in the list of Annex 3, or

f) in the case of the fulfilment of those set out in point b) above, it orders the deletion of the operator from the list of operators of essential services,

g)[4] decides on the upholding or revocation of the designation on the basis of the new identification report submitted after five years.

---

[1] Declared by Government Decree 323/2018 (XII.28.) section 28. Effective from: 01.01.2019

[2] Modified by Government Decree 375/2020 (VII.30.) section 52c)

[3] Declared by Government Decree 94/2020 (IV.7.) section 1. Effective from: 08.04.2020

[4] Added by Government Decree 375/2020 (VII.30.) section 40(1). Effective from 31.07.2020

(3a)[1] In the procedure for upholding the designation, seeking the advisory authority may be omitted if the new identification report did not reveal any new fact, circumstance, does not propose to designate a new infrastructure.

(4) In the procedure for designation as a national critical infrastructure or the revocation of such designation, the submission of the application at the government window is excluded.

(5) The designating authority informs the provider of the uniform digital radiocommunication system (hereinafter UDR) for government communication services on the fact and date of the designation as a national critical infrastructure, and the fact and date of the revocation of the designation. The service provider may not disclose the data known to it to third parties.

(5a)[2] The sectoral designating authority examines in the procedure initiated ex officio of the basis of the case initiating proposal of the general advisory authority, whether the sectoral criteria are fulfilled as regards the critical infrastructures, services, operators indicated in the case initiating proposal.

(6)[3]

4. Rules on designation as European critical infrastructure and revocation of the designation

Section 5[4] (1)[5] If the minister responsible for disaster control does not agree with those contained in the identification report prepared by the operator on the basis of the identification test conducted, or does not agree with the initiative of the advisory authority on the designation as a European critical infrastructure, the designation authority is obliged to examine the matter of designation as a national critical infrastructure, and in the case the conditions set out in the legal regulation are met, it decides on the designation a national critical infrastructure.

(2) If the minister responsible for disaster control does not agree with the initiative of another state party to the Agreement on the European Economic Area (hereinafter EEA state) on the designation of a European critical infrastructure, the minister informs the state initiating the designation thereof.

(3)[6] If the minister responsible for disaster control agrees with the initiative of an EEA state on the revocation of the designation of a European critical infrastructure or agrees with the request of the operator on the revocation of the designation of a European critical infrastructure the relevant rules of section 3(1a) of the Hungarian CIP Act shall be applied mutatis mutandis. The designating authority revokes the designation as European critical infrastructure by the adequate application of section 3(1a) of the Hungarian CIP Act, and in the case the conditions defined in the relevant legal regulations are fulfilled, it decides on the designation as a national critical infrastructure.

---

[1] Added by Government Decree 375/2020 (VII.30.) section 40(2). Effective from 31.07.2020

[2] Added by Government Decree 375/2020 (VII.30.) section 40(3). Effective from 31.07.2020

[3] Repealed by Government Decree 375/2020 (VII.30.) section 53a). Ineffective from 31.07.2020

[4] Declared by Government Decree 323/2018 (XII.28.) section 29. Effective from 01.01.2019

[5] Modified by Government Decree 375/2020 (VII.30.) section 52b)

[6] Modified by Government Decree 375/2020 (VII.30.) section 52d)

(4)[1] If the minister responsible for disaster control does not agree with the request of the operator on the revocation of the designation of a European critical infrastructure, the designating authority informs the operator on the upholding of the designation. If the revocation was initiated by an EEA state, the relevant rules of section 3(1a) of the Hungarian CIP Act shall be applied mutatis mutandis.

(5) In the course of designation as a European critical infrastructure, the minister responsible for disaster control examines the possibility of the fulfilment of the horizontal criteria.

(6) If the minister responsible for the relevant sector and the minister responsible for disaster control are of different opinions in the matter of the designation as a European critical infrastructure or the revocation of such designation, the Government shall settle the matter finally.

(7) In the procedure for the designation as a European critical infrastructure or the revocation of such designation, the submission of the application at a government window is excluded.

(8) The designating authority informs the provider of the uniform digital radiocommunication system (hereinafter UDR) for government communication services on the fact and date of the designation as a European critical infrastructure, and the fact and date of the revocation of the designation. The service provider may not disclose the data known to it to third parties.

(9)[2]

5. Qualification requirement and employment conditions of the security liaison officer

Section 6 (1)[3]

(2) Besides having a qualification relevant to the certain sector, the security liaison officer shall have

a)[4] higher education degree specialising in defence administration, disaster control or law enforcement administration,

b) qualification in law enforcement administration management specialising in fire protection, industrial security, or an equivalent qualification,

c) specialist training in industrial security,

d) higher education degree specialising in industrial security, or

e) with at least 5 years of experience in industrial security at the public service bodies of disaster control.

(3) The person having a higher education degree, employed for at least five years previously by a law enforcement body in responsibilities in the basic functions of the law enforcement body, is exempted from the requirements set out in paragraph (2)a)-c) above. Meeting the requirements for exemption shall be verified by the relevant person.

---

[1] Modified by Government Decree 375/2020 (VII.30.) section 52e)

[2] Repealed by Government Decree 375/2020 (VII.30.) section 53b). Ineffective from 31.07.2020

[3] Repealed by Government Decree 375/2020 (VII.30.) section 53c). Ineffective from 31.07.2020

[4] Declared by Government Decree 368/2016 (XI.29.) section 2. Effective from 01.01.2017

(3a)[1] In the case of critical infrastructures in the national defence sector, the person having higher education degree, employed for at least five years previously by a national defence body in responsibilities in the basic functions of the national defence body, is exempted from the requirements set out in paragraph (2) above. Meeting the requirements for exemption shall be verified by the relevant person.

(4) If the operator already provided for the employment of a person having the required qualifications, this person may be appointed as security liaison officer.

(5) The relevant person shall verify compliance with the conditions for eligibility.

(6)[2] The security liaison officer may be the employee of the operator, or may perform its tasks under an engagement agreement. The rules concerning the security liaison officer are set out in the rules of procedure of the operator, its regulations and other, internal document related to its organisation, as well as in the engagement agreement, whereby the security liaison officer reports to the highest management of the operator.

6. Operator security plan

Section 7 (1) The designating authority determines its decision pursuant to the Hungarian CIP Act on the content of the operator security plan with consideration to those set out in Annex 2.

(2)[3] The operator security plan shall be promptly modified by the operator

a) if such a change occurs that affects the service, activity, operation or security of the critical infrastructure,

b) in order to manage a risk newly emerged, if the risk related to the exceptional occurrence that took place was not tested in the operator security plan,

c) on the basis of the prescriptions of the authority or of the monitoring coordinating body, as regards the deficiencies revealed during monitoring or at the complex exercise.

(2a)[4] The operator shall review the operator security plan biannually, following its preparation and approval by the designating authority. The operator shall draw up the minutes of the review, and shall send it to the designating and registration authority by electronic means.

(3)[5] Prompt review may be initiated by

a) the designating authority,

b) with the exception of those set out in point c), the central body of the national disaster management at the designating authority, or

c) in the case of sectoral critical infrastructures for national defence, and those non-sectoral critical infrastructures for national defence, which have not been designated by other sectors as critical infrastructure, the monitoring coordinating body for the national defence sector, at the designating authority.

---

[1] Added by Government Decree 375/2020 (VII.30.) section 41(2). Effective from 31.07.2020

[2] Added by Government Decree 375/2020 (VII.30.) section 41(3). Effective from 31.07.2020

[3] Declared by Government Decree 375/2020 (VII.30.) section 42(1). Effective from 31.07.2020

[4] Declared by Government Decree 375/2020 (VII.30.) section 42(1). Effective from 31.07.2020

[5] Declared by Government Decree 375/2020 (VII.30.) section 42(1). Effective from 31.07.2020

(4)[1] The operator shall perform the prompt review within the deadline set out by the initiator and send the document prepared as a result of the review by electronic means for control to the designating authority and if the initiator was the central body of the national disaster management, then to the central body of the national disaster management.

(5)[2] If the operator security plan shall be modified pursuant to paragraphs (2)-(3) above, or section 6(8) o the Hungarian CIP Act, then the modified part of the plan or in the case of significant modifications, the consolidated draft of the operator security plan shall promptly be sent by the operator to the designating authority for material and formal control. If the modification was prepared on the basis of an imposition by the body conducting the complex monitoring, then the operator promptly sends the draft of the operator security plan to the designating authority for formal control only. The deadline for the control is 30 days following the receipt of the modified operator security plan by the designating authority. Following its material and formal control, the operator security plan modified pursuant to paragraphs (2)-(3) above is approved and sent by the sectoral designating authority – provided it is adequate – to the registration authority. If the modification was prepared on the basis of an imposition by the body conducting the complex monitoring, then the operator sends the draft of the operator security plan to the designating authority for formal control only.

(6) If as a result of the review the operator security plan does not need to be modified, the operator sends the minutes on the review, in copy, immediately after the closing of the review to the registration authority and the designating authority.

(7)[3] In compliance with the operator security plan, the operator organises and continuously ensures the security of the operation of the critical infrastructure and the conditions for its operational continuity.

(8)[4] The operator security plan and the risk analysis serving as the basis thereof shall be prepared and sent by the operator in the format defined and published on the website of the central body of the national disaster management, to the sectoral designating authority.

7. Monitoring and special rules of monitoring[5]

Section 8 (1)[6] The protection of the critical infrastructure – with the exception of the sectoral critical infrastructure for national defence, and those non-sectoral critical infrastructures for national defence, that were not designated in other sectors as critical infrastructure – is inspected by the body entitled to conduct the on-site inspection, with the coordination of the monitoring coordinating body, in a scheduled way, on the basis of an annual monitoring plan as well, acting jointly, in such a way, that the critical infrastructure is monitored at least in every 5 years. The annual monitoring plan is prepared by the monitoring coordinating body until 31 December of the year preceding the reference year. If the monitoring coordinating body intends to request the authority responsible for electronic information security to

[1] Declared by Government Decree 375/2020 (VII.30.) section 42(1). Effective from 31.07.2020
[2] Declared by Government Decree 375/2020 (VII.30.) section 42(1). Effective from 31.07.2020
[3] Declared by Government Decree 375/2020 (VII.30.) section 42(2). Effective from 31.07.2020
[4] Added by Government Decree 375/2020 (VII.30.) section 42(3). Effective from 31.07.2020
[5] Declared by Government Decree 375/2020 (VII.30.) section 43. Effective from 31.07.2020
[6] Declared by Government Decree 375/2020 (VII.30.) section 44(1). Effective from 31.07.2020

conduct the information and network security monitoring within the framework of the complex monitoring as regards critical infrastructures pursuant to Section 8(6) of the Hungarian CIP Act, then when compiling the annual monitoring plan, it shall take into account those set out in the annual monitoring plan pursuant to section 14(4) of Act L of 2013 on the electronic information security of state and municipal bodies (hereinafter Hungarian Cyber Security Act).

(2)[1] The central body of the national disaster management prepares a summary report on the complex monitoring procedures, the implementation of the monitoring plan until 1 March of the year following the reference year.

(3)[2] The monitoring coordinating body may request information from the bodies participating in the complex monitoring acting in their own competence when conducting inspections, moreover from the authority responsible for electronic information security on the results of their inspections, on the rectification of the deficiencies found, which information shall be provided by these bodies promptly.

(4)[3] Within the framework of complex monitoring the public service disaster control entity monitors

a) the authenticity of the data kept and managed by the registration authority pursuant to section 5(1) of the Hungarian CIP Act,

b) the completeness of the comprehensive personal, physical, administrative security of, the risks threatening the continuous operation of the critical infrastructure, as well as their management, included in the operator security plan.

(5)[4] The monitoring coordinating body may conduct extraordinary complex monitoring following

a) the event of extraordinary occurrence, or

b) the exceptional modification of the operator security plan.

(6)[5] The authority inspection may be conducted by requesting documents as well, if the inspection is aimed at the availability of the documentation and its contents.

(7)[6] The on-site inspection shall cover the authenticity, feasibility of the operator security plan, as well as the monitoring of the defects revealed at the operational exercise.

(8)[7] If the body entitled to conduct the on-site inspection does not participate in the complex monitoring, and the monitoring coordinating body presumes an infringement, that belongs to the competence of the body entitled to conduct the on-site inspection, such fact is disclosed to the body entitled to conduct the on-site inspection by the monitoring coordinating body within 8 days after the monitoring. The body entitled to conduct the on-

[1] Declared by Government Decree 368/2016 (XI.29.) section 4(1). Modified by Government Decree 375/2020 (VII.30.) section 52f)

[2] Declared by Government Decree 375/2020 (VII.30.) section 44(2). Effective from 31.07.2020 See Government Decree 375/2020 (VII.30.) section 52g) for its non-enforceable modifications

[3] Declared by Government Decree 368/2016 (XI.29.) section 4(2). Modified by Government Decree 375/2020 (VII.30.) section 52g).

[4] Added by Government Decree 375/2020 (VII.30.) section 44(3). Effective from 31.07.2020

[5] Added by Government Decree 375/2020 (VII.30.) section 44(3). Effective from 31.07.2020

[6] Added by Government Decree 375/2020 (VII.30.) section 44(3). Effective from 31.07.2020

[7] Added by Government Decree 375/2020 (VII.30.) section 44(3). Effective from 31.07.2020

site inspection shall inform the monitoring coordinating body within 30 days on the measures taken in relation to the findings set out in the notification.

8. The amount of the administrative fine to be levied on the operator and rules on levying such fine

Section 9 (1) Levying the fine on the operator pursuant to the Hungarian CIP Act may be initiated at the designating authority by authorities participating in administrative procedures related to the critical infrastructure as well.

(2)[1] The fine set out in paragraph (1) above may extend from HUF one hundred thousand to HUF ten million, in the case of the infringement set out in Annex 4 in the amount determined therein.

(3)[2] The amount of the fine shall be paid within 15 days from the decision on the fine becoming final to the fine deposit account set by the designating authority.

(4)[3] When making the payment, in the notes section of the transfer, the text "Lrtv bírság" (Hungarian CIP Act fine), the number of the decision and the name of the person obligated to pay the fine shall be indicated.

(5)[4] In the case of simultaneous existence of multiple infringements, the amount of the fine is the sum of the fines that may be levied for each of the infringements, which cannot exceed the cap of HUF ten million.

(6)[5] The fine may be levied again for the same facts – with the exception of the infringements that may be corrected immediately – after two months of communication of the final decision levying the fine.

9. Rules on record keeping and data security

Section 10 (1)[6] The central body of the national disaster management is appointed by the Government to keep the records of and manage the data in the registry of the designated European and national critical infrastructures and the operators of essential services – with the exception of the sectoral critical infrastructures for national defence, and the non-sectoral critical infrastructures for national defence, not designated by the designating authority responsible for the infrastructure or facility. In the case of non-sectoral critical infrastructures for national defence, that have been designated in other sectors too as critical infrastructures, keeping the records of and managing the data in the registry are done simultaneously by the central body of the national disaster management and the registration authority of the national defence sector. The designating decision shall be sent by the registration authority of the national defence sector to the central body of the national disaster management, with the exception of the sectoral critical infrastructures for national defence.

---

[1] Declared by Government Decree 375/2020 (VII.30.) section 45(1). Effective from 31.07.2020
[2] Modified by Government Decree 457/2017 (XII.28.) section 440b).
[3] Added by Government Decree 375/2020 (VII.30.) section 45(2). Effective from 31.07.2020
[4] Added by Government Decree 375/2020 (VII.30.) section 45(2). Effective from 31.07.2020
[5] Added by Government Decree 375/2020 (VII.30.) section 45(2). Effective from 31.07.2020
[6] Declared by Government Decree 375/2020 (VII.30.) section 46(1). Effective from 31.07.2020

(2)[1] The operator shall inform the registration authority pursuant to paragraph (1) and at the same time the designating authority on any change in the registered data, within 72 hours from such change, by electronic means.

(3) The bodies set out in section 5(4) of the Hungarian CIP Act may request data from the registration authority in writing, by defining the purpose of the data request and the accurate scope of the data to be received. The data reporting shall be fulfilled within 15 days.

(4)[2] The central body of the national disaster management provides access to the registry set out in paragraph (1) above, to the authority responsible for electronic information security, to the single point of contact appointed on the basis of Directive (EU) 2016/1148 of the European Parliament and of the Council by a government decree (hereinafter single point of contact) and to the case management centre set out in section 19(1)-(2) of the Hungarian Cyber Security Act, for the purpose of performing the tasks set out in section 5(4)g) of the Hungarian CIP Act, and to the advisory authority of the national defence sector for the purpose of performing the tasks set out in section 5(4)h) and i) of the Hungarian CIP Act.

10. Cooperation

Section 11 (1)[3] In the procedure of the authority or the administrative authority set out in section 4(1) above, the central or regional body of the national disaster management may request the opinion of

a) the central body of the National Tax and Customs Administration as regards the fulfilment of the criterion of economic effect,

b) the regional and central body for general policing responsibilities, the central body of the Constitutional Protection Office, the Counter-Terrorism Center, Counter-Terrorism Information and Criminal Analysis Center, the National Directorate General for Aliens Policing as regards the fulfilment of the criterion of societal effect,

c) the relevant government commissioner as regards the possible fulfilment of the criterion of political effect,

d) the regional environment protection authority, the regional water and water protection authority, the national nature conservation and environment protection authority, and the national water and water protection authority as regards the fulfilment of the criterion of environmental effect,

e) the regional body of the national disaster management as regards the fulfilment of the criterion of protection.

(2)[4]

(3)[5] In the course of providing their opinion on the basis of the identification report or their participation in the complex monitoring, the bodies defined in paragraph (1) above shall examine – besides the existence of the circumstances on which the designation was based – the existence of the physical, human and information technology security conditions of the

[1] Declared by Government Decree 375/2020 (VII.30.) section 46(1). Effective from 31.07.2020
[2] Declared by Government Decree 375/2020 (VII.30.) section 46(2). Effective from 31.07.2020
[3] Declared by Government Decree 375/2020 (VII.30.) section 47(1). Effective from 31.07.2020
[4] Repealed by Government Decree 375/2020 (VII.30.) section 53d). Ineffective from 31.07.2020
[5] Declared by Government Decree 375/2020 (VII.30.) section 47(2). Effective from 31.07.2020

critical infrastructures, the public areas belonging to them and the persons supervising and operating them which guarantee the protection against the risks identified, the intended operation, the avoidance of wilful and negligent injury.

(4)[1] For the purpose of preparing the monitoring plan set out in section 8(1) above, the relevant bodies shall – within the framework of cooperation – send their proposals necessary for the preparation of the monitoring plan to the central body of the public service disaster control entity each year, until 15 October of the year preceding the reference year, and indicate such in their own monitoring system, as well.

(5)[2] Within the framework of the cooperation, the operator shall immediately notify the designating authority and the central body of the public service disaster control entity, in the case of critical infrastructures for national defence – besides the above – the Central Emergency Operation of the Hungarian Defence Force, in the case of disaster threat or disaster.

(6)[3] Within the framework of the cooperation, upon the existence of an exceptional occurrence defined in the operator security plan,

a) the central body of the public service disaster control entity is entitled to obtain data necessary for intervention and averting such from the authorities and bodies responsible, and request their assistance;

b) the data reporting set out in point a) above shall be done by the relevant authority and body promptly, and the reporting cannot be denied by the authority or body sought;

c) the response to the exceptional occurrence, the organisation and management of rescue, the informing of the public, the assessment of damage, the possible restoration to the original status is done under the coordination of the central body of the public service disaster control entity;

d) the relevant designating authority may make proposals as to the involvement of the forces, assets necessary;

e) in identifying the underlying causes and the assessment of the measures taken, the relevant designating authority, the bodies involved in the intervention and the security liaison officer act jointly.

(7)[4] The sectoral designating authority shall inform the single point of contact as to the significance of the operator providing essential service relevant to the sector or sub-sector concerned.

11.[5] Complex exercise

Section 12[6] (1) The complex exercise under the Hungarian CIP Act shall be included in the annual monitoring plan under section 8 (1). The central body of the public service disaster

[1] Declared by Government Decree 368/2016 (XI.29.) section 5. Modified by Government Decree 375/2020 (VII.30.) section 52h).
[2] Declared by Government Decree 94/2020 (IV.7.) section 3. Effective from 08.04.2020
[3] Declared by Government Decree 375/2020 (VII.30.) section 47(3). Effective from 31.07.2020
[4] Added by Government Decree 375/2020 (VII.30.) section 47(4). Effective from 31.07.2020
[5] Declared by Government Decree 375/2020 (VII.30.) section 48. Effective from 31.07.2020
[6] Declared by Government Decree 375/2020 (VII.30.) section 48. Effective from 31.07.2020

control entity shall notify the operators involved in the complex exercise by 15 January of the relevant year. The complex exercise shall be so designed and implemented that

a) it does not adversely affect the performance of the operator's core activity,

b) the organisational and asset system as well as the information and network security resilience identified in the operator security plan shall be modelled on the possibility of real occurrence, taking into account the sectoral, sub-sectoral and territorial characteristics of the critical infrastructure,

c) it points to the interdependency exposures of each system, and

d) it facilitates the effective treatment of the damage and increased responsiveness.

(2) The complex exercise shall involve, in addition to the operator, the sectoral designating authority, the central body of the national disaster management and its regional or local body competent on the basis of the place of operation of the operator, and the security liaison officer. The complex exercise may involve the operator's supervisory body, as well as other entities involved in the elimination of an extraordinary occurrence, managed or controlled by the operator.

(3) If the result of the complex exercise is not qualified as adequate, the central or regional body of the national disaster management shall require the operator to reiterate the exercise by setting a deadline, whereby the failure to reiterate the complex exercise or in the case of another non-adequate classification a fine pursuant to Annex 4 may be levied.

(4) The complex exercise does not qualify as adequate if those contained in the operator security plan differ from reality to such an extent, that it may affect the business continuity of the designated critical infrastructure.

(5) Where, in the course of a complex exercise, the central or regional body of of the national disaster management determines that the operator security plan is inadequate, the operator shall be obliged to modify the operator security plan by setting a time-limit, in the case of the failure of which a fine in accordance with Annex 4 may be levied.

(6) Where, in the course of a complex exercise, the central or regional body of the national disaster management detects that a review of the information security policies and rules is necessary, it initiates a review of the information security policies and rules with the authority responsible for electronic information security.

11/A.[1] *Other rules for identifying operators of essential services*

Section 12/A[2] For the identification of operators of essential services which do not operate designated critical infrastructure the Government appoints the Special Service for National Security (hereinafter identification authority) under the Hungarian CIP Act.

Section 12/B[3] (1) The identification authority shall examine the possibility of identification as an operator of essential service

a) in the case of a refusal in accordance with section 4(3)c), or the revocation provided for in section 4(3)g),

b) in the case of bodies and facilities under national security,

[1] Added by Government Decree 375/2020 (VII.30.) section 49. Effective from 31.07.2020

[2] Added by Government Decree 375/2020 (VII.30.) section 49. Effective from 31.07.2020

[3] Added by Government Decree 375/2020 (VII.30.) section 49. Effective from 31.07.2020

c) with respect to the entity in the request from the European Union arrived at the single point of contact pursuant to the government decree on task and powers of the authorities responsible for the security oversight of electronic information systems, and the information security supervisor, moreover on the definition of closed electronic information systems,

d) on the basis of the data of the authority responsible for the security oversight of electronic information systems, data deriving from the vulnerability test and incident investigation pursuant to the Hungarian Cyber Security Act, as well as the data from the incident response centre defined in section 19(1) of the Hungarian Cyber Security Act.

(2) If the designating authority rejects the proposal for designation in accordance with section 4(3)c) above, or revokes the designation in accordance with section 4(3)g) above, it shall inform the identification authority about its decision.

(3) In the case of paragraphs (1) and (2) above, if the criteria set out in section 1d) of the Hungarian CIP Act are met, the identification authority initiates an official administrative procedure informing the relevant entity of the data on the basis of which it satisfies the criteria for identification as an operator of essential services.

(4) If the entity concerned agrees with the communication in accordance with paragraph (3) above, it shall inform the identification authority thereof within 30 days.

(5) If the entity concerned does not agree with the communication in accordance with paragraph (3) above, it shall - within 60 days - send its detailed reasoned opinion to the identification authority. The detailed reasoned opinion shall include the relevant entity's

a) detailed description of the service it provides,

b) list of its electronic information systems involved in providing the service, their role, their gravity in providing the service,

c) the contribution in the provision of other services.

(6) The identification authority decides whether or not to identify the entity as an operator of essential service by considering the information in paragraph (5).

(7) The identification authority shall send the decision on the identification as an operator of essential service and the data referred to in section 5(1)a) of the Hungarian CIP Act to the authority pursuant to section 10(1) above, for the purpose of registration.

Section 12/C[1] (1) The identification authority shall review the circumstances which serve as reasons for the identification of the operators of essential services in accordance with section 12/B,

a) at least once in every 3 years,

b) at the request of the operator of essential services upon termination, or

c) having regard to the change notified by the operator of essential services.

(2) It shall maintain or revoke its decision on the identification, depending on the outcome of the review.

Section 12/D[2] The identified operator of essential services shall promptly notify the identification authority in the case of the occurrence of such a change in its operation that affects the provision of essential services.

[1] Added by Government Decree 375/2020 (VII.30.) section 49. Effective from 31.07.2020

[2] Added by Government Decree 375/2020 (VII.30.) section 49. Effective from 31.07.2020

Section 12/E[1] The identification authority shall initiate a review of the list of essential services pursuant to the table set out in Annex 3, with the involvement of the relevant central administrative bodies, every 2 years.

Section 12/F[2] (1) In order to ensure that the scope of the operators of essential services is as aligned as possible with the operators of designated critical infrastructure, the authority in section 10(1) above shall inform the sectoral designating authority on the identification of the operator of essential services in accordance with section 12/B(3), that belongs to its sector.

(2) The sectoral designating authority shall examine the sub-sectors and sectoral criteria on which the designation is based, and shall, if necessary, initiate the inclusion of a new sub-sector into Annex 1 of the Hungarian CIP Act, as well as the amendment of the sectoral criteria.

12. Provisions on entry into force

Section 13 (1) This decree shall enter into force on the 3rd day following its promulgation with the exceptions set out in paragraphs (2)-(3) below.

(2) Paragraphs (2) and (3) of section 6 shall enter into force on 1 September 2014.

(3)[3] Section 17 shall enter into force on 1 July 2023.

13. Transitional provisions

Section 14[4]

Sections 15-15/C[5]

Section 15/D[6] (1) On the basis of the table set out in Annex 3 and the sectoral thresholds, the sectoral designating authority shall review the identification of the previously identified operators of essential services within 90 days from the entering into force of Government Decree 375/2020 (VII.30.) on the modification of certain cyber security related and other government decrees.

(2) Where, in the case of paragraph (1), the sectoral designating authority maintains the identification as the operator of essential services, it shall record in its decision the relevant row in Annex 3 as regards which the identification took place. It shall promptly communicate its decision to the registration authority keeping the registry of the operators of essential services and the authority responsible for the security oversight of electronic information systems.

(3) If, in the event of paragraph (1), the sectoral designating authority concludes - as a result of the review - that the operator of essential services who has previously been identified does not meet the criteria in accordance with section (1)d) of the Hungarian CIP Act, it shall adopt a decision on the revocation of the identification, which it shall communicate to the operator and it shall immediately inform the registration authority keeping the registry of the

---

[1] Added by Government Decree 375/2020 (VII.30.) section 49. Effective from 31.07.2020

[2] Added by Government Decree 375/2020 (VII.30.) section 49. Effective from 31.07.2020

[3] Added by Government Decree 368/2016 (XI.29.) section 6. Effective from 01.01.2017

[4] Repealed by Government Decree 233/2013 (VI.30.) section 11. Ineffective from 01.07.2013

[5] Repealed by Government Decree 375/2020 (VII.30.) section 53e). Ineffective from 31.07.2020

[6] Declared by Government Decree 375/2020 (VII.30.) section 50. Effective from 31.07.2020

operators of essential services and the authority responsible for the security oversight of electronic information systems.

14. Compliance with the law of the European Union

Section 16 This decree serves the purpose of compliance with the Council Directive (EU) 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

Section 16/A[1] This decree serves the purpose of compliance with the Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

15.[2]

Section 17[3]

Annex 1 to Government Decree No. 65/2013 (III.8.)

HORIZONTAL CRITERIA

Concerning single or directly related incidents in Hungary:

1. The criteria for losses shall be:

- under 24 hours, the number of victims exceeds 20 persons or the number of persons with serious injuries is at least 75, or
- under 72 hours, the number of victims exceeds 40, or the number of persons seriously injured is at least 150.

2. The economic impact criterion means the level of economic loss or the degree of deterioration of products and services, direct or indirect damage resulting from physical injury or loss of the system and facility, which exceeds 25% of the level of gross national income per capita (GNI) per any 30-day period regarding fifty thousand persons.

3. The societal impact criterion means serious disruption to public peace, including adverse psychological and public health effects, at a population of more than 300 inhabitants per km^2.

4. The political impact criterion means the loss of public confidence in the state and its institutions, due to a state body becoming inoperable, the perception of safety in the public falls under the critical level.

5. The environmental impact criterion means the event or process due to which, in the natural or constructed environment, in particular:

- an injury or disturbance occurring in the infrastructure, causes such a level of harm in the constructed or natural environment, as a result of which

= the evacuation or relocation of 10,000 persons becomes necessary, or

= an area of at least 100 km^2 will be permanently polluted, or

---

[1] Added by Government Decree 394/2017 (XII.13.) section 2(6). Effective from 10.05.2018

[2] Repealed on the basis of Act CXXX of 2010 section 12. Ineffective from 02.07.2018

[3] Enters into force on 01.07.2023

= groundwater or its natural aquifers, the rivers and natural lakes, as well as their beds or their flora and fauna suffer persistent damage;

- there is an irreversible negative change in the geographical areas or prominent regions of the country.

6.[1] The criterion on protection means injury, disruption, status, occurrence or process

- due to which the critical infrastructure is unable to fulfil its role in the supply chain,
- in the case of its injury or destruction the time period needed for intervention, rescue or remediation increase disproportionately, or
- the prevention of disasters, the remediation becomes temporarily impossible.

Annex 2 to Government Decree 65/2013 (III.8.)[2]

STRUCTURE OF THE OPERATOR SECURITY PLAN

Requirements for content

1. General presentation
1.1. name of the critical infrastructure
1.1.1. name of the operator
1.1.2. registered seat of the operator
1.1.3. address of the operator
1.1.4. mailing address of the operator
1.1.5. company registration number or sole entrepreneur's registration number of the operator
1.1.6. tax identification number of the operator
1.1.7. name of operator's representative
1.1.8. phone and fax number of the operator
1.1.9. e-mail address of the operator
1.1.10. in lack of accurate address, other identification data, geographical coordinate of the location of the infrastructure designated
1.2. security liaison officer
1.2.1. name of the security liaison officer
1.2.2. natural identification data of the security liaison officer (family name and first name, family name and first name at birth, place of birth, date of birth, mother's family name and first name at birth)
1.2.3. phone and fax number of the security liaison officer
1.2.4. e-mail address of the security liaison officer
1.3. general presentation of the organisation
1.3.1. activities of the organisation
1.3.2. governance structure of the organisation
1.3.3. main aims related to the security of the designated infrastructure
1.3.4. examination of the fulfilment and reasonability of the horizontal and sectoral criteria regarding the infrastructure
1.4. organisational structure and business management

[1] Added by Government Decree 375/2020 (VII.30.) section 51a), Annex 2. Effective from 31.07.2020

[2] Declared by Government Decree 375/2020 (VII.30.) section 51b), Annex 3. Effective from 31.07.2020

1.4.1. organisational structure, organisational chart
1.4.2. management of the organisation, senior management and their responsibilities
1.5. organisation personnel (own employees, external, contract employees)
1.5.1personnel number of the organisation, grouped by the status of the employees
1.5.2. number of external employees (from third parties, placement and outworkers, contract employees, contractors) grouped by the status of the worker, as regards critical procedures from operational point of view
1.6. general description of the activity and operation of the designated infrastructure, normal parameters of expected operation
1.6.1. overview of the activities of the infrastructure
1.6.2. normal operation parameters of the infrastructure (in particular the production number, capacity, fixed capital reserve and district supplied)
1.6.3. suppliers, designation of the upstream or downstream supply chain, general description of operational critical processes
1.6.4. if any element of the supply chain threatens the operational functioning of the designated critical infrastructure
1.6.4.1. supplier's company data
1.6.4.2. supplier's representative's contact details
1.6.4.3. guarantee for business continuity of the infrastructure, in the agreement with the supplier
1.6.4.4. supplier audit regulation, its existence, results, periodicity, penalties
1.6.5. description of the dependencies of the sectors and subsectors in which the infrastructures concerned and services may have an impact on operation
1.6.6. existing and completed conformity with standards, sectoral requirements
1.6.7. operations, technologies, conditions, services and processes critical to the operation of the infrastructure
1.7. identification and evaluation of elements of the designated infrastructure on the basis of the sectoral and horizontal criteria met
1.7.1. indication of sectoral criteria
1.7.2. indication of horizontal criteria
1.8. internal audit and management review
1.8.1. presentation of the internal audit system (especially the person of the auditors, their qualifications and internal training)
1.8.2. periodicity, results and documentation of internal audits
1.8.3. presentation of the management review system
1.8.4. periodicity, results, documentation of management review
1.9. managing and following-up changes.
1.9.1. changes implemented as a result of internal audits and management reviews and their follow-ups ("change management")

2. Presentation of the environment of the designated infrastructure
2.1. characterization of the areas surrounding the designated infrastructure
2.1.1. the natural location of the designated infrastructure
2.1.1.1. settlement
2.1.1.2. street
2.1.1.3. house number
2.1.1.4. floor, door
2.1.2. the topographical number of the designated infrastructure

2.1.3. geographical location (coordinates) of the designated infrastructure
2.1.4. top view (satellite) image of the designated infrastructure and its surroundings
2.1.5. the airspace and characteristics of the environment of the designated infrastructure
2.1.6. the name, address and scope of activities of the hazardous plants, factories and power plants located in the vicinity of the designated system infrastructure that affect its operation
2.1.6.1. potential impact on its activities
2.1.7. key information on the natural environment
2.1.7.1. area-specific meteorological characteristics resulting in damage to the designated infrastructure and influencing the consequences
2.1.7.2. the most important geological and hydrological characteristics of the site that affect the safe activities, operation and business of the designated infrastructure
2.1.7.3. presentation of other external factors affecting operation

3. Presentation of the designated infrastructure
3.1. a detailed description of all the elements of the designated infrastructure (in particular the means, equipment, technological and maintenance processes, operations and logging to ensure the operation of the designated infrastructure during normal operation)
3.1.1. presentation of the process of proper operation, together with the equipment ensuring operation
3.1.1.1. a description of the resources and capacities required to ensure proper operation
3.1.1.2. presentation of backup assets and services for proper operation
3.1.1.3. the time required to integrate backup assets and services into normal operation
3.1.1.4. the process, rules and timeline of returning to normal operation from backup equipment and services
3.1.1.5. periodic testing of backup equipment and services
3.1.1.6. presentation of the minimum operation process, together with the equipment ensuring operation
3.1.1.7. a description of the resources and capacities required to ensure minimum operation
3.1.2. scale drawing of all its elements, as well as the related explanation and guide
3.1.3. a description of the IT systems, devices and networks that affect the operation of the designated infrastructure in a relevant way
3.1.4. description of the role of IT systems, devices, networks in the operation of the designated infrastructure
3.2. the infrastructure serving the site
3.2.1. provision of electric power
3.2.1.1. provider of electric power
3.2.1.2. territorial provision of electric power
3.2.1.3. presentation of technical maintenance and repairs performed by the service provider (especially the method, order, periodicity of communication)
3.2.1.4. presentation of power supply connection points
3.2.1.5. presentation of internal electric power supply
3.2.1.6. provision of backup and alternative electrical systems
3.2.1.6.1. presentation of backup electrical system
3.2.1.6.2. backup electrical system capacity
3.2.1.6.3. backup electrical system supply area

3.2.1.6.4. presentation of technical maintenance and repairs of the backup electrical system
3.2.1.6.5. presentation of the alternative electrical system
3.2.1.6.6. alternative electrical system capacity
3.2.1.6.7. alternative electrical system supply area
3.2.1.6.8. presentation of technical maintenance and repairs of an alternative electrical system
3.2.2. provision of pipeline gas supply
3.2.2.1. pipeline gas supply provider
3.2.2.2. territorial provision of pipeline gas supply
3.2.2.3. presentation of the technical maintenance and repairs performed by the service provider
3.2.2.4. presentation of pipeline gas supply connection points
3.2.2.5. presentation of internal pipeline gas supply
3.2.2.6. providing a backup and alternative gas system
3.2.2.6.1. presentation of a backup gas system
3.2.2.6.2. backup gas system capacity
3.2.2.6.3. backup gas system supply area
3.2.2.6.4. presentation of technical maintenance and repairs of the backup gas system
3.2.2.6.5. presentation of an alternative gas system
3.2.2.6.6. alternative gas system capacity
3.2.2.6.7. alternative gas system supply area
3.2.2.6.8. presentation of technical maintenance and repairs of an alternative gas system
3.2.3. provision of public drinking water supply
3.2.3.1. service provider of public drinking water supply
3.2.3.2. territorial provision of public drinking water supply
3.2.3.3. presentation of technical maintenance and repairs performed by the service provider
3.2.3.4. presentation of connection points for public drinking water supply
3.2.3.5. presentation of internal public drinking water supply
3.2.3.6. providing a backup and alternative drinking water system
3.2.3.6.1. presentation of the backup drinking water system
3.2.3.6.2. backup drinking water system capacity
3.2.3.6.3. backup drinking water system supply area
3.2.3.6.4. presentation of technical maintenance and repairs of the backup drinking water system
3.2.3.6.5. presentation of an alternative drinking water system
3.2.3.6.6. alternative drinking water system capacity
3.2.3.6.7. alternative drinking water system supply area
3.2.3.6.8. presentation of technical maintenance and repairs of an alternative drinking water system
3.2.4. drinking water purification procedure (in case of own water source)
3.2.4.1. presentation of procedure
3.2.4.2. capacity data and maintenance
3.2.5. provision of public utility sewage drainage
3.2.5.1. service provider for public utility sewage drainage
3.2.5.2. territorial supply of public utility sewage drainage

3.2.5.3. presentation of technical maintenance and repairs performed by the service provider
3.2.5.4. presentation of connection points for public utility sewage drainage
3.2.5.5. presentation of internal public utility sewage disposal
3.2.6. information and communication technologies (hereinafter ICT) network supply
3.2.6.1. list of ICT services
3.2.6.2. ICT service provider
3.2.6.3. presentation of technical maintenance and repairs performed by the service provider
3.2.6.4. presentation of internal ICT system
3.2.6.5. presentation of internal ICT network
3.2.6.6. presentation of ICT systems / applications necessary for the operation of the critical infrastructure
3.2.6.7. presentation of ICT systems and applications obtained from third parties, necessary for the operation of the critical infrastructure
3.2.6.8. presentation of the dependence and effects of the critical infrastructure on ICT systems and applications
3.2.6.9. the dependence of the ICT systems, applications and networks of the critical infrastructure on the power supply systems providing service
3.2.6.10. presentation of the service levels of the ICT systems defined by the operator (thus especially normal, reduced, minimum operation)
3.2.6.11. providing a backup and alternative ICT system
3.2.6.11.1. presentation of a backup ICT system
3.2.6.11.2. backup ICT system capacity
3.2.6.11.3. backup ICT system supply area
3.2.6.11.4. presentation of technical maintenance and repairs of the backup ICT system
3.2.6.11.5. presentation of an alternative ICT system
3.2.6.11.6. alternative ICT system capacity
3.2.6.11.7. alternative ICT system supply area
3.2.6.11.8. presentation of technical maintenance and repairs of the alternative ICT system
3.2.7. district heating supply
3.2.7.1. list of district heating service
3.2.7.2. district heating service provider
3.2.7.3. service coverage area
3.2.7.4. presentation of technical maintenance and repairs by the service provider
3.2.7.5. presentation of on-site processing of district heating
3.2.7.6. presentation of alternative or backup systems used in case of district heating outage
3.2.7.7. list of district heating system providers that ensure the continuous operation of the designated critical infrastructure
3.2.8. other
3.2.8.1. presentation of all other services that are essential for the operation of the infrastructure and that affect the continuity of business operations, detailing the following points
3.2.8.2. presentation of the service system used
3.2.8.3. presentation of the service providers used
3.2.8.4. alternative service provider to ensure provision of the same service
3.2.8.5. presentation of service capacity data

3.2.8.6. presentation of the minimum level of service required for proper operation
3.2.8.7. presentation of the impact of service outages on operations
3.2.8.8. providing a backup and alternative service system used
3.2.8.8.1. presentation of the backup service system used
3.2.8.8.2. capacity of the backup service system used
3.2.8.8.3. the area of supply of the backup service system used
3.2.8.8.4. presentation of technical maintenance and repairs of the backup service system used
3.2.8.8.5. presentation of the alternative service system used
3.2.8.8.6. capacity of the alternative service system used
3.2.8.8.7. the area of supply of the alternative service system used
3.2.8.8.8. presentation of technical maintenance and repairs of the alternative service system used
3.3. presentation of the structure, elements, detailed activities, production and operational processes of the designated infrastructure, the most important technological and maintenance processes and operations related to the activities
3.3.1. presentation of the activity of the critical infrastructure, together with capacity data
3.3.2. presentation of the most important technological, operational and work processes related to the activities
3.3.2.1. the purpose of the activity
3.3.2.2. the resource required for proper operation
3.3.2.2.1. human
3.3.2.2.2. technical, technological
3.3.2.2.3. material
3.3.2.2.4. third party service
3.3.2.2.5. detailed presentation of the connection points of the server infrastructure and the technological, operational and work processes
3.3.2.3. the minimum resources required for proper operation
3.3.2.3.1. human
3.3.2.3.2. technical, technological
3.3.2.3.3. material
3.3.2.3.4. third party service
3.3.2.3.5. detailed presentation of the connection points of the server infrastructure and the technological, operational and work processes
3.3.3. presentation of the most important maintenance processes related to the activities
3.4. identification, quantity and storage data of potentially hazardous materials and equipment
3.4.1. presentation of materials posing a threat to proper operation
3.4.2. handling, transport and storage of materials that pose a threat to proper operation
3.4.3. destruction and removal of materials that pose a threat to proper operation
3.4.4. presentation of equipment that pose a threat to proper operation
3.4.5. handling, transport, storage and maintenance of equipment that pose a threat to proper operation
3.4.6. destruction and removal of equipment that pose a threat to proper operation
3.5. internal and external information systems
3.5.1. presentation of the organisation's communication strategy
3.5.2. the organisation's communication procedures
3.5.3. presentation of the organisation's crisis communication strategy

3.5.4. the organisation's crisis communication procedures
3.5.5. presentation of internal information systems, tools, services
3.5.6. presentation of external (third-party) information systems, tools, services
3.6. supervisory and security organisations, their equipment and operation
3.6.1. presentation of security service [if outsourced, presentation of third-party security service(s)]
3.6.2. presentation of first aid and rescue organisations (if outsourced, presentation of third-party security services)
3.6.3. presentation of occupational safety and health organisation (if outsourced, presentation of third-party service)
3.6.4. presentation of fire protection organisation (if outsourced, presentation of third-party service)
3.6.5. presentation of environmental organisation (if outsourced, presentation of third-party service)
3.6.6. presentation of technical security service (if outsourced, presentation of third-party service)
3.6.7. presentation of a disaster response organisation (if outsourced, presentation of third-party service)
3.6.8. presentation of the remote monitoring and surveillance network (if outsourced, presentation of third-party service), minimum requirement is for the signalling and sensing devices in the system to be indicated on the blueprint and to attached to the document
3.6.9. demonstration of laboratory capacity (if outsourced, demonstration of third-party service)
3.6.10. presentation of the access and intrusion detection system, minimum requirement is for the places protected by the system to be indicated on the blueprint and attached to the document
3.6.11. presentation of a closed-circuit camera surveillance system, minimum requirement is the layout drawing of cameras and dispatch centres, indicating the areas covered by the cameras
3.6.12. presentation of the fire alarm system, minimum requirement is for the locations, equipment and dispatch centres protected by the system to be indicated on the blueprint and attached to the document
3.6.13. presentation of the fire-fighting system, minimum requirement is for the places and devices protected by the system to be indicated on the blueprint and attached to the document
3.6.14. presentation of other device, system, service ensuring the security of the infrastructure (if relevant, indicating it on the blueprint and attaching it to the document)

4. Identification, assessment, management of risks (the operator identifies, assesses and manages the risks associated with the designated infrastructure)
4.1. presentation of the risk management system maintained by the operator
4.1.1. presentation of responsibilities
4.1.2. presentation of risk management methodology
4.2. itemized identification and assessment of risks, in particular using the following elements:
4.2.1. meteorological risks
4.2.1.1. stormy wind
4.2.1.2. lightning strike

4.2.1.3. extreme temperature conditions (extreme high / low)
4.2.1.4. extreme rainfall
4.2.2. geological risks
4.2.2.1. earthquake
4.2.2.2. flooding
4.2.2.3. inland water
4.2.3. human risks
4.2.3.1. external attack
4.2.3.2. wilful damage caused by an internal employee
4.2.3.3. negligent damage caused by an internal employee
4.2.3.4. lack of skills
4.2.3.5. critical staff shortage
4.2.3.6. wilful damage caused by an outside worker
4.2.3.7. negligent damage caused by an outside worker
4.2.3.8. epidemic of human origin
4.2.3.9. epidemic of animal origin
4.2.4. technical risks
4.2.4.1. electricity supply outage
4.2.4.2. building engineering failure
4.2.4.3. dispatch centre failure
4.2.4.4. water supply outage
4.2.4.5. district heating service outage
4.2.4.6. gas supply outage
4.2.4.7. pipe breaking, inside a facility, building
4.2.4.8. pipe breaking within the technological field
4.2.4.9. redundant power failure
4.2.4.10. air conditioning outage
4.2.5. communication risks
4.2.5.1. failure of news technology
4.2.5.2. failure of redundancy technique
4.2.5.3. failure of communication channels
4.2.5.4. UDR failure
4.2.5.5. IP phone failure
4.2.5.6. analogue phone failure
4.2.5.7. internet service outage
4.2.6. fire
4.2.6.1. facility fire
4.2.6.2. fire in technological space
4.2.6.3. server room fire
4.2.7. IT risks
4.2.7.1. server failure
4.2.7.2. failure of software used
4.2.7.3. data connection failure
4.2.7.4. workstations failure
4.2.7.5. uninterruptible power supply failure
4.2.7.6. network failure
4.2.7.7. failure of IT system, application used (per system)
4.2.7.8. cyber-attack, attack from cyberspace

4.2.8. risks related to hazardous materials and technologies
4.2.8.1. radiological hazard
4.2.8.2. danger related to hazardous materials (fire, overpressure, poisoning)
4.2.8.3. biological hazard
4.2.9. other sector-specific risks
4.3. interdependent connections of the designated infrastructure and assessment of the resulting risks (i.e. what other sectors, organisations, persons are affected by the failure of the designated infrastructure) and supplementing the risk list with them
4.4. exploration of the probable causes of the risks, determination of the negative effects that can be predicted upon occurrence, determination of the damage value incurred
4.5. preparation of a risk assessment table based on the probability of occurrence, the level of jeopardising effects and the exposure to third parties
4.5.1. the probability of occurrence may be: very rare, rare, occasional, frequent, very frequent (on a scale of 1 to 5)
4.5.2. the level of jeopardising effects can be: negligible, low, medium, high, catastrophic (on a scale of 1-5)
4.5.3. exposure to a third party may be: obtained from a third party or provided by the operator on its own responsibility or not applicable (on a scale of 1-2) - where the value of "2" is weighted
4.6. Risk management
4.6.1. supplementing the risk assessment table with measures taken to manage, accept and transfer the risk
4.6.2. definition of extraordinary occurrences (minimum content requirement: name, extent of the event, notification procedure, procedure to be followed)
5. Means of protection of the designated infrastructure in the event of an extraordinary occurrence
5.1. description of the general measure to ensure the protection of the infrastructure
5.2. presentation of the special measure ensuring the protection of the infrastructure individually as per the risks identified in points 4.2-4.5 above
5.3. description of the procedure to be followed in the event of an extraordinary occurrence to ensure the protection of the infrastructure
5.4. list of organisational units involved in the management of the extraordinary occurrence
5.5. presentation of the equipment required for the protection of the designated infrastructure and the processes and infrastructures required for management and decision-making
5.5.1. instruments for notifying the management in the event of an extraordinary occurrence
5.5.2. procedures for notifying the management in the event of an extraordinary occurrence
5.5.3. instruments for alerting employees upon extraordinary occurrence
5.5.4. procedures for alerting employees upon extraordinary occurrence
5.5.5. application of own means and resources to mitigate the consequences of an extraordinary occurrence
5.5.6. managerial governance process
5.5.7. decision-making competencies, responsibilities
5.5.8. conditions and measures necessary for a minimum level of continuous operation
5.5.9. conditions and measures necessary for the normal level of continuous operation

5.5.10. conditions and measures necessary for on-site and remote work in continuous operation
6. The procedure for communication and co-operation with national defence bodies in the case of a critical infrastructures for national defence
6.1. The procedure for communication with national defence bodies in the case of a critical infrastructures for national defence
6.2. The procedure for co-operation with national defence bodies in the case of a critical infrastructures for national defence

Formal requirements

The operator security plan shall be prepared in writing, with the sections indicated in the part “Content requirements”. The approved operator security plan shall be submitted electronically to the designating authority, signed by the operator and the security liaison officer.
Maps may also be submitted on electronic media. The map outline or site plan shall contain the entire designated infrastructure and shall be in a resolution and format that provides adequate navigation.

Annex 3 to Government Decree 65/2013 (III.8.)[1]

LIST OF ESSENTIAL SERVICES

	A	B	C	D
	SECTOR	SUB-SECTOR	NAME OF ESSENTIAL SERVICE	DEFINITION OF ESSENTIAL SERVICE
1.	Energy	electric energy	electric energy - operation of transmission grid	the service, defined in point 1 of section 3 of Act LXXXVI of 2007 on Electric Energy, and means any technical and economic activity necessary for the transmission of electricity over the transmission grid or related thereto which is justified in order to ensure the transmission of electricity in an appropriate quality
2.			electric energy – transmission system operator	the service, defined in point 51 of section 3 of Act LXXXVI of 2007 on Electric Energy, provides for the smooth and safe operation of the electricity system, the equilibrium of its capacities and the total of the dedicated activities for the availability of international links
3.			electric energy - distribution	the service, defined in point 8 of section 3 of Act LXXXVI of 2007 on Electric Energy, providing for the transmission of electricity to users through transmission grids, and any related technical and economic activities necessary for the transmission of electricity to ensure an adequate quality transmission
4.			electric energy - production	the service provided by accredited power plants with a production operation licence, with a nominal capacity of 50 MW or greater than 50 MW pursuant to Section 4(1) of Act LXXXVI of 2007 on Electric Energy

[1] Declared by Government Decree 375/2020 (VII.30.) section 51c), Annex 4. Effective from 31.07.2020

5.			Black Start Service (keeping equipment necessary for the restarting of the system on standby for the transmission system operator)	the service resulting from the capability of each accredited producer, operator to start at least one generating unit without external voltage and capability of regulating the voltage and power emitted on the grid and the frequency (island)
6.		petroleum	production of finished petroleum product	the service that ensures the production of the domestic finished product demand (motor diesel, motor gasoline, kerosene type jet fuel)
7.			storage necessary for the production of finished petroleum product	the service that provides the stockpiling of raw materials required for the production of domestic finished product demand (motor diesel, motor gasoline, kerosene type jet fuel)
8.		natural gas	natural gas transmission	the service defined by point 34. of section 3 of Act XL of 2008 on natural gas supply, which is necessary for the transmission of natural gas through a transmission pipeline
9.			system management	the service defined by point 52 of section 3 of Act XL of 2008 on natural gas supply, which covers the performance of the management and coordination tasks of the cooperating natural gas system, specified in the act on natural gas supply
10.			natural gas distribution	the service defined by point 24 of section 3 of Act XL of 2008 on natural gas supply, and by means of which natural gas is transmitted to the user through a distribution pipeline
11.			natural gas storage	the service defined by point 31 of section 3 of Act XL of 2008 on natural gas supply, and which is the storage of natural gas on the basis of a permit

12.		district heating	district heating service	in accordance with section 3 q) of Act XVIII of 2005 on the district heating service, it is a public service providing the user with heat supply, i.e. heating and/or other heat-generating power from a district heating system through a heating pipeline, in the course of the commercial operation of the licensee
13.	Transportation	aviation	air traffic controller (ATC) service	a service (including area control service, approach control service and airport control service), whose duties are to: a) prevent collisions between aircrafts as well as between aircraft and barriers in the working area and b) ensure fast and orderly air traffic
14.			airport security control service	the activity which includes the use of electronic access control systems, CCTV and electronic fence systems, and the use of protective equipment incorporated in the baggage handling system, and the application of the electronic control of the network of security equipment and of the access cards (before a security screening)
15.			ground handling	the activity involving the operation and use of the baggage handling system (check-in desks, CUTE terminal, baggage conveyor belts), automatic baggage tag printing, automatic boarding pass control gates, stand planning and apron services, and noise monitoring system
16.		rail transport	rail infrastructure management service	the service involving the operation and maintenance of the railway infrastructure, including the operation of

				control-command, safety and signalling systems
17.			rail infrastructure capacity allocation service	the service which provides for the definition of each train path, the assessment of its availability and its allocation for the purpose of operating rail transport
18.			passenger transport by rail	the service which means passenger transport by rail vehicle on the basis of a contract for a fee, and ancillary services related thereto
19.			rail freight services	the service which means the freight of goods by rail with a railway vehicle to a third party on the basis of a contract for a fee.
20.			logistics centre operation	the service involving the operation of railway communication networks, traffic control systems and data transmission lines in order to ensure the efficient organisation of the movement of goods
21.		road transport	traffic control system	the traffic control system which a) is linked to the designated critical infrastructure pursuant to section 10a) of Government Decree 161/2019 (VII.4.) on the identification, designation and protection of critical systems and including any intelligent transport system that may be part of it, or b) operates in a town with a population exceeding 500,000 persons
22.	Drinking water supply	-	public utility drinking water supply	drinking water service pursuant to point 24. of section 2 of Act CCIX of 2014 on water supply utilities which is provided through the water supply utility set out in point 1. of section 2 of Government Decree 541/2013 (XII.30.) on the identification,

				designation and protection of critical water management infrastructures and water construction works
23.	Healthcare system	-	healthcare services	the service provided for by section 3e) of Act CLIV of 1997 on the healthcare system (hereinafter Healthcare Act) which is carried out by such a healthcare service provider, that is publicly financed, participates either directly or indirectly in the healthcare services set out in the Healthcare Act (indirect participation shall mean the healthcare service that is purchased from a third party by a publicly financed healthcare service provider)
24.			pharmaceutical supply	pharmaceutical wholesale activities provided to ensure healthcare services, carried out by an economic entity set out in section 10a) of Government Decree 246/2015 (IX.8.) on the identification designation and protection of critical systems and facilities for healthcare
25.	Finance	-	banking services	a credit institution carrying out activities set out in section 3(1)a)-b) of Act CCXXXVII of 2013 on credit institutions and financial undertakings, having a registered seat in Hungary, with at least 10% market share (on a balance sheet total basis)
26.			operation of multilateral or organised trading facilities	investment service activities pursuant to Section 5 (1) h) and i) of the Act CXXXVIII of 2007 on investment firms and commodity exchange service providers and the rules on the activities they may carry out, performed in connection with a financial instrument in the framework of a regular economic activity

27.			central counterparty service	the activity defined in section 5(1)83 of Act CXX of 2001 on the capital market
28.	Digital infrastructure	-	fixed internet access service	service specified in the classification developed and published by the National Media and Communications Authority pursuant to point 58 of section 188 and section 76 (4) of Act C of 2003 on Electronic Communications for the purpose of organising electronic communication networks and electronic communication services
29.			nomadic internet access service	service specified in the classification developed and published by the National Media and Communications Authority pursuant to point 58 of section 188 and Section 76 (4) of Act C of 2003 on Electronic Communications for the purpose of organising electronic communication networks and electronic communication services
30.			mobile internet access service	service specified in the classification developed and published by the National Media and Communications Authority pursuant to point 58 of section 188 and section 76 (4) of Act C of 2003 on Electronic Communications for the purpose of organising electronic communication networks and electronic communication services
31.			data exchange (IXP) service	electronic communications services provided by a natural or legal person through a data exchange centre (a shared electronic communications network), on the basis of received IP data traffic or initiated by subscribers, electronic communications

				providers or by technically independent networks of providers of information society services (autonomous systems)
32.			DNS service	a service that serves queries for data registered in a hierarchically structured domain name system (DNS) on the Internet
33.			top level domain name (TLD) registry service	service for the registration and management of internet domain names under a top-level domain (TLD)

Annex 4 to Government Decree 65/2013 (III.8.)[1]

FINE

	A	B	C
1.	Name of infringement	Smallest amount of fine (in HUF)	Largest amount of fine (in HUF)
2.	Failure to prepare the identification report	500,000	500,000
3.	Failure to review the identification report	300,000	600,000
4.	Failure to prepare the operator security plan	500,000	3,000,000
5.	Incomplete preparation of the operator security plan	100,000	500,000
6.	Failure to modify, review, send to the authority of the operator security plan	100,000	500,000
7.	Failure to employ a security liaison officer	500,000	500,000
8.	Failure to report an extraordinary occurrence	500,000	3,000,000
9.	Failure to comply with the relevant prescriptions in the decision of the designating authority, affecting the business continuity of the critical infrastructure	100,000	500,000
10.	Failure to report changes occurred in the data registered	100,000	100,000

[1] Added based on Government Decree 375/2020 (VII.30.) section 51d), Annex 5. Effective from 31.07.2020

11.	Failure to comply with the relevant prescriptions set out in the authority order	100,000	5,000,000
12.	Failure to hold a repeated complex exercise, or repeated non-adequate qualification at such	1,000,000	1,000,000
13.	Failure to modify the operator security plan, as a result of the finding of the complex exercise	500,000	500,000