GOVERNMENT

3940

Pursuant to Article 8, Paragraph 5 of the Law on Information Security ("Official Gazette of RS", issue No. 6/16) and Article 42, Paragraph 1 of the Law on Government ("Official Gazette of RS", issue No. 55/05, 71/05 – correction, 101/07, 65/08, 16/11, 68/12 – US, 72/12, 7/14 – US and 44/14), the Government hereby enacts the

REGULATION
on More Detailed Contents of Enactment on Security of Information and Communication Systems of Special Significance, the Manner of Testing and Contents of Report on Testing Security of Information and Communication Systems of Special Significance

Subject of the regulation
Article 1

This regulation shall regulate more detailed contents of the enactment on security of information and communication systems of special significance, the manner of testing information and communication systems of special significance and the contents of the report on testing the information and communication systems of special significance.

Enactment on Security of ICT Systems of Special Significance
Article 2

The operator of an ICT system of special significance (hereinafter referred to as: ICT system operator) shall be under obligation to adopt an enactment on security of the ICT system of special significance (hereinafter referred to as: enactment on security) which must be harmonized with the Law and this Decree.

Contents of the Enactment on Security
Article 3

The enactment on security, pursuant to the Law, shall regulate the protective measures, principles, the manner and procedures for achieving and maintaining an adequate level of security of the system, as well as the authorities and responsibilities in relation to security and resources of the ICT system of special significance (hereinafter referred to as: ICT system).

If individual issues referred to in Paragraph 1 of this Article are regulated under other enactments of the ICT system operator, the enactment on security should contain provisions referring to those enactments.

Protective Measures
Article 4

The protective measures regulated under the enactment on security must be harmonized with protective measures regulated under Article 7 of the Law on Information Security and the enactment of the Government that regulates the protective measures in more detail (hereinafter referred to as: Decree on Measures of Protection).

Descriptions of protective measures within the enactment on security should be grouped in 28 sections in accordance with the titles and the sequence of points in Article 7, Paragraph 3 of the Law on Information Security.

Each section referred to in Paragraph 2 of this Article shall contain a description of protective measures, including procedures, authorities and responsibilities of participants in the implementation of measures, and if those descriptions are contained in other enactments of the ICT system operator, provisions referring to those enactments shall be provided.

If any of the conditions under Article 7, Paragraph 3 of the Law on Information Security is impossible to apply or the risk analysis has shown that for a specific condition it is not necessary to apply it in full scope, that needs to be explained in the enactment on security.

Amendments to Enactment on Security

Article 5

Enactment on Security must be harmonized with changes in the environment and within the ICT system itself.

Changes in the environment and in the ICT system itself are those changes that can lead to increased exposure of the ICT system to security risks, due to onset of technical and technological, staff related, organizational changes in the ICT system and events at the global and national level that may disrupt information security, as well as those changes that create opportunities for improvement of protective measures.

In case of the changes referred to in Paragraph 2 of this Article, if necessary, amendments to the Enactment on Security shall be performed, i.e. adjustments and improvement of protective measures, manner and procedure for achieving and maintaining an adequate level of security of the ICT system, as well as re-examination of authorities and responsibilities in connection with security and resources of the ICT system.

ICT System Testing

Article 6

The ICT system operator shall be under obligation to perform the testing of the ICT system, i.e. the check of harmonization of protective measures being applied with the Enactment on Security, protective measures prescribed under the Law on Information Security and Decree on Measures of Protection.

The testing can be performed independently or upon engagement of external experts.

The testing shall access the adequacy of the level of information security through checking the protective measures, procedures and responsibilities stipulated under the enactment on security.

The testing shall determine any threat or disruption to information security which has onset in the use of inadequate procedures and technical means.

The ICT system operator shall be under obligation to perform the testing once a year at least and to compile a report on that.

The testing shall be performed in such a manner that:

1) harmonization of the Enactment on Security of the ICT system shall be tested, taking into account also the enactments referred to, with the prescribed conditions, i.e. it shall be tested whether the Enactment adequately envisages protective measures, procedures, authorities and responsibilities in the ICT system;

2) it shall be tested whether, in operational work, the envisaged protective measures and procedures are being adequately applied in compliance with specified authorities and responsibilities, using methods of interviews, simulation, observations, insight into envisaged records and other documentation;
3) testing shall be performed of the security weaknesses at the level of technical characteristics of components of the ICT system, using the method of insight into selected products, architectures of solutions, technical configurations, technical data on statuses, records on events (logs) as well as the method of testing for the presence of known security weaknesses in similar environments.

Contents of Reports on ICT System Testing

Article 7

The report on ICT system testing shall contain the following:

1) name of the operator of the ICT system which is being tested;
2) time of testing;
3) data on persons who had performed the testing;
4) report on actions of testing that were implemented;
5) conclusion concerning the issue of harmonization of the Enactment on Security of the ICT system with prescribed conditions;
6) conclusions concerning the issue of adequate application of envisaged protective measures in operating work;
7) conclusions concerning the issue of potential security weaknesses at the level of technical characteristics of ICT system components;
8) assessment of the overall level of information security;
9) signature of the responsible person who had implemented the ICT system testing.

Transitional Provision

Article 8

Enactment on Security shall be adopted within the deadline of 90 days from the date of entry into effect of this Decree.

Final Provision

Article 9

This Decree shall enter into effect on the eighth day from the date of its publication in the "Official Gazette of the Republic of Serbia".

05 number 110-9465/2016-2
In Belgrade, November 17, 2016
Government
President
Aleksandar Vucic, in person