unofficial translation

THE CABINET OF MINISTERS OF UKRAINE
RESOLUTION

No. 943 of 9 October 2020
Kyiv

Some issues involving critical information infrastructure facilities

In accordance with the first indent of Article 4(3) of the Law of Ukraine "On the Key Principles of Ensuring Cyber Security of Ukraine", the Cabinet of Ministers of Ukraine hereby **resolves**:

1. That the following acts attached hereto be approved:

The Procedure for formation of a list of critical information infrastructure facilities;

The Procedure for placing critical information infrastructure facilities on the state register of critical information infrastructure facilities, its formation and maintenance.

2. That the Administration of the State Service of Special Communication and Information Protection of Ukraine:

form a list of critical information infrastructure facilities and submit it to the Cabinet of Ministers of Ukraine under the established procedure;

establish the state register of critical information infrastructure facilities and maintain it;

set a form for entering data in the state register of critical information infrastructure facilities.

3. That the ministries and other executive authorities, within six months, form sectoral lists of critical information infrastructure facilities under their management and ensure their maintaining and submission of information on critical information infrastructure facilities to the Administration of the State Service of Special Communication and Information Protection of Ukraine.

4. That the Resolution of the Cabinet of Ministers of Ukraine No. 563 of 23 August 2016 "On approval of the Procedure for formation of the list of information telecommunication systems of the State's critical information infrastructure facilities (Official Bulletin of Ukraine, 2016, No. 69, p. 2332) be repealed.

Prime Minister of Ukraine **D.SHMYHAL**

Ind. 49

APPROVED
by the Resolution of the Cabinet of Ministers of Ukraine
No. 943 of 9 October 2020

PROCEDURE
for formation of a list of critical information infrastructure facilities

1. This Procedure shall set up the mechanism of formation of the national and sectoral lists of critical information infrastructure facilities.

2. The terms used herein shall have the following meanings:

critical infrastructure facility's security shall be the state of a critical infrastructure facility's security ensuring its functionality and operational continuity and/or enabling provision of core services by that facility;

critical infrastructure facility's owner and/or manager (hereinafter — "the core service operator") shall be a public authority, enterprise, institution, organization of any form of ownership, a legal entity and/or a natural person to whom belongs a critical infrastructure facility by right of ownership, or on the rental basis, or on any other legal grounds, or who/which is responsible for its current functioning;

vital services and functions (hereinafter — "core services") shall be the services provided, and functions performed by the core service operators, failures and disruptions in provision/performance of which may result in adverse effects for public, society, social and economic situation and national security and defense of Ukraine;

protection of the critical information infrastructure facilities shall mean organizational, legal and normative, engineering and technical and other action aiming at ensuring security of the critical information infrastructure facilities;

identification of a critical information infrastructure facility shall mean the Procedure for designation of a critical information infrastructure facility as the critical information infrastructure facility;

critical information infrastructure shall mean a totality of critical information infrastructure facilities;

sector (sub-sector) of critical infrastructure shall mean a totality of critical infrastructure facilities belonging to the same sector/sub-sector of economy and/or having common functional use;

designated public authority responsible for a sector/sub-sector of critical infrastructure (hereinafter — "designated authority") shall be a central executive authority or other public authority ensuring development and/or implementation of the state policy in one or more areas.

Other terms shall be used in the meanings as set out in the Laws of Ukraine "On Information", "On Telecommunications", "On Protection of Information in Automated Systems" and "On the Key Principles of Ensuring Cyber Security of Ukraine".

3. The core service operator shall conduct identification of the critical information infrastructure facilities which support a critical infrastructure facility's operation and ensure provision of core services by it.

4. Identification of critical information infrastructure facilities shall follow the procedure set out below:

a core service operator shall establish all information infrastructure facilities (automated, information, telecommunication, information and telecommunication systems, automated process control systems) operated within the critical infrastructure facility;

a core service operator shall decide which of the above information infrastructure facilities are necessary for ensuring continuous and sustainable functioning of a critical infrastructure facility in the terms of core services it provides, and then, it shall carry out their criticality assessment.

5. To carry out criticality assessment of an information infrastructure facility, the core service operator shall apply the following three criteria:

critical infrastructure facility's importance both for sustainable and continuous functioning of a critical infrastructure facility and for its provision of core services;

cyber attack, cyber incident, incident affecting information security at a critical infrastructure facility, having the significant influence on continuity and sustainability of core services provided by a critical infrastructure facility;

where continuity and sustainability of core services provided by a critical infrastructure facility is disrupted, there is no alternate facility (method) of provision thereof.

Information infrastructure facilities meeting all three criteria shall be designated by a core service operator as the critical information infrastructure facilities. At the same time, criticality category into which a critical information infrastructure facility falls shall be established based on the criticality category of the critical infrastructure facility.

6. A core service operator shall, within 30 days from designation of a critical information infrastructure facility, submit information on the critical information infrastructure facilities to a designated authority which shall form a sectoral list of the critical information infrastructure facilities on the basis thereof. The information in accordance with the form contained in annex shall be submitted in a paper and/or electronic format. A qualified electronic signature of a critical infrastructure facility's manager or of an authorized signatory shall be added to the information in electronic form, and such information shall be dispatched written on an electronic data medium.

Information on the critical information infrastructure facilities of I, II, III and IV criticality categories shall be added to the sectoral list.

7. A core service operator shall take measures to update information on the critical information infrastructure facilities contained in the sectoral list of the critical information infrastructure facilities within ten business days from changes that have taken place, in case of:

changes in information indicated in annex;

creation, upgrade or decommissioning of a critical information infrastructure facility.

8. The designated authority shall review the submitted information on the critical information infrastructure facilities and shall, where necessary, provide commentaries and recommendations as regards accuracy and/or fullness of information provided, and shall also have the right to request from the core service operator the information on the provided data as indicated in annex.

9. The designated authority shall, based on the data on the critical information infrastructure facilities in its ownership or disposal, and on the information received from the core service operators within the sector/sub-sector under its supervision, form and keep a sectoral list of the critical information infrastructure facilities.

10. The designated authority shall update the sectoral list of the critical information infrastructure facilities every two years or within one month from changes in data as indicated in annex that took place as regards critical information infrastructure within the sector/sub-sector under its supervision.

11. The designated authority shall submit the data on criticality category I and II critical information infrastructure facilities within the sector/sub-sector of critical infrastructure under its

supervision to the Administration of the SSSCIP in a paper or an electronic format, in accordance with annex, and shall take measures to update the data on the facilities within the sector/sub-sector under its supervision, contained in the national list, in case of:

changes in information indicated in annex;

creation, upgrade or decommissioning of a criticality category I and II facility.

12. The designated authority shall, within 10 business days from placing a critical information infrastructure facility on a sectoral list, notify the core service operator to that effect to enable the latter to enter data on a critical information infrastructure facility in a critical infrastructure facility's ID.

13. The Administration of SSSCIP shall, based on the data from the sectoral lists of the critical information infrastructure facilities received from the designated authorities in their respective sectors/sub-sectors of the State's critical infrastructure, form and keep the national list of the critical information infrastructure facilities. Information on the critical information infrastructure facilities of I and II criticality categories shall be added to the national list.

14. The Administration of SSSCIP shall review the submitted information on the critical information infrastructure facilities and shall, where necessary, provide commentaries and recommendations as regards accuracy and/or fullness of information provided, and shall also have the right to request, from the designated authority or from core service operators, the information on the provided data as indicated in annex.

15. A critical infrastructure facility's owner included in the national list shall take priority measures to protect such facility from cyber attacks.

16. Information on the critical information infrastructure facilities included in the national list shall be entered in the state register of the critical information infrastructure facilities.

17. Information on the critical information infrastructure facilities contained in the national list and the sectoral lists of the critical information infrastructure facilities shall be restricted information whose protection shall be secured in accordance with the requirements of information security legislation.

Annex
to the Procedure for formation of a list of
critical information infrastructure facilities

INFORMATION
on a critical information infrastructure facility

_____

(facility name)

to be entered in the sectoral/national list of the critical information infrastructure facilities

Necessary information	Information provided	Note
Full name of a legal entity in whose ownership/disposal is a critical information infrastructure facility, address of a legal entity, USREOU code, form of ownership,		

manager's surname, first name and patronymic (if available)

Full name of a critical infrastructure facility a critical information infrastructure facility is part of, its function, sector or sub-sector it is part of, list of core services it provides, criticality category

Full name of a critical information infrastructure facility, its function, list of core services whose provision it supports, criticality category

Type of information in terms of access, which is processed or is planned to be processed at a critical information infrastructure facility

Physical location of a critical information infrastructure facility

Availability of a critical information infrastructure facility's connection to Internet, other information telecommunication systems not being part thereof, and IP address range used

Full name of the telecommunication provider legal entity/legal entities which provides/provide Internet access services to a critical information infrastructure facility, address of the legal entity/legal entities

Existence of interaction between a critical information infrastructure facility and other critical information infrastructure facilities and/or dependence of functioning of a critical information infrastructure facility on other such facilities

Availability of a certificate of compliance of a comprehensive system of the critical information infrastructure facility's information security or of the results of independent audit of a critical information infrastructure facility's information security

Persons and/or a subdivision, responsible for protection of information (ensuring information security) and cyber protection of a critical information infrastructure facility, including those charged with the duty of

information security service (surname, first name, patronymic (if available), telephone, e-mail)

_____ (name of a position of a manager of the critical infrastructure facility —in accordance with paragraphs 6 and 7 of the Procedure for placing critical information infrastructure facilities on the state register of critical information infrastructure facilities, its formation and maintenance name of a position of a head of the designated authority in a sector (sub-sector) of critical infrastructure —in accordance with paragraph 11 to the Procedure for formation of a list of the information infrastructure facilities)	_____ (signature)	_____ (surname, first name, patronymic (if available)
___ _____ 20__		

APPROVED
by the Resolution of the Cabinet of Ministers of Ukraine
No. 943 of 9 October 2020

PROCEDURE
for placing critical information infrastructure facilities on the state register of critical information infrastructure facilities, its formation and maintenance.

1. This Procedure establishes a mechanism for placing critical information infrastructure facilities on the state register of critical information infrastructure facilities (hereinafter — "the register"), its formation and maintenance.

2. The terms used herein shall have the following meanings:

critical infrastructure facility's security shall be the state of a critical infrastructure facility's security ensuring its functionality and operational continuity and/or enabling provision of core services by that facility;

critical infrastructure facility's owner and/or manager (hereinafter — "the core service operator") shall be a public authority, enterprise, institution, organization of any form of ownership, a legal entity and/or a natural person to whom belongs a critical infrastructure facility by right of ownership, or on the rental basis, or on any other legal grounds, or who/which is responsible for its current functioning;

vital services and functions (hereinafter — "core services") shall be the services provided, and functions performed by the core service operators, failures and disruptions in provision/performance of which may result in adverse effects for public, society, social and economic situation and national security and defense of Ukraine;

protection of the critical information infrastructure facilities — organizational, legal and normative, engineering and technical and other action aiming at ensuring security of the critical information infrastructure facilities;

identification of a critical information infrastructure facility shall mean the Procedure for designation of a critical information infrastructure facility as the critical information infrastructure facility;

critical information infrastructure shall mean a totality of critical information infrastructure facilities;

sector (sub-sector) of critical infrastructure shall mean a totality of critical infrastructure facilities belonging to the same sector/sub-sector of economy and/or having common functional use;

designated public authority responsible for a sector/sub-sector of critical infrastructure (hereinafter — "designated authority") shall be a central executive authority or other public authority ensuring development and/or implementation of the state policy in one or more areas.

Other terms shall be used in the meanings as set out in the Laws of Ukraine "On Information", "On Telecommunications", "On Protection of Information in Automated Systems" and "On the Key Principles of Ensuring Cyber Security of Ukraine".

3. The register shall be formed with a view to keeping records of the critical information infrastructure facilities part of I and II criticality category critical infrastructure facilities.

4. The register is an information telecommunication system processing and storing information on the critical information infrastructure facilities part of I and II criticality category critical infrastructure facilities (hereinafter — "data in the register").

5. The Administration of SSSCIP shall be the administrator of the information telecommunication system and holder of information (data) contained in the register, and the Administration of SSSCIP shall:

take measures with a view to creation and management of the register;

establish organizational and methodological principles of the register's functioning, and also, maintain it;

establish the procedure for, and forms of, submission of the data to the register, and also, determine arrangements for the access to the data in the register;

ensure formation and update of the register on the basis on the data received;

ensure protection of the data in the register in accordance with the requirements of legislation on information security and state secrets;

take other measures aiming at maintaining the register.

6. The data submitted to the register shall contain the following information:

full name of a legal entity in whose ownership/disposal is a critical information infrastructure facility, address of a legal entity, USREOU code, form of ownership, manager's surname, first name and patronymic (if available)

full name of a critical infrastructure facility a critical information infrastructure facility is part of, its function, sector or sub-sector it belongs to, list of core services it provides, criticality category;

full name of a critical information infrastructure facility, its function, list of core services whose provision it supports, criticality category;

designated authority in the sector (sub-sector) of critical infrastructure a critical infrastructure facility is part of;

type of information in terms of access, which is processed or is planned to be processed at a critical information infrastructure facility;

physical location of a critical information infrastructure facility;

availability of a critical information infrastructure facility's connection to Internet, other information telecommunication systems not being part thereof, and IP address range used;

full name of the telecommunication provider legal entity/legal entities which provides/provide Internet access services to a critical information infrastructure facility, address of the legal entity/legal entities;

existence of interaction between a critical information infrastructure facility and other critical information infrastructure facilities and/or dependence of functioning of a critical information infrastructure facility on other such facilities;

availability of a certificate of compliance of a comprehensive system of the critical information infrastructure facility's information security or of the results of independent audit of a critical infrastructure facility's information security;

persons and/or a subdivision, responsible for protection of information (ensuring information security) and cyber protection of a critical information infrastructure facility, including those charged with the duty of information security service;

the information of compliance with the General requirements to cyber protection of critical infrastructure facilities as approved by the Resolution of the Cabinet of Ministers of Ukraine No. 518 of 19 June 2019 (Official Bulletin of Ukraine, 2019, No. 50, p. 1697) by the critical information infrastructure facility.

7. Data for the register shall be submitted by the core service operators to the Administration of SSSCIP in an electronic format, with a qualified electronic signature of a critical infrastructure facility's manager or of an authorized signatory attached thereto; those dispatched written on an electronic data medium.

The data shall be submitted to the register once a year (actual as on 31 December of the previous year) till 1 February of a current year, in the format as stipulated by the Administration of SSSCIP, or within one month — in case of changes in the data on a critical information infrastructure facility as set out in paragraph 6 hereof, or putting of a new critical information infrastructure facility into operation, or decommissioning of the old one.

Information on the critical information infrastructure facilities of I and II criticality categories referred to in the national list of the critical information infrastructure facilities shall be submitted to the register.

8. Data in the register shall be restricted information whose protection shall be secured in accordance with the requirements of legislation on information security and state secrets.

9. Access to the register shall be granted to external authorized users subject to the presence of statutory grounds and in compliance with the requirements of legislation on information security and state secrets.

10. Access to the register shall be granted to a designated authority, upon the latter's written request within the area of its management.