GOVERNMENT OF THE REPUBLIC OF LITHUANIA

RESOLUTION NO 796

of 29 June 2011

ON THE APPROVAL OF THE PROGRAMME FOR THE DEVELOPMENT OF ELECTRONIC INFORMATION SECURITY (CYBER-SECURITY) FOR 2011–2019

Vilnius

For the purpose of implementing Measure No 65 of table 3 of the Implementation Measures of the Programme of the Government of the Republic of Lithuania for 2008–2012, approved by Resolution No 189 of the Government of the Republic of Lithuania of 25 February 2009 (*Valstybės žinios* (Official Gazette) No 33-1268, 2009, the Government of the Republic of Lithuania has r e s o l v e d:

1. To approve the Programme for the Development of Electronic Information Security (Cyber-Security) for 2011–2019 (as appended).

2. To propose that the State Security Department of the Republic of Lithuania and the Communications Regulatory Authority of the Republic of Lithuania participate in the implementation of the Programme for the Development of Electronic Information Security (Cyber-Security) for 2011–2019.

Prime Minister Andrius Kubilius

Minister of Justice acting as
Minister of the Interior Remigijus Šimašius

APPROVED by
Resolution No 796 of the Government of
the Republic of Lithuania
of 29 June 2011

THE PROGRAMME FOR THE DEVELOPMENT OF ELECTRONIC INFORMATION SECURITY (CYBER-SECURITY) FOR 2011–2019

I. GENERAL PROVISIONS

1. The Programme for the Development of Electronic Information Security (Cyber-Security) for 2011–2019 has been developed considering the increasing significance of electronic information, processed and transmitted by means of information and communication technologies, and also considering the fact that the newly emerged possibilities of electronic information processing fostered the development of national and global information societies and facilitated further modernization of national economies as well as led to more efficient public administration, while at the same time, with more and more information being converted into electronic format and various public administration and economic processes being automated, the global cyberspace and the public services delivered online have become an attractive target for individuals, criminal groups, political forces and other subjects.

2. The purpose of the Programme is to determine the objectives and tasks for the development of electronic information in order to ensure the confidentiality, integrity and accessibility of electronic information and services provided in cyberspace, safeguarding of electronic communication networks, information systems and critical information infrastructure against incidents and cyber attacks, protection of personal data and privacy, as well as to set the tasks, implementation of which would allow total security of cyberspace and entities operating in this medium.

3. The strategic objective of the Programme is the development of the security of electronic information in Lithuania, ensuring cyber security in order to achieve, in the year 2019, a 98 per cent level of compliance of state-owned information resources with legislative requirements on electronic information security (cyber security), reduction to 0.5 hour of the average time of response to critical information infrastructure incidents and a 60 per cent level of the Lithuanian residents who feel secure in cyberspace.

4. The terms used in the Programme shall have the following meaning:

Information resources shall mean an aggregate of information which is managed by members of the information society and processed by means of information technology as well as the information technology means used to process the said information.

Incident shall mean an event, act or omission which gives rise or may give rise to an unauthorized access to an information system or electronic communications network, disruption or change of the operation (including takeover of control) of an information system

or electronic communications network, destruction, damage, deletion or the change of electronic information, removal or limiting of the possibility to use electronic information and, also, which gives rise or may give rise to the appropriation, publication, dissemination or any other use of non-public electronic information by persons unauthorized to do so.

Critical information infrastructure shall mean an electronic communications network, information system or a group of information systems where an incident that occurs causes or may cause grave damage to national security, national economy or social well-being.

5. The Programme complies with the action steps presented in the Communication of the European Commission of 30 March 2009 "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" – COM(2009)149.

II. OBJECTIVES, TASKS, ASSESSMENT CRITERIA AND THEIR INDICATORS

6. For the purpose of Programme implementation the following objectives shall be established:

6.1. To ensure the security of state-owned information resources.

This objective is being addressed, since no system for coordination of the management of electronic information security has yet been created, except in the public sector (i.e. in the institutions accountable to the Government of the Republic of Lithuania). The Ministry of the Interior has no power to exercise a proper control and coordination for ensuring the security of electronic information (cyber security), the governance and supervision structure at the level of state and public institutions is not hierarchical, the lack of cooperation among Lithuanian public and private sector entities prevents an efficient planning of the development of the sphere of electronic information security (cyber security), the existing and regularly detected vulnerabilities of information technologies, if not removed on time, give rise to the disruption of the operation of information resources as well as critical information infrastructures, while the efficiency of detection and removal of these vulnerabilities increases through the centralization of said activities. The compliance with the requirements on electronic information security (cyber security) ensures that information resources are managed in accordance with the requirements of international standards and examples of good practice, however, Lithuania has no efficient compliance management structure; the information maturity model of an organization allows for a better awareness among information resources managers of the need for information resources security and a more efficient management thereof. The dependence of different state and public activity areas on the use of information resources and services varies, therefore, in order to use funds efficiently, it is necessary to consolidate efforts and information resources in the areas where this dependence is stronger; the rate of criminal acts in cyberspace is rapidly increasing and large scale incidents in cyberspace can lead to a national crisis.

There is no law on electronic information security (cyber security) and the regulation thereof by legal acts of lower force is fragmentary and does not cover all members of the information society, at the same time, there is no legal basis to allow an efficient response to incidents in public electronic communications networks, the providers of electronic communications and Internet access services are not required to report the incidents to the National Electronic Communications Network and Information Security Incidents Investigation Service CERT-LT (hereinafter referred to as CERT-LT). Consequently, the instructions of the national CERT-LT for services' providers regarding the elimination of incidents are not mandatory either, there is no legal basis to regulate the use of identification measures directed at reducing the risk of identity falsification and theft in cyberspace.

Often, the services delivered by providers of Internet and other information infrastructure services do not ensure their users' security. During the period of economic hardship, electronic information security (cyber security) received neither sufficient attention nor information resources, however, the application of the principle of collective security would allow for a more efficient use of information resources; no backup information resources or backup infrastructure to sustain the emergency operation of critical infrastructures and information resources have yet been developed. Reliable identification reduces the risk of major threats related to cyberspace and increases users' confidence in cyberspace.

Secure cyberspace (i.e. assurance of electronic information security (cyberspace) security) is the concern of all entities whose activities are related to the provision of services in cyberspace (public institutions, private economic entities, academic society and others). Electronic information security (cyberspace security) projects implemented in cooperation enable the achievement of protection of all stakeholders' interests.

Cyberspace is a global space which has no national boundaries, hence, the rapid spread of threats across cyberspace. The European Union and NATO devote much attention to the security of electronic information and critical information infrastructure. It would be appropriate to apply the principle of collective security not only on a national, but also on international level. Cooperation among highly competent experts, exchange of available information and experience is a prerequisite for an efficient early warning and preventive action.

6.2. To ensure an efficient functioning of critical information infrastructure.

The objective is being pursued, since, currently, the security of critical information infrastructure is ensured only on an institutional level, the coordination structure is not yet in place, no analysis of relationship between objects of this infrastructure or the national impact of its failure has been done, there is no planning of the continuity of activities. Penetration test is the most objective method to evaluate the proper functioning of a security system, however, neither a regulatory framework for its application nor a practice of such testing exist. An efficient monitoring system facilitates the prevention of incidents.

6.3. To seek to ensure the cyber security of the Lithuanian residents and persons staying in Lithuania.

This objective is being pursued, since not all users of electronic information are concerned about electronic information security (cyber security), there is a shortage – and it is likely to be felt even more in the future – of qualified electronic information security experts. Basic knowledge and tools of electronic information security (cyber security) allow the users to avoid many threats facing them in cyberspace.

To ensure cyberspace security it is necessary to establish a continuous and properly managed system covering all phases of incident management, such as early warning, prevention, detection, elimination and investigation. An effective way to fight against malware spreading via remote control computer networks or other malicious cyber activities is to block Internet access to persons and/or equipment engaged in malicious activates. The current social stereotype is that illegal activities conducted in cyberspace are not punishable, therefore, it is important that this stereotype be removed.

Cyber attacks launched from an overseas source can and must be stopped across Lithuania's virtual cyber perimeter in order to avoid their impact on the national electronic communications network. The Lithuanian Internet Traffic Exchange (ITE) node, being a naturally emerged entity, serves as a convenient and efficient centre for hosting protection capabilities of Lithuania's cyberspace (as well as of its virtual perimeter).

Given the implementation of a one-stop-shop principle, the prevailing trend in the area of electronic services is that of unification and centralization; it would be appropriate to exploit this trend also for ensuring the security of these services. The users' confidence in cyberspace services is a major factor of the popularity and further development of these services.

7. In order to achieve the objective specified in paragraph 6.1 of the Programme, the following tasks shall be implemented:

7.1. to improve the coordination and supervision of electronic information security (cyber security);

7.2. to improve the regulatory framework of electronic information security (cyber security);

7.3. to expand and improve a secure national information infrastructure;

7.4. to promote the implementation of electronic information (security cyber security) projects;

7.5. to develop international cooperation in the area of electronic information security (cyber security).

8. In order to achieve the objective specified in paragraph 6.2 of the Programme, it is necessary to implement the task of ensuring the security of critical information infrastructure.

9. In order to achieve the objective specified in paragraph 6.3 of the Programme, the following tasks must be implemented:

9.1. to enhance the culture of protection of electronic information security (cyber security);

9.2. to strengthen Lithuania's cyber security;

9.3. to ensure the protection of Lithuania's virtual cyber perimeter from external cyber attacks;

9.4. to reinforce the security of services delivered in cyberspace.

10. The assessment criteria for Programme implementation and their indicators to be attained in 2011, 2015 and 2019 are specified in the Annex to the Programme.

11. Taking into account the fact that the Programme covers one area, the administration of which falls under the responsibility of the Minister of the Interior, no allocation of EU-financed Programme funding among Programme implementing institutions will be planned.

III. IMPLEMENTATION OF THE PROGRAMME

12. Coordination of Programme implementation shall be carried out by the Ministry of the Interior (hereinafter referred to as Programme Coordinator).

13. Responsibility for the implementation of the objectives and tasks of the Programme shall be with the institutions and bodies specified in the Annex to the Programme.

14. Institutions participating in the implementation of the Programme shall:

14.1. taking into account the tasks and targeted outcomes laid down in the Programme, plan the level of the outcome to be achieved within the planned period, select measures and plan funds and include them into strategic action plans and/or annual action plans and annually, by 1 August, submit this information to the Programme Coordinator;

14.2. submit annually, by 1 February, to the Programme Coordinator information on implemented measures and achieved results.

15. The Programme Coordinator shall:

15.1. supervise the implementation of the strategic goal, objectives and tasks of the Programme, carry out an interim review of the tasks laid down in the Programme and changes in the levels of task assessment criteria and, if necessary, initiate an update of the Programme;

15.2. present information on implementation and results of the Programme in an annual Programme Coordinator's Activity Report.

16. Preparation of additional legal acts other than referred to in paragraph 14.1 of the Programme will not be required.

_____

Annex to the 2011–2019 Programme for the Development of Electronic Information Security (Cyber Security)

PROGRAMME FOR THE DEVELOPMENT OF ELECTRONIC INFORMATION SECURITY (CYBER SECURITY) FOR 2011–2019
ASSESSMENT CRITERIA AND THEIR EXPECTED INDICATORS

No. Nr.	*Objective*	*Task*	Assessment criterion	Indicator in 2011	Indicator in 2015	Indicator in 2019	Institution responsible for implementation of the criterion
1.	*1. To ensure the security of national information resources*		Level of compliance of national information resources with security requirements, (%)	–	95	98	All the institutions specified in items 3 to 29 of this Annex, according to their competences
2.		1.1. to improve the coordination and monitoring of electronic information security (cyber security);	Level of resources (%), security of which is monitored by an institution designated by the law on the basic requirements related to ensuring electronic information security (cyber security)	–	70	100	All the institutions specified in items 3 to 10 of this Annex, according to their competences
3.			Percentage of entities in defining and implementing national policy in the area of electronic information security (cyber security) that belong to the national system of coordination of electronic information security (cyber security), (%) Permanent collegial consultative council of electronic information security (cyber security) established	– –	80 yes	100 yes	Ministry of the Interior, Ministry of National Defence, Ministry of Transport and Communications, State Data Protection Inspectorate
4.			Number of evaluation studies of existing capabilities in the area of electronic information security (cyber security) and their potential	–	1	2	Ministry of the Interior

No. Nr.	*Objective*	*Task*	Assessment criterion	Indicator in 2011	Indicator in 2015	Indicator in 2019	Institution responsible for implementation of the criterion
5.			Methods for evaluation of threats and vulnerabilities approved Number of performed evaluations of threats and vulnerabilities Level of uncontrollable vulnerabilities, (%)	– – –	yes 4 20	yes 8 10	Ministry of the Interior, Communications Regulatory Authority, State Data Protection Inspectorate
6.			Percentage of information systems monitored by the system for monitoring compliance with the requirements of electronic information security (cyber security), (%)	0	60	100	Ministry of the Interior
7.			Percentage of information systems managers who have enhanced their level of maturity in electronic information security management, (%)	–	50	100	Ministry of the Interior
8.			Percentage of public institutions, economic entities that provide services to public institutions and of public services provided to society with an estimated level of reliance on cyberspace and the use of information and communication technologies, (%)	–	60	100	Ministry of the Interior, Ministry of Transport and Communications
9.			Percentage of completed pre-trial investigations into criminal offences in cyberspace, (%)	–	30	50	Police Department under the Ministry of the Interior
10.			Participation in the investigation of cyber incidents that have caused or may have caused a crisis, (%)	–	60	90	Office of the Prime Minister
11.		1.2. to improve the regulatory framework of electronic information security (cyber security)	Percentage of adopted or amended legal acts among the legislation for which the need for adoption or amendment was identified (%)	–	80	100	All the institutions specified in items 12 to 15 of this Annex, according to their competences

No. Nr.	*Objective*	*Task*	Assessment criterion	Indicator in 2011	Indicator in 2015	Indicator in 2019	Institution responsible for implementation of the criterion
12.			Specific laws providing for the basic requirements related to ensuring electronic information security (cyber security) and regulating appropriate acts and legal relationships (including the Law of the Republic of Lithuania on Electronic Communications Networks and Information Security) adopted	–	yes	yes	Ministry of the Interior, Ministry of Transport and Communications, Communications Regulatory Authority
13.			Percentage of adopted or amended legal acts among the legislation for which the need for adoption or amendment was identified, (%)	–	80	100	Ministry of the Interior, Communications Regulatory Authority, State Data Protection Inspectorate
14.			Requirements for the provision of services of a secure national (state) data communication network approved	–	yes	yes	Ministry of Transport and Communications, Ministry of the Interior, Communications Regulatory Authority
15.			Classification of identification measures (methods) and reliability of services (harmonized with that of other Member States of the European Union), technical and procedural requirements as well as the procedure for its accreditation and use approved	–	yes	yes	Ministry of the Interior, Communications Regulatory Authority (as far as it is related to its function as a supervisory authority for electronic signature)
16.		1.3. to expand and improve a secure national information infrastructure	Level of information resources using the secure infrastructure, (%)	–	70	100	All the institutions specified in items 17 to 21 of this Annex, according to their competences
17.			Approval of service provision requirements for enhancing the responsibility of economic entities in the provision of information infrastructure services for the security of provided services	–	yes	yes	Ministry of Transport and Communications

No. Nr.	*Objective*	*Task*	Assessment criterion	Indicator in 2011	Indicator in 2015	Indicator in 2019	Institution responsible for implementation of the criterion
18.			Proportion of the amount of funds planned for information systems security by information systems managers compared to the amount planned for the development and maintenance of information systems, (%)	–	10	15	Ministry of the Interior, Ministry of Transport and Communications
19.			Proportion of the backup capabilities of communications and information systems designed to ensure public administration needs compared to the active capabilities, (%)	–	20	30	Ministry of the Interior, Ministry of Transport and Communications
20.			Level of information systems using the collective defence system of e-Government information resources against public network threats, (%) 1st category information system 2nd category information system 3rd category information system 4th category information system	 0 0 0 0	 80 60 50 40	 100 100 100 100	Ministry of the Interior
21.			System for ensuring a reliable identification of the users and information resources within the national information infrastructure and the critical information infrastructure as well as for providing electronic identification services is in place	–	yes	yes	Ministry of the Interior
22.		1.4. to encourage the implementation of electronic information security (cyber security) projects	Proportion of projects implemented on the basis of cooperation between entities engaged in government activities compared to the total number of information infrastructure protection projects, (%)	–	30	50	Ministry of the Interior, Ministry of National Defence, Lithuanian Research and Studies Computer Network LITNET Council (hereinafter referred to as LITNET)

No. Nr.	*Objective*	*Task*	Assessment criterion	Indicator in 2011	Indicator in 2015	Indicator in 2019	Institution responsible for implementation of the criterion
23.			Percentage of projects that received proposals from associations, (%)	–	20	50	Ministry of the Interior, Communications Regulatory Authority
24.			Percentage of the initiatives of national economic entities and education institutions (research, projects, decisions and etc.) implemented jointly with public institutions, (%)	–	30	50	Ministry of Education and Science, Ministry of the Interior, Communications Regulatory Authority, LITNET Council
25.		1.5. to develop international cooperation in the area of electronic information security (cyber security)	Number of areas (the pillars for addressing the challenges specified in the EC Communication COM (2009) 149 of 30 March 2009) of international cooperation	–	3	5	All the institutions specified in items 26 to 29 of this Annex, according to their competences
26.			Participation, upon invitation, in the events on electronic information security (cyber security) organized by the NATO, European Union and the United Nations Organization, (%)	–	50	80	Communications Regulatory Authority, Ministry of National Defence, Ministry of the Interior, Ministry of Transport and Communications
27.			Number of representatives delegated to the NATO Cooperative Cyber Defence Centre of Excellence Participation, upon invitation, in events organized by to the NATO Cooperative Cyber Defence Centre of Excellence, (%)	1 –	1 50	2 80	Ministry of National Defence
28.			Participation, upon invitation, in international cyber security exercises, (%)	–	50	80	Communications Regulatory Authority, Ministry of National Defence, LITNET Council

No. Nr.	*Objective*	*Task*	Assessment criterion	Indicator in 2011	Indicator in 2015	Indicator in 2019	Institution responsible for implementation of the criterion
29.			Number of agreements signed with the CERT services of other states	–	3	6	Communications Regulatory Authority, Ministry of National Defence, Ministry of the Interior, LITNET Council
30.	*2. To ensure an efficient functioning of critical information infrastructure*		Average time taken to respond to critical information infrastructure incidents, (hours)	–	1	0,5	All the institutions specified in items 32 to 40 of this Annex, according to their competences
31.		2.1. to ensure the security of critical information infrastructure	Percentage of critical information infrastructures that comply with the requirements on electronic information security (cyber security), (%)	–	60	100	All the institutions specified in items 32 to 40 of this Annex, according to their competences
32.			Percentage of identified critical information infrastructures, (%) Percentage of critical information infrastructures subject to analysis of critical resources and services as well as risk assessment of the disruption of performance due to failure of their information infrastructure or their vital external infrastructures, (%)	– –	100 70	100 100	Ministry of the Interior, Communications Regulatory Authority, Ministry of National Defence, LITNET Council
33.			Security requirements for critical information infrastructures approved	–	yes	yes	Ministry of the Interior, Ministry of National Defence, LITNET Council
34.			Percentage of critical information infrastructures subject to resilience assessment, (%)	–	60	100	Ministry of the Interior

No. Nr.	*Objective*	*Task*	Assessment criterion	Indicator in 2011	Indicator in 2015	Indicator in 2019	Institution responsible for implementation of the criterion
35.			Number of Lithuania's critical electronic communications and Internet network infrastructures that are under regular monitoring and the number of elements of Lithuania's cyber perimeter compared to the total, (%)	–	95	99,5	Communications Regulatory Authority, LITNET Council
36.			Number of institutions taking part in the activities of the European Union's Critical Infrastructure Warning Information Network (CIWIN)	–	7	12	Office of the Prime Minister
37.			Institution responsible for continuity of the performance of critical infrastructures during failures designated	–	yes	yes	Office of the Prime Minister
38.			Cyber Defence Plan for protecting critical information infrastructures by institutions for national defence approved National Cyber Defence Plan for protecting critical information infrastructures and national information resources approved	– –	yes –	yes yes	Ministry of National Defence, State Security Department, Communications Regulatory Authority, Ministry of the Interior, Ministry of Transport and Communications, Ministry of Economy, Ministry of Energy, Ministry of Finance
39.			The plan for preparation and management, during a crisis, of backup infrastructure required for ensuring the viability of critical information infrastructures approved	–	yes	yes	Ministry of the Interior, Ministry of National Defence

No. Nr.	*Objective*	*Task*	Assessment criterion	Indicator in 2011	Indicator in 2015	Indicator in 2019	Institution responsible for implementation of the criterion
40.			Percentage of critical information infrastructures, excluding the electronic communications networks designed to secure national defence and/or required to ensure defence capabilities in fulfilment of the commitments to the NATO or the European Union, that have been connected to a secure inter-institutional data transmission network, the services of which are provided by the provider/providers of the Secure State Data Communication Network appointed by the Government of the Republic of Lithuania, (%)	–	70	100	Ministry of the Interior
41.	*3. To ensure the cyber security of the Lithuanian residents and persons staying in Lithuania*		Percentage of the Lithuanian population who feel secure in cyberspace, (%)	–	40	60	All the institutions specified in items 43 to 59 of this Annex, according to their competences
42.		3.1. to enhance the culture of protection of electronic information security (cyber security);	Percentage of the Lithuanian population who are aware of cyber security principles, (%)	–	60	80	All the institutions specified in items 43 to 48 of this Annex, according to their competences
43.			Number of programmes drafted for the training and professional development of specialists in electronic information security (cyber security) Number of specialists that have completed the programmes	– –	1 80	2 200	Ministry of Education and Science, Ministry of the Interior, Communications Regulatory Authority, LITNET Council
44.			Number of specialists who have been trained in information law Research in the area of information law carried out	– –	20 10	30 15	Ministry of Education and Science LITNET Council

No. Nr.	*Objective*	*Task*	Assessment criterion	Indicator in 2011	Indicator in 2015	Indicator in 2019	Institution responsible for implementation of the criterion
45.			Number of operational cyber security self-education websites Percentage of visitors who gave a positive assessment of a website's usefulness, (%)	– –	1 50	1 60	Ministry of the Interior, State Data Protection Inspectorate
46.			Number of organized events to increase awareness on the importance of electronic information security (cyber security)	–	4	8	Ministry of the Interior, Communications Regulatory Authority, Ministry of Education and Science, State Data Protection Inspectorate
47.			Average number of electronic information security measures used by a user, (measures)	–	2	4	Ministry of the Interior, Ministry of Transport and Communications, Communications Regulatory Authority
48.			Number of press releases on electronic information security initiatives	–	8	16	Communications Regulatory Authority, Ministry of the Interior, Ministry of Education and Science
49.		3.2. to strengthen Lithuania's cyber security	Average time of response to cyber incidents, (hours)	–	1	0,5	All the institutions specified in items 50 to 52 of this Annex, according to their competences
50.			Number of operational and cooperating CERT teams engaged in computer emergency response activities	–	5	8	Communications Regulatory Authority, Ministry of National Defence, LITNET Council

No. Nr.	*Objective*	*Task*	Assessment criterion	Indicator in 2011	Indicator in 2015	Indicator in 2019	Institution responsible for implementation of the criterion
51.			National early warning system to alert of network and information security vulnerabilities and threats established	–	yes	yes	Ministry of the Interior, Communications Regulatory Authority, State Data Protection Inspectorate, LITNET Council
52.			Number of digital evidence investigation laboratories for identifying illegal activities in cyberspace	–	0	1	Ministry of the Interior, Police Department under the Ministry of the Interior, Communications Regulatory Authority, LITNET Council
53.		3.3. to ensure the protection of Lithuania's computer network (virtual cyber perimeter) from external cyber attacks	Level of network connections' compliance with the requirements of electronic information security, (%)	–	70	100	All the institutions specified in items 54 to 56 of this Annex, according to their competences
54.			Legal framework established and the requirements for setting up international network connections and their further management defining the monitoring and alerting responsibilities of operators of such network connections, as well as the coordination of operators' activities in the case of an external cyber attack approved	–	yes	yes	Ministry of Transport and Communications, Communications Regulatory Authority
55.			Institution responsible for the supervision of the operators for managing the network connections across Lithuania's virtual cyber perimeter designated	–	yes	yes	Ministry of Transport and Communications, Communications Regulatory Authority

No. Nr.	*Objective*	*Task*	Assessment criterion	Indicator in 2011	Indicator in 2015	Indicator in 2019	Institution responsible for implementation of the criterion
56.			Provisions on the Lithuanian Internet Traffic Exchange (ITE) approved	–	yes	yes	Ministry of the Interior, Ministry of Transport and Communications, State Data Protection Inspectorate
57.		3.4. to reinforce the security of services delivered in cyberspace	Percentage of cyber services that comply with the requirements of electronic information security (cyber security), (%)	–	70	100	All the institutions specified in items 58 to 59 of this Annex, according to their competences
58.			Percentage of services protected and controlled by the system for implementation and control of collective security of services provided in cyberspace, (%)	–	70	100	Ministry of Transport and Communications, Ministry of the Interior
59.			Proportion of the Lithuanian population who trust in the services provided in cyberspace, (%)	–	50	67	Ministry of the Interior, Communications Regulatory Authority, public administration institutions providing services in cyberspace

_____