DRAFT

ACT

of ….2014

on Cyber Security and Change of Related Acts (Act on Cyber Security)

The Parliament has resolved on the following Act of the Czech Republic:

PART ONE
CYBER SECURITY

CHAPTER I
GENERAL PROVISIONS

§ 1

Subject of the Act

(1) This Act regulates rights and obligations of natural and legal persons and power and competence of public authorities and their mutual cooperation in the field of cyber security.

(2) This Act shall not apply to information and communication systems handling classified information.

§ 2

Basic periods

For the purpose of this Act:

a) Cyber space means digital environment, enabling to create, process and exchange information, created by information systems and services and electronic communication networks[1],

b) Cyber security means a complex of legal, organizational, technical and educational means ensuring the protection of cyber space,

c) Critical information infrastructure means an element or system of elements of the critical infrastructure in the sector of communication and information systems[2] within the field of cyber security,

d) Security of information means ensuring confidentiality, integrity and availability of information,

e) Important information system means an information system administrated by a public authority, that is not critical information infrastructure and which may endanger or noticeably limit the performance of public administration in case of information security breach; Important information systems and their determinative criteria shall be set by the implementing legal regulation,

[1] Act No. 127/2005 Coll. on Electronic Communications and on Amendment to certain related Acts (Electronic Communications Act)

[2] §2 of the Act No. 240/2000 Coll. on Crisis Management (the Crisis Act), as amended by Act No. 320/2002 Coll. and Act No. 430/2010 Coll.

f) Administrator of information system means an entity, which determines the purpose of the information processing and conditions for the information system administration,

g) Administrator of the communication system means an entity, which determines the purpose of the communication system and conditions for its administration and

h) Important network means electronic communication network[1] providing direct international interconnection to public communication networks or providing direct connection to critical information infrastructure.

§ 3

Liable persons in the cyber security field

Liable persons in the cyber security field are as follows:

a) Electronic communication service provider and entity operating electronic communication network[1], unless set out in b),

b) Entity administrating important network, unless set out in d),

c) Administrator of critical information infrastructure information system,

d) Administrator of critical information infrastructure communication system and

e) Administrator of important information system.

CHAPTER II

SYSTEM TO ENSURE CYBER SECURITY

§ 4

System to ensure cyber security consists of security measures, cyber security incidents reporting, countermeasures, contact details notifications and activities of the National Security Authority (hereinafter referred to as "NSA") and supervisory units.

Security measures

§ 5

(1) Security measures mean a complex of activities and procedures, with the purpose of ensuring the security of information in information systems and availability and reliability of services and networks in cyber space.

(2) Liable persons set out in § 3 c) to e) shall implement security measures for critical information infrastructure information system, critical information infrastructure communication system or important information system and keep security measures record in security documentation.

§ 6

(1) Security measures are as follows

a) Organisational measures and

b) Technical measures.

(2) Organisational measures are particularly

a) Information security management system,

b) Risk management,

c) Security policy,

d) Organisational security,

e) Security requirements on suppliers setting,

f) Assets management,

g) Human resources security,

h) Critical information infrastructure or important information system operation and communication management,

i) Access of persons to critical information infrastructure or to important information system management,

j) Acquisitions, development and maintenance of critical information infrastructure and important information systems,

k) Cyber security events and cyber security incidents management,

l) Business continuity management and

m) Critical information infrastructure and important information systems control and audit.

(3) Technical measures are particularly

a) Physical security,

b) Communication networks integrity protection tools,

c) Users´ identity verification tools,

d) Access authorization management tools,

e) Counter malicious code protection tolls,

f) Critical information infrastructure and important information systems, their users and administrators activities recording tools,

g) Cyber security events detection tools,

h) Collection and evaluation of cyber security events tools,

i) Application security,

j) Cryptographic devices,

k) Tools for ensuring the levels of information availability and

l) Industrial and management systems security.

§ 7

Implementing legal regulation shall set out the following:

a) Security measures content,

b) Content, structure and form of security documentation and

c) Extent of security measures implementation for liable persons set out in § 3 c) to e).

Cyber security event and cyber security incident

§ 8

(1) Cyber security event means an event which may cause security of information breach in information systems or security of services or security and integrity of electronic communication networks breach[1].

(2) Cyber security incident means a cyber security event during which security of information in information systems breach or security of services or security and integrity of electronic communication networks[1] breach occurred.

(3) Liable persons set out in § 3 b) to e) are obliged to detect cyber security events in their important network, critical information infrastructure information system, critical information infrastructure communication system or important information system.

§ 9

Cyber security incident report

(1) Liable persons set out in § 3 b) to e) are obliged to report cyber security incidents in their important network, critical information infrastructure information system, critical information infrastructure communication system or important information system immediately after their detection; this shall not affect informational duty set out in other legal regulation[3].

(2) Liable persons set out in § 3 b) shall report cyber security incidents to the national supervisory unit (hereinafter referred to as „National CERT“).

(6) Liable persons set out in § 3 c) to e) shall report cyber security incidents to the NSA.

(3) Implementing legal regulation shall set out the following:

a) Cyber security incident's types and categories and
b) cyber security incident report's requirements and form.

Record keeping

§ 10

(1) The NSA keeps cyber security incidents record (hereinafter referred to as "incidents record") which contains:

a) Cyber security incident report,
b) Identification data of a system where the cyber security incident occurred,
c) Cyber security incident source data and
d) Cyber security incident solving procedure, its outcome and countermeasures adopted.
e) The data set out in § 22 e) to g) may make part of the incidents record.

[3] For example §98 paragraph 4 and §99 paragraph 4 of the Act No. 127/2005 Coll. , as amended by Act No. 153/2010 Coll. and Act No. 468/2011 Coll.

(7) The NSA provides incidents record data to the public authorities only for the purpose of fulfilling tasks within their authority.

(8) The NSA may provide incidents record data to the National CERT, to bodies performing authority in the field of cyber security abroad and to other entities acting in the field of cyber security in the extent necessary for ensuring protection of cyber space.

§ 11

(1) The NSA shall not provide incidents record data, if it enable identification of the liable person, which notified the cyber security incident; this shall not apply in case of proceeding according to § 10 paragraphs 3 or 4.

(2) The NSA may restrict incidents record data providing, if providing this data could endanger the force of countermeasures according to § 15 or 16; this shall not apply in case of proceeding according to § 10 paragraphs 3 or 4.

§ 12

(1) Employees of the NSA, taking part in solving cyber security incident, are bound by confidentiality about incidents record data. Confidentiality lasts even after the termination of the labour law relationship towards the NSA.

(2) The director of the NSA may waive incidents evidence data confidentiality of persons set out in paragraph 1, together with determination of the data and waiver extent.

Countermeasures

§ 13

(1) Countermeasures mean the acts of the NSA needed to protect information systems or services and electronic communication networks[1] from the threat in the cyber security field or from the cyber security incident or acts to solve already present cyber security incident.

(2) Countermeasures are as follows:

a) Warnings,
b) Reactive countermeasures and
c) Protective countermeasures.

(3) The following liable persons are obliged to carry out reactive countermeasures:

d) Liable persons set out in § 3 a) and b) under the state of cyber emergency or under the state of emergency[4] in cases set out in §24 paragraph 6 and
e) Liable persons set out in § 3 c) to e).

(4) Liable persons set out in § 3 c) to e) are obliged to carry out protective countermeasures.

[4] Constitutional Act of Law No. 110/1998 Coll., on the Security of the Czech Republic, as amended by Act No. 300/2000 Coll.

§ 14

Warning

(1) The NSA shall issue warning in case it finds out, particularly from its own action or on the initiative of the National CERT administrator or from foreign cyber security authorities, that the threat in the field of cyber security occurs.

(2) Warning shall be published by the NSA on the internet websites of the governmental supervisory unit (hereinafter referred to as „Governmental CERT“) and shall be notified to liable persons via contact details kept in the contact details evidence. A part of warning may be a recommendation on facing the threat in the field of cyber security.

§ 15

Reactive countermeasure

(1) The NSA shall issue reactive countermeasures in the form of a decision to solve cyber security incident and shall deliver it to the liable person. The decision is executory upon delivery. If it is not possible to deliver the decision into the hands of the addressee within 24 hours from its issuance, it is executory upon publishing on the NSA´s public noticeboard. The NSA may issue a decision on site5.

(2) Appeal against decision and decision issued on site is possible. Appeal has no suspensive effect.

(3) The NSA shall issue reactive countermeasures by a measure of general nature, which shall assign the method of information systems or networks and electronic communication services[1] securing from a cyber security incident.

(4) The liable person shall immediately inform the NSA about execution of the reactive countermeasure and its result. Terms of the notice shall be set out in implementing legal regulation.

(5) Implementing legal regulation shall set out examples of reactive countermeasures.

§ 16

Protective countermeasure

(1) The NSA shall issue protective countermeasure by measure of general nature on the basis of an already solved cyber security incident analysis in order to increase protection of information systems or services or electronic communication networks1.

(2) The NSA shall determine the method of increasing protection of information systems or services and electronic communication networks1 and deadline for its execution to liable persons set out in § 3 c) to e) by a measure of general nature.

[5] § 143 of the Administrative Procedure Code

§ 17

(1) Measures of general nature come into force upon publishing on the NSA´s public noticeboard, before proceeding in accordance with § 172 of the Administrative Procedure Code. Concurrently, measures of general nature shall be published on the internet websites of the Governmental CERT. Liable person shall be informed about the issuance of the measure of general nature via contact details.

(2) The comments to the measure of general nature issued according to paragraph 1 may be applied within 15 days upon its publishing on the NSA´s public noticeboard. The NSA may change or repeal the measure of general nature in line with applied comments.

Contact details

§ 18

(1) The contact details of a liable person mean:

a) As for legal person, the trading company or the name including differentiating amendment or other marking, address of the seat, identification number of the person or similar number assigned abroad,
b) As for natural person pursuing business, the trading company or the name including differentiating amendment or other marking, address of the place of pursuing business and identification number of a person,
a) As for public authority, its name, address of the seat, person registration number, if assigned and the public authority identificator, when the person registration number is not assigned,

and the natural person's data, who is authorized to act on behalf of the liable person in issues provided for by this Act, including name, surname, telephone number and electronic mail address.

(2) Contact details and their changes shall be announced by

a) Liable persons set out in § 3 a) and b) to the National CERT and
b) Liable persons set out in § 3 c) to e) to the NSA.
2

(3) Liable persons set out in § 3 c) and e) shall immediately announce changes only of the details set out in paragraph 1, which are not referential details kept in the basic registers.

(4) The NSA shall keep contact details evidence, which contains details set out in paragraph 1.

(5) The NSA is authorized to require contact details collected by the National CERT according to paragraph 2 a) under the state cyber emergency.

(6) Contact details notice template and its form shall be set out in the implementing legal regulation.

Supervisory units

§ 19

National CERT

(1) National CERT is a unit usually run by a private entity, which ensures information sharing on national and international level in the field of cyber security, particularly for private entities.

(2) National CERT shall

a) Accept the contact details notice from liable persons set out in § 3 a) and b), keep record of and store them,
b) Accept cyber security incidents reports from liable persons set out in § 3 b), keep record of, store and protect them,
c) Evaluate cyber security incidents as for liable persons set out in § 3 b),
d) Provide liable persons set out in § 3 a) and b) with methodical support and help,
e) Cooperate with liable persons set out in § 3 a) and b) when a cyber security incident occurs,
f) Act as point of contact for liable persons set out in § 3 a) and b),
g) Carry out vulnerability analysis in the cyber security field,
h) Transmit to the Governmental CERT the cyber security incident data without disclosing the announcer of the cyber security incident and
i) Under the state of cyber emergency and on NSA's request, transmits contact details of liable persons set out in § 3 a) and b).

(7) National CERT may perform also other activity in the field of cyber security, in case when such activity does not harm the duties fulfilment set out in paragraph 2.

(8) National CERT shall coordinate its activities with the NSA while fulfilling its duties set out in paragraph 2.

§ 20

National CERT administrator

(9) National CERT administrator shall be a legal person, who does not carry out activities against the interests of the Czech Republic and has never done so and

a) Who fulfils conditions set out in paragraph 2 and
b) Who was concluded a public-law contract with the NSA according to § 21.

(10) National CERT administrator shall only be a legal person who proves to

a) Have experience with information systems or services and electronic communication networks[1] administration,
b) Have technological and personnel background,
c) Take part in international cooperation with organisations operating in the field of cyber security abroad,
d) Have transparent proprietary structure,
e) Fulfil financial duties towards the state, natural and legal persons,
f) Have a clean criminal record.

(11) Relationship between the National CERT administrator and liable person shall not influence its impartiality while fulfilling duties set out in § 19 paragraph 2.

(12) The NSA shall publish the National CERT administrator´s data on the internet websites of the Governmental CERT.

§ 21

Public-law contract

(1) The NSA concludes a public-law contract (hereinafter referred to as „contract“) with a legal person chosen by the selection procedure in line with the Administrative Procedure Code in order to cooperate in the field of cyber security and ensure activities set out in § 19 paragraphs 1 and 2. The selection procedure shall be published by the NSA.

(2) The contract contains

a) Indication of contracting parties,
b) Definition of the subject of the contract,
c) Rights and obligations of the contracting parties,
d) Cooperation conditions of the contracting parties,
e) Terms and conditions of the parties´ withdrawal from the contract,
f) Notice period and notice reasons,
g) Ban on misuse of data acquired while performing activities set out in §19 paragraph 2,
h) Terms of National CERT activities financing and
i) Terms of handover and extent of data handed over to the NSA if the contract loses effect.

(3) The contract concluded according to paragraph 1 shall be published in the NSA´s Bulletin, except for the parts of the contract, whose publishing is not allowed by other legal regulation.

(4) If the contract is not concluded according to paragraph 1, or if the contract loses effect, the activity of the National CERT shall be fulfilled by the NSA.

§ 22

Governmental CERT

Governmental CERT, as a part of the National Centre of Cyber Security, is a unit of the NSA, which

a) Receives the contact details notice from liable persons set out in § 3 c) to e),
b) Receives cyber security incidents reports from liable persons set out in § 3 c) to e),
c) Evaluates cyber security events and cyber security incidents data from critical information infrastructure, from important information systems and from other information systems of the public administration,
d) Cooperates with liable persons set out in § 3 c) to e) during cyber security incidents and cyber security events,
e) Receives impulses and data from liable persons and from entities not set out in § 3, and analyses this impulses and data,
f) Receives data from the National CERT and analyses this data,

g) Receives data from bodies, performing authority in the field of cyber security abroad, and analyses this data,
h) Provides the National CERT, bodies performing authority in the field of cyber security abroad and other entities acting in the field of cyber security with incidents record data and
i) Performs vulnerability analysis in the field of cyber security.

§ 23

(1) This Act shall apply only to such information or communication systems of intelligence services, which fulfil conditions for critical information infrastructure determination, in the extent of § 14 and § 18; provisions of § 5 shall apply to these systems adequately and the NSA shall not suggest them as critical infrastructure elements set out in § 26 paragraph 2 n).

(2) This Act shall apply to the Police of the Czech Republic information system for analytical activity within criminal proceedings only in the extent of § 14 and § 18; provisions of § 5 shall apply to this system adequately. This shall not apply in case that this system is critical information infrastructure.

CHAPTER THREE

STATE OF CYBER EMERGENCY

§ 24

(1) State of cyber emergency means a state, during which information security in information systems or services or electronic communication networks[1] security is seriously endangered and the interests of the Czech Republic may thus be violated or endangered.

(2) State of cyber emergency shall be declared by the Prime Minister upon the NSA Director´s proposal. The decision of the state of cyber emergency declaration shall be announced in communication mass media. The provider of the television or radio broadcasting is obliged to announce the information on the state of cyber emergency declaration without cost reimbursement, on request of the NSA, without delay and with no content and meaning adjustment.

(3) State of cyber emergency declaration enters into force at the moment stipulated in the decision. The government of the Czech Republic shall authorize or cancel the state of cyber emergency decision within 24 hours. State of cyber emergency shall be declared for a necessary period of time, for a maximum of 7 days. The period given may be prolonged repeatedly only after the prior government´s authorization; total period of a declared state of cyber emergency shall not exceed 30 days.

(4) During the state of cyber emergency the NSA Director shall inform the Prime Minister about the procedure of the state of cyber emergency solving and about current state of threats, which led to the state of cyber emergency declaration. Under the state of cyber emergency and under the state of emergency[4] in cases set out in paragraph 6, the NSA is entitled to issue countermeasures according to §15 also to liable persons set out in §3 a) and b).

(5) State of cyber emergency shall not be declared in case when the threat to security of information in the information systems or security of services or security and integrity of electronic communication networks[1] threat may be averted by the Governmental CERT activities.

(6) If it is not possible to avert the threat to information security in information systems or to security of services or security and integrity of electronic communication networks[1] within the framework of the state of cyber emergency, the NSA Director shall promptly ask the government to declare state of emergency[4]. Countermeasures issued by the NSA before the state of emergency declaration remain effective as long as these countermeasures do not contradict emergency measures declared by the government.

(7) State of cyber emergency shall terminate after the given period, unless government decides to terminate it earlier or by declaration of state of emergency[4].

(8) Government resolution on approval of the declared state of cyber emergency, on extension of the state of cyber emergency or on cancellation of the state of cyber emergency before the given period, shall be published in the Collection of Law.

§ 25

(1) Cyber security commission is an advisory body of the NSA Director for prevention and solving the state of cyber emergency.

(2) The chairperson of the Cyber security commission is the NSA Director, who appoints its other members from the representatives of public authorities, representatives of public-law corporations and representatives of private-law entities active in the field of cyber security or in the field of electronic communications.

CHAPTER FOUR

STATE ADMINISTRATION PERFORMANCE

§ 26

(1) State administration performance in the field of cyber security is carried out by the NSA, unless otherwise stipulated by this Act or other legal regulation.

(2) The NSA, as the central administrative body:

a) Determines security measures,
b) Issues countermeasures,
c) Ensures the activities of the National Cyber Security Centre,
d) Keeps records according to this Act,
e) Controls fulfilment of duties set out by this Act,
f) Imposes fines for administrative offences according to this Act,
g) Acts like a coordination body during the state of cyber emergency,
h) Cooperates with public authorities, public-law corporations, research and development units and other supervisory units,

i) Coordinates international cooperation in association with the Ministry of Foreign Affairs,
j) Negotiates and concludes agreements on international cooperation in association with the Ministry of Foreign Affairs,
k) Ensures prevention, education and methodical support/activity in the field of cyber security,
l) Ensures research and development in the field of cyber security,
m) Concludes public-law contract with the National CERT administrator,
n) According to Emergency law, it sends to the Ministry of Interior proposals of critical infrastructure elements in the area of communication and information systems in the field of cyber security, the administrator of which is an organisational state body,
o) Determines elements of critical infrastructure in the area of communication and information systems in the field of cyber security according to Emergency law, except elements set out in n) and
p) Fulfils other tasks in the field of cyber security set out by this Act.

(3) The Ministry of Interior controls the fulfilment of duties set out in § 5 paragraph 2 by liable persons set out in § 3 e).

CHAPTER FIVE

CONTROL, SUPERVISION AND ADMINISTRATIVE OFFENCES

Control

§ 27

(1) The NSA shall perform control in the field of cyber security. While performing control, the NSA determines how liable persons fulfil duties set by this Act, legal regulations, decisions and measures of general nature issued by the NSA and how they respect the implementing legal regulations. The control in the field of cyber security is further performed by the Ministry of Interior, according to paragraph 4.

(2) The control shall be performed according to the controlling rules[6], unless otherwise stipulated by this Act.

(3) The NSA controls

a) Liable persons set out in § 3 a) and b), whether they fulfil duties set out by countermeasures issued according to § 15 under the state of cyber emergency,
b) Liable persons set out in § 3 c) and d), whether they fulfil duties set out in § 5 paragraph 2, § 9 paragraph 3, countermeasure issued according to §15 or 16 and §18 paragraph 2 b) and
c) Liable persons set out in § 3 e), whether they fulfil duties set out in § 9 paragraph 3, countermeasure issued according to § 15 or 16 and § 18 paragraph 2 b).

(4) The Ministry of Interior controls liable persons set out in § 3 e), whether they fulfil duties set out in § 5 paragraph 2.

[6] Act No. 255/2012 Coll., on Inspection (Inspection order).

§ 28

Corrective measures

(1) In case the controlling body ascertains any deficiencies during control performed according to § 27, it assigns the liable person to rectify ascertained deficiencies in a specified period of time and possibly determines, what measures to eliminate deficiencies has this liable person to accept.

(2) In case the critical information infrastructure information system, critical information infrastructure communication system or important information system is immediately endangered by cyber security incident, which can significantly damage or destroy it, because of ascertained deficiencies, the controlling body may prohibit the liable person from using this system or its parts until the ascertained deficiency will be eliminated.

(3) While issuing corrective measures, the NSA shall take account of all measures of the given case and the corrective measure issued shall be adequate to pursued purpose and possible consequences. Costs bound to the implementation of corrective measures shall be covered by the liable person.

Administrative offences of legal entities and natural entities pursuing business

§ 29

(1) Liable person set out in § 3 a) or b) commits administrative offence in the following cases:

a) Does not implement countermeasures issued by the NSA according to § 15 under the state of cyber emergency or

b) Does not fulfil some of the obligations imposed by the corrective measure according to § 28.

(2) Liable person set out in § 3 c) to e) commits administrative offence in the following cases:

d) Does not implement security measures contrary to § 5 paragraph 2 or does not keep security measures record,
e) Does not notify cyber security incident to the NSA according to § 9 paragraph 3,
f) Does not implement countermeasures issued by the NSA according to § 15 or § 16,
g) Does not notify contact details or their changes to the NSA according § 18 paragraph 2 b) or
h) Does not fulfil some of the obligations imposed by the corrective measure according to § 28.

(3) The penalty in case of administrative offence reaches up to:

a) 100 000 CZK in case of administrative offence set out in paragraph 1 a), b) or paragraph 2 a) to c) or e),.

b) 10 000 CZK in case of administrative offence set out in paragraph 2 d).

§ 30

(1) Legal entity is not responsible for the administrative offence in case it can prove making every effort that was possible to demand, to prevent the breach of the legal obligation.

(2) The responsibility of a legal entity for an administrative offence ceases to exist if the NSA has not launched the proceedings within 1 year from the day, when such an offence was discovered. The responsibility ceases to exist within 3 years from the day, when the administrative offence was committed.

(3) While determining the penalty assessment of a legal entity, the gravity of the administrative offence shall be taken into account, especially the way of its committing and its consequences and circumstances of its committing.

(4) Administrative offences set out by this Act shall be debated by the NSA.

(5) Responsibility for actions during the individual´s entrepreneurship or in direct connection to it is regulated by the responsibilities and legal entity´s penalty provisions of this Act.

(6) The penalties shall be collected by the NSA. The penalties´ income shall be public revenue.

(7) The penalty is due 30 days from the day of entering into force of the decision of its imposition.

CHAPTER SIX
FINAL PROVISIONS

§ 31

Enabling provisions

(1) The NSA and the Ministry of Interior shall stipulate important information systems and their determinative criteria according to §2 e) by the implementing legal regulation.

(2) The NSA shall stipulate by the implementing legal regulation the following:

a) Content, structure and form of the security documentation, extent of security measures and extent of implementation of security measures according to §7,

b) Types and categories of cyber security incidents and requirements and form of cyber security incident report according to §9 paragraph 4,

c) Requirements on implementation and result of a reactive countermeasure notice according to § 15 paragraph 4,

d) Examples of reactive countermeasures according to § 15 paragraph 5 and

e) Contact details notice template and its form according to §18 paragraph 6.

Transitional provisions
§ 32

(1) Liable persons set out in § 3 a) and b) are obliged to notify contact details according to § 18 within 30 days from entering into force of this Act.

(2) Liable persons set out in § 3 b) are obliged to implement cyber security incident notice according to §9 paragraph 3 within 1 year from entering into force of this Act at the latest.

§ 33

Liable persons set out in § 3 c) to d) are obliged to

a) Notify contact details according to § 18 within 30 days from the day of determination of their information system or communication system as critical information infrastructure,

b) Implement cyber security incident notice according to § 9 paragraph 3 within 1 year from the day of determination of their information system or communication system as critical information infrastructure at the latest and

c) Implement security measures according to § 5 paragraph 2 within 1 year from the day of determination of their information system or communication system as critical information infrastructure.

§ 34

Liable persons set out in § 3 e) are obliged to

a) Notify contact details according to § 18 within 30 days from the day of fulfilment of determinative criteria of the important information system,

b) Implement cyber security incident notice according to § 9 paragraph 3 within 1 year from the day of fulfilment of determinative criteria of the important information system at the latest and

c) Implement security measures according to § 5 paragraph 2 within 1 year from the day of fulfilment of determinative criteria of the important information system.

§ 35

The activity of the National CERT shall be performed, until the time when a public-law contract concluded according to § 21 comes into force, by the entity, which concluded a cooperation contract with the NSA before this Act entered into force, for no longer than 2 years from the day of entering into force of this Act.

PART TWO

Change of the Act on the Protection of Classified Information and Security Eligibility

§ 36

Act No. 412/2005 Coll., on Protection of Classified Information and Security Eligibility, as amended by Act No. 119/2007 Coll., Act No. 177/2007 Coll., Act No.

296/2007 Coll., Act No. 32/2008 Coll., Act No. 124/2008 Coll., Act No. 126/2008 Coll., Act No. 250/2008 Coll., Act No. 41/2009 Coll., Act No. 227/2009 Coll., Act No. 281/2009 Coll., Act No. 255/2011 Coll., Act No. 420/2011 Coll., Act No. 458/2011 Coll. and Act No. 167/2012 Coll., will change in the following way:

1. In § 145 at the end of paragraph 5, a full stop shall be replaced by a comma and letter f) shall be added:

„f) on request notice about respective cyber security incidents from critical information infrastructure."

2. In § 146 paragraph 1, the wording "or within the administrative procedure on issuance of countermeasures according to the Act on Cyber Security" shall be inserted behind the wording "security procedure".

3. In § 146 paragraph 2, the wording "or according to the Act on Cyber Security" shall be inserted behind the wording "according to this Act".

PART THREE

Change of the Electronic Communications Act

§ 37

Act No. 127/2005 Coll., on Electronic Communications and on Amendment to certain related Acts (the Electronic Communications Act), as amended by Act No. 290/2005 Coll., Act No. 361/2005 Coll., Act No. 186/2006 Coll., Act No. 235/2006 Coll., Act No. 310/2006 Coll., Act No. 110/2007 Coll., Act No. 261/2007 Coll., Act No. 304/2007 Coll., Act No. 124/2008 Coll., Act No. 177/2008 Coll., Act No. 189/2008 Coll., Act No. 247/2008 Coll., Act No. 384/2008 Coll., Act No. 227/2009 Coll., Act No. 281/2009 Coll., Act No. 153/2010 Coll., Constitutional Court judgement promulgated under No. 94/2011 Coll., Act No. 137/2011 Coll., Act No. 341/2011 Coll., Act No. 375/2011 Coll., Act No. 420/2011 Coll., Act No. 457/2011 Coll., Act No. 458/2011 Coll., Act No. 468/2011 Coll., Act No. 18/2012 Coll., Act No. 19/2012 Coll., Act No. 142/2012 Coll., Act No. 167/2012 Coll. and Act No. 273/2012 Coll. will change in the following way:

1. In § 89 paragraph 4 shall be added, including footnote No. 62:

„(4) Entrepreneur administrating a public communication network or providing publicly accessible electronic communications service is obliged, on the participant´s request free of charge and in the form enabling further electronic data processing, to provide operational and localization data, available on the basis of this Act, in case when the participant was not able to collect or save them because of his/her device failure in consequence of a cyber security incident[62)]. The entrepreneur shall transmit the data, if technically possible, immediately, however, at the latest within 3 days from the day of the delivery of the request or in the case of an ongoing communication from the day of its realization.

62) § 8 paragraph 2 of the Act No. …/2014 Coll., on Cyber Security and on Amendment to related Acts (Act on Cyber Security).”.

2. In § 118 paragraph 14 letter y) the word “or” shall be cancelled.

3. In § 118 at the end of paragraph 14, a full stop shall be replaced by the word “or” and letter aa) shall be added:

„aa) contrary to § 89 paragraph 4 does not provide data or provides them late.”.

4. In § 118 paragraph 22 letter a), the word “or” shall be replaced by a comma and at the end of the text of the letter the wording “or of the paragraph 14 letter aa)”shall be added.

PART FOUR

ENTERING INTO FORCE

§ 38

This Act shall enter into force on 1 January 2015.