THIS IS AN UNOFFICIAL ENGLISH SUMMARY OF THE PROPOSALS, THE OFFICIAL PROPOSAL CAN BE FOUND IN FINNISH AND IN SWEDISH HERE:
http://valtioneuvosto.fi/paatokset/paatos?decisionId=0900908f8057a85c

SUMMARY OF THE PROPOSAL

The key objective of the Government Programme of Juha Sipilä's Government is to promote digitalisation. According to the Government Programme, it is Finland's objective to take a productivity leap in public services and the private sector by grasping the opportunities offered by digitalisation. Furthermore, a favourable operating environment will be created for digital services and new business models. As a part of the key project to create a growth environment for digital business operations, introduction of new technologies, digitalisation and new business concepts will be promoted by legislative means, and data security and its potential for creating more competitive benefit will be ensured.

Under the Government's plan of action, the Government's objective is to improve the capabilities required by internal security also in the area of digital security because a digital society requires a high level digital security dimension.

This government proposal is part of the implementation of the objective of the Government Programme to promote digitalisation and ensure digital security by improving the level of computer security in services that are essential to society and citizens. The proposal will increase citizens' and companies' confidence in digitalisation and hence also the growth and competitiveness of digital business.

The proposal includes obligations concerning risk management and disruption reporting concerning computer security to certain providers of services that are considered essential to societal activities and to certain providers of digital services. Legislation would also be enacted on the supervising of these obligations, exchange of information and general activities of the authorities regarding computer security.

In order to improve the computer security of services that are essential to societal activities, amendments should be made to the Information Society Code (917/2014), the Aviation act (864/2014), the Railway act (304/2011), the Vessel Traffic Service Act (623/2005), the Act on Security Measures on certain Ships and in Ports Serving them and on Monitoring the Security Measures (485/2004), the Traffic Services Act (320/2017), the Electricity market act (588/2013), the Natural gas market act (xx), the Water Services Act (119/2001), and provisions should be added on the obligation of providers of essential service to ensure the management of risks concerning communications networks and information systems and to report to the supervisory authority and the public of significant disruptions associated with computer security. The obligations laid down in the Information Society Code would apply to providers of on-line market places, search engines and cloud services. The obligations of the Aviation act would apply to providers of air navigation services and operators of airports that are essential to societal activities. The obligations of the Railway Act would concern the operators of the state rail network and the companies providing traffic control services. The obligations of the Vessel Traffic Service Act would apply to providers of vessel traffic services. The obligations laid down in the Act on Security Measures on certain Ships and in Ports Serving them and on Monitoring the Security Measures would apply to operators of ports that

are essential to societal activities. The obligations laid down in the Electricity market act would apply to system operators. The obligations laid down in the Natural gas market Act would apply to the operator of the transmission system, and the obligations laid down in the Water Services Act would apply to water utilities that supply at least 5000 cubic meters of water per day.

To secure the comprehensive control and supervision of obligations associated with the security of operations in different sectors and to avoid overlapping supervisory authorities and administrative burden, the authority to supervise compliance with risk management and incident reporting obligations should rest with sector-specific supervisory authorities. This would apply to the Finnish Communications Regulatory Authority, the Finnish Transport Safety Agency, Energy Authority, the Financial Supervisory Authority and the National Supervisory Authority for Welfare and Health. To ensure collaboration between authorities it is proposed that provisions would be included in conjunction with legislation concerning the powers of the authorities on co-operation between supervisory authorities and the exchange of significant confidential information related to carrying out duties associated with computer security.

In addition, the Finnish Communications Regulatory Authority would be given a statutory obligation to co-operate with computer security incident response teams, supervisory authorities and the Cooperation Group that respond to and investigate computer security violations referred to in the Network and Information Security Directive.

The proposed legislation would transpose to national legislation the Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union.

Identification of operators of essential services

The Network and Information Security Directive requires Member States to identify the providers with an establishment on their territory that provide the services that are essential in the sectors and their sub-sectors that fall within the scope of the Directive. The sectors and sub-sectors that fall within the scope of the Directive have been specified in Annex II of the Directive.

The criteria for the identification of the operators of essential services, as referred to in point (5) of Article 4, shall be as follows: providers of essential services must provide a service that is essential to the maintenance of critical societal and/or economic activities; the provision of that service must depend on network and information systems; and in addition, incidents affecting the service must have a significant disruptive effect on the provision of the service, as referred to in Article 6 of the Directive. In fact, the Directive allows Member States considerable room for manoeuvre in identifying essential services.

According to the introduction of the Directive, operators of essential services could be identified by adopting a list enumerating all operators of essential services or by adopting national measures, which make it possible to determine which entities are subject to obligations regarding the security of network and information systems.

Infrastructure or services that are critical to societal activities have not been defined in Finnish legislation and the current laws do not contain proper procedures under which providers of essential services as referred to in the Network and Information Security Directive could be directly specified by supervisory authorities, for example. Considering the existing administrative structures and current legislation, it would be most natural to identify the providers of essential services in the context of issuing laws concerning the transposition of the Network and Information Security Directive.

Under the Network and Information Security Directive, essential service providers provide a service which is essential for societal activities. The Directive leaves the assessment of what is essential to the discretion of the Member States.

In each of the sectors and sub-sectors referred to in the Directive, identifying services that are essential to societal activities is dependent on the special features of each sector. Whether a service is essential depends on, among other things, its significance to citizens and businesses, the reliance of industry on the services and the number of different competing services available on the market. Services that are essential to societal activities may be critical to national emergency supply or a wider group of entities than critical infrastructure.

Furthermore, an essential service must be dependent on network and information systems. The Directive also leaves the evaluation of this dependence to the discretion of the Member States. When evaluating the dependency, the organisation of the provision of the service must be considered. As a general principle, it can be assumed that a large part of services are currently dependent in one way or another on the use of communications networks and information systems.

In addition, the Directive provides that incidents affecting a service must have a significant disruptive effect on the provision of the service. The Directive specifies that in the evaluation of a significant disruptive effect, consideration must be given to the number of dependent users, the dependency of other essential services on the service offered by the entity in question, the impact of the incidences on economic and societal activities or general security, the market share of the entity, the geographic reach of the entity in the area that may affected by the incident and the availability of alternative means of providing the service. The obligations listed in the Directive are such that they must be evaluated on a national basis by sector and service.

In October 2016, the Ministry of Transport and Communications established a cross-sectoral working group to provide support in the transposition of the Network and Information Security Directive. In its final report the working group proposed that the providers of essential services as referred to in the Directive be defined in law. In order to assign the obligations we must assess which services must be considered societally essential from a national perspective as referred to in the Directive in the sectors that fall within the Directive's scope. Subsequently, we must determine whether the providers of such services are already under existing legislation obliged to guarantee computer security at least at the level required by the Directive. If the answer is yes, there is no need to lay down new obligations in law. In contrast, providers of services that are essential to the providers of which sufficient obligations in light of the Directive have not been laid down in current law must be specified.

Energy

Under the Network and Information Security Directive, essential services and their providers must be specified in the energy sector's sub-sectors electricity, oil and gas.

Today, societal activities are highly dependent on various electric systems. Moreover, nearly all services essential to societal activities require electricity. The distribution of electricity is so important to services that are essential to society and continuity that it must always be considered an essential service to its customers irrespective of the size of the distribution system, for example.

The Finnish electrical network consists of the main grid, regional grids and distribution systems. The main grid is used to transmit electricity from power generation areas and abroad to centres of consumption. The majority of the electricity consumed in Finland is transmitted via the main grid. Some of the electricity-generating power plants are connected directly to the main grid as are major consumers such as large factories. Power plants may also be connected to the regional and distribution systems. For instance, electrified sections of railway are powered directly by the main grid as is the Helsinki-Vantaa Airport. There are 77 operators of electrical distribution systems and 11 operators of high-voltage distribution systems in Finland. The main grid operator responsible for the electrical network system is Fingrid Oyj.

Under point (2), Article of the Network and Information Security Directive, the following may be considered electricity distribution services that are essential to critical societal and(or economic activities

1) transmission service in the main grid and system services provided by a main grid operator responsible for the system
2) electricity transmission in a distribution system, excluding transmission in a closed distribution system
3) electricity transmission in a high-voltage distribution system to which a distribution system is connected, excluding transmission in a closed distribution system

In the gas sub-sector natural gas plays a major role in Finnish energy consumption. Natural gas is used to produce approximately eight per cent of the energy consumed in Finland. Natural gas is used especially in the combined production of district heat and electricity. Industrial manufacturing processes are another major user of natural gas. In 2016. 23.8 terawatt hours of natural gas was used in Finland.

Disruption-free distribution operations and natural gas transfer network are essential to the use of natural gas. Under point (2), Article 5 of the Network and Information Security Directive, distribution services in a distribution system and system services provided by distribution system operators that are responsible for the system as referred to in the Natural gas markets act may be considered services that are essential to critical societal and/or economic activities.

No essential services or their providers have been identified that meet the criteria of the Directive in the oil sub-sector.

Transport

In the sector of transport, services can be roughly divided into three levels: traffic control services, maintenance of essential infrastructure and provision of transport services. The nature of the services varies depending on the level of the transport system.

Traffic control services

Traffic control is essential to the operation of the transport system and has an immediate impact on the safety of the transport system as a whole. Disruptions in traffic control may directly endanger traffic safety or cause interruption of traffic. Furthermore, traffic control operations are centralised and dependent on a small number of operators. The significance of traffic control to the operation and safety of the transport system will in the future be emphasised as intelligent traffic automation increases.

In the case of aviation, air navigation services are responsible for traffic control. Under section 160 of the Aviation act, air navigation services included air traffic services, communications, navigation and control services, weather services for air navigation and aeronautical information services. In Finland, air navigation service are provided by Air Navigation Services Finland Oy (ANS Finland), which is wholly owned by the State. ANS Finland is responsible for special duties related to air navigation, including airspace management, air guard, services to government aviation and air rescue services. The Government has appointed the Finnish Meteorological Institute as the provider of aviation weather services as referred to in section 108 of the Aviation act.

Under section 36 of the Railway act, railway network operators are responsible for traffic control of the railway network they manage. Operators of railway networks can organise traffic control services by themselves or acquire them from public or private service providers. The Finnish Transport Agency is responsible for the supervising and coordination of the operations of railway traffic control. The actual operative railway traffic control is purchased from Finrail Oy.

Water traffic control is provided by vessel traffic service. Under the Vessel Traffic Service Act, vessel traffic service (VTS) means the supervision and management of vessel traffic with a capability to interact with traffic and respond to changing traffic situations. The vessel traffic service is operated by the VTS authority. Under the Vessel Traffic Service Act, the VTS authority is the Finnish Transport Agency.

The role played by traffic control in road transport is somewhat different from the role it plays in other modes of transport in relation to its effects. To a significant degree, traffic control is currently still based on traffic regulations and such means of traffic control that are not dependent on communications networks and information systems (road markings, road signs).

Under point (2) Article 5 of the Network and Information Security Directive, the traffic control services may be considered essential to critical societal and(or economic activities In other words, the essential services of the different modes of transport are air navigation services, railway traffic control services and vessel traffic services. Currently, road traffic control services would not be considered essential to society as referred to in the Network and Information Security Directive. However, this will have to be re-evaluated as the intelligent automation of transport advances.

Maintenance of essential traffic infrastructure

In addition to traffic control the provision of many traffic control services depends on essential traffic infrastructure (airports, ports, railways, road network) and it is often not possible to provide alternative services if the essential infrastructure is not available. Essential traffic infrastructure includes especially airports, ports, railways and the road network.

Airports play an important role in passenger traffic in Finland and the number of passengers is on the increase. In 2016, the Finnish passenger volume exceeded 16 million. The number of passengers travelling via Finavia’s airports increased by eight per cent on 2015. In 2016, 183 442 tonnes of cargo passed through Finavia’s airports. Air cargo accounted for approximately 10 per cent of foreign trade.

Several service providers provide services at airports. However, the airport managing body, which is responsible for management of the airport, is the most essential one from the perspective of infrastructure maintenance.. The Aviation act provides on the conditions for granting approval certificates. Airport operators are also responsible for implementing measures and arrangements with the purpose of improving aviation safety. Airport operators have statutory emergency planning obligations. Airport operators operating in Finland include Finavia Corporation, the City of Mikkeli and Seinäjoen lentoasema Oy.

In addition to airports, ports are part of the essential traffic infrastructure. In 2014, maritime transports in foreign trade were 96 million tonnes and land transports were approximately 11 million tonnes. 96 per cent of the goods in Finland's foreign trade are shipped by sea. Hence the economy and the rest of society as a whole are very dependent on the operation of ports. As is the case with airports, services at ports are provided by several different entities. It is the duty of the port operator to maintain the port and its infrastructure. The obligations of port operators are laid down in the Act on Security Measures on certain Ships and in Ports serving them.

Railways are also essential in both passenger and goods transport. In 2016, approximately 82 million persons travelled by train. The volume of goods transport on the railways was 37 million tonnes in 2014 and total haulage was approximately 9.6 billion tonne-kilometres. Infrastructure managers carry out the maintenance, development and upkeep of the railway network. Under the Railway Act, the infrastructure manager of the state railway is the Finnish Transport Agency. In contrast, private railways mean railways other than those owned by the state and managed by the Finnish Transport Agency. The operators of such railways include municipalities, ports and businesses. Private railways may be significant to a particular industrial plant or a port. However, their maintenance is not essential to societal activities in the same way as that of state railways.

The road network is also an essential part of the traffic infrastructure. From the perspective of computer security, the digital information systems associated with the road infrastructure are essential to road network maintenance. Such information systems include ITS systems as referred to in the ITS directive. The ITS Directive has been transposed in Finland into the Transport Code. Part III, Chaper 2, section 6, of the Transport Code provides on the implementation of intelligent transport systems. At the moment, the eCall emergency call system and the Digiroad (road information) and Digitraffic (traffic information) systems maintained by the Finnish Transport Agency can be considered intelligent transport systems as referred to in the ITS Directive. The eCall system is maintained by the Emergency Response Centre Administration.

Digiroad is a national information system maintained by the Finnish Transport Agency that includes the centreline geometry of the entire Finnish street and road network and its most important attribute data. Digiroad is a digital description of the transport network. Digitraffic is a Finnish Transport Agency service that provides up-to-date traffic information on the Finnish road network and railway and maritime traffic.

Under point (2), Article 5 of the Network and Information Security Directive, the maintenance of essential transport infrastructure may as a general principle be considered essential to critical societal and/or economic activities In other words, essential services within the different modes of transport are the operation of airports, ports and the state rail network and the ITS systems referred to in the ITS directive.

Transport services

In addition to traffic control and the maintenance of the transport infrastructure, many types of services are available in the transport sector (including air carriers, shipping companies and rail transport operators). The essential nature of transport services for society is, however, somewhat

different from the services of traffic control and infrastructure maintenance mentioned above. Several competing entities can offer transport services. In addition, there may be alternative ways to provide a service. While services for some transport modes are provided by only a few or even only one entity in Finland (such as air and rail transport), there are usually alternative services available due to international competition or alternative modes of transport. In general, transport services are becoming increasingly international. In the case of aviation, for example, this has led to an internationally harmonised regulation of the common global aviation system. Consequently, it is apparent that in the future it will be possible to develop computer security in a more targeted and harmonised way also with regard to transport service operators as a part of a transport mode specific development of international agreements and EU regulations. This way any disruptions to the operation of transport systems,safety and international competitive circumstances due to national regulations could be avoided.

The banking sector and financial market infrastructures

With regard to the infrastructures of the banking sector and the financial markets, the Network and Information Security directive's annex does not identify the sub-sectors in which services essential to societal activities must be identified. Annex II of the directive mentions credit institutions as operator types, operators of trading venues as defined in point (4), Article 1 of Directive 2014/65/EU of the European Parliament and of the Council, and central counterparts. With regard to the essential infrastructure of the Finnish banking sector and the financial markets, credit institutions referred to in the Act on Credit Institutions and engaging in stock-exchange activity as referred to in the Act on Trading in Financial Instruments should be considered essential services to critical societal and/or economic activities under point (2), Article 5 of the Network and Information Security Directive. No central counterparts falling within the scope of the directive operate in Finland.

Health sector

The purpose of health care is to promote and maintain the health, wellbeing, working and functional capacity, and social security of the population and to narrow health disparities. The disruption-free operation and continuity of healthcare is essential to societal activities. Healthcare sector service providers include public and private providers of social welfare and healthcare services. From the perspective of computer security, the most significant disruptive effects to society could include computer security incidents concerning systems that handle information or are part of healthcare equipment. As a result, electronic processing of healthcare customer information and maintenance and operation of healthcare equipment in the provision of public and private social welfare and healthcare services should be considered services that are essential to critical societal and/or economic activities as referred to in point (2), Article 5 of the Network and Information Security Directive.

Drinking water supply and distribution

Basic societal activities must have a functioning water supply. Along with electricity supply, water supply is one of the most important societal services and should operate in all circumstances. Water

supply is very important especially for households as drinking water and in maintaining hygiene, in healthcare and in the food and other industries.

Water utilities provide water supply to communities. Under point (2), Article 5 of the Network and Information Security Directive, water supply may be considered essential to critical societal and/or economic activities.

Digital Infrastructure

Under the Information Society Code, a telecommunications operator means a network operator or a communications service operator offering services to a set of users that is not subject to any prior restriction, i.e. provides public telecommunications services. The definition of a telecommunications operator is broad and covers the key activities of digital infrastructure, including internet exchange points at least in so far as they are used to connect public communications networks and the provision of domain name services when it is associated with providing an internet service.

Communication networks other than public ones can also connect to internet exchange points and this typically occurs. For instance, large content providers may use internet exchange points. There is also traffic between public communications networks outside of internet exchange points. Finnish operators exchange traffic also outside of Finland, in Swedish exchange points, for example. Two exchange point providers exist in Finland and a third one is launching operations.

While public telecommunications services could be considered essential to societal activities in the sector of digital infrastructure, telecommunications operators are mainly considered to not be included within the scope of the Network and Information Security Directive. Furthermore, the Information Society Code already includes provisions on computer security risk management that applies to telecommunications operators and their obligation to notify of incidents.

In addition to public telecommunications services, top-level domain name registries can be considered essential to digital infrastructure. In Finland, maintenance of TLD registries is essential with regard to the fi and the ax country code TLDs. Under point (2), Article 5 of the Network and Information Security Directive, the maintenance of a TLD registry may be considered essential for critical societal and/or economic activities

Requirements concerning computer security risk management and incident reporting associated with the operations of service providers

Energy

In the electricity sub-sector the following have been identified as services that are essential to societal activities as referred to in point (2) of Article 5 of the Network and Information Security Directive

1) transmission service in the main grid and system services provided by a main grid operator responsible for the system

2) electricity transmission in a distribution system, excluding transmission in a closed distribution system
3) electricity transmission in a high-voltage distribution system to which a distribution system is connected, excluding transmission in a closed distribution system

Under Article 5 of the Network and Information Security Directive, the provision of an essential service must also be dependent on network and information systems. Furthermore, an incident affecting the service should have significant disruptive effects on the provision of that service. Electricity distribution can always be considered dependent on network and information systems because modern electricity systems are to a large degree automated systems and their reliability is essential to ensuring the availability of energy. Computer security disruptions concerning electricity distribution may have significant disruptive effects to electricity distribution and the provision of other services that area essential to societal activities. These effects may be significant irrespective of the size of the distribution system. Consequently, main grid operators with system responsibility and any other main grid operators, all distribution system operators irrespective of their size and those high-voltage distribution system operators whose system has been connected to a distribution system, but excluding closed distribution systems, could be considered operators of essential services under the Network and Information Security Directive.

With regard to natural gas, transfer services in a transfer network and system services provided by transmission system operators that are responsible for the system as referred to in the Natural gas markets act have been above considered essential for critical societal and/or economic activities as referred to in point (2), Article 5 of the Network and Information Security Directive. These services are, as a general principle, always dependent on network and information systems because modern natural gas systems are, to a large degree, automated and their reliability is essential for ensuring the availability of energy. In addition, significant computer security disruptions to the service could have a significant disruptive effect on the continuity of the natural gas transmission service.Consequently, transmission system operators with system responsibility and any other transmission system operators could be considered essential service providers as referred to in the Network and Information Security Directive.

While there are some risk management obligations in the Electricity market act and the Natural gas markets act, no provisions have been laid down concerning the management of risks associated with communications networks and information systems of the providers of essential services specified above. Furthermore, no provisions have been laid down in law on reporting disruptions, with the exception of notifying users as referred to in section 59 of the Electricity market act. Hence provisions should be added to the Electricity market act and the Natural gas markets act that would oblige the providers of essential services to ensure the security of communications networks and information systems and report to the Energy Authority on disruptions to computer security.

Transport

In the transport sector, the following have been identified as services that are essential to society as referred to in the Network and Information Security Directive

1) air navigation services,
2) railway traffic control services,
3) vessel traffic services,
4) airport operations,
5) operation of the state railway network,
6) port operations, and
7) ITS system operations as referred to in the ITS directive.

As a general principle, air navigation services, railway traffic control services, vessel traffic services, operating the state rail network and maintenance of ITS systems referred to in the ITS directive can always be considered dependent on network and information systems. Significant computer security disruptions to these services could also have a significant disruptive effect on the safety and continuity of the transport system. The providers of all of these services should be considered essential service providers as referred to in the Network and Information Security Directive.

The operation of airports and ports differs to some degree from the aforementioned services. The size of airports and ports varies. As a consequence, their dependence on network and information systems also varies, as does the impact of computer security disruptions on the provision of services that are essential to societal activities. For instance, the ten largest ports in Finland handle approximately 80 per cent of the total maritime transport volume. Disruptions impacting these ports could have a much more significant impact than those impacting smaller ports. Hence not all managing bodies of these services should be considered providers of essential services as referred to in the Network and Information Security Directive. Assigning obligations should be assessed especially in the light of Article 6 of the Network and Information Security Directive. Assigning obligations to the providers of essential services referred to in the Network and Information Security Directive could be done with greater precision with a Government decree.

In the transport sector, the following can be considered providers of essential services as referred to in the Network and Information Security Directive

- providers of air navigation services
- companies providing railway traffic control services and infrastructure managers of the state railway
- providers of vessel traffic services
- operators of ITS systems as referred to in Part III, chapter 2, section 6, of the Transport Code
- operators of ports that are essential to societal activities (would be identified by Government decree)
- operators of airports that are essential to societal activities (would be identified by Government decree).

While the legislation concerning risk management that providers of essential services engage in could as such me considered to include obligations that are associated with network and information systems, current transport-mode specific legislation does not include actual obligations to manage risks associated with communications networks and information systems. When computer security

is endangered, the traffic safety and the continuity of essential services may also be endangered as a result. Hence obligations regarding ensuring computer security and notifying the Finnish Transport Safety Agency of significant disruptions to computer security should be included in

- the Aviation act concerning the providers of air navigation services and airport operators,
- in the Railway Act concerning companies providing railway traffic control services and the State railway network operator
- in the Vessel Traffic Service Act concerning providers of vessel traffic services
- in the Act on Security Measures on certain Ships and in Ports Serving them concerning port operators, and
- in the Transport Code concerning the operators of ITS systems as referred to in Part III, chapter 2, section 6 of the Transport Code (the Emergency Response Centre Administration as the eCall service operator and the Finnish Transport Safety Agency as the operator of the Digiroad and Digitraffic services).

The banking sector and financial market infrastructures

With regard to the essential infrastructure of the Finnish banking sector and the financial markets, credit institution operations as referred to in he Act on Credit Institutions and engaging in stock-exchange activity as referred to in the Act on Trading in Financial Instruments should be considered essential services under the Network and Information Security Directive.

The Act on Credit Institutions contains comprehensive provisions on obligations associated with operative risk management in credit institution operations, supplemented by the Financial Supervisory Authority's regulation on management of operational risks. With regard to risk management and reporting of disruptions, these obligations can as such be considered to fulfil the obligations of network and information system security for essential services as laid down in Article 14 of the Network and Information Security Directive. These obligations concern all credit institutions operating in Finland.

Stock exchange operations can be considered dependent of network and information as referred to in the Network and Information Security Directive. In addition, significant computer security disruptions to the operations could have a significant disruptive effect on the operation of stock exchange services. Hence, with regard to the infrastructure of the financial markets, a stock exchange should be considered a provider of essential services as referred to in Article 5 of the Network and Information Security Directive.

With regard to engaging in stock market operations, provisions concerning risk management obligations and reporting of disruptions are included in the government proposal to Parliament made on 26. October on acts on amending the Act on Investment Services and the Act on Trading in Financial Instruments and on certain acts related to them (government proposal 151/2017 vp), chapter 3 (sections 1 and 2.2). These obligations fulfil the network and information system security obligations for essential services as laid down in Article 14 of the Network and Information Security Directive.

Health sector

Electronic processing of healthcare customer information and maintenance and operation of healthcare equipment in the provision of public and private social welfare and healthcare services would be considered essential services as referred to in the Network and Information Security Directive.

The Act on the electronic processing of customer information in social welfare and healthcare and the Act on healthcare equipment and materials lay down obligations on the computer security of systems intended for the processing of customer information and requirements on healthcare equipment and obligations on reporting disruptions to the supervisory authority. With regard to risk management and reporting of disruptions, these obligations can as such be considered to fulfil the obligations of network and information system security for essential services as laid down in Article 14 of the Network and Information Security Directive.

Drinking water supply and distribution

Water supply could be considered an essential service for societal activities as referred to in point (2), Article 5, item a, of the Network and Information Security Directive with regard to supply and distribution of drinking water. Under the Water Services Act, water utilities are responsible for the water services of communities. All water utilities can be considered dependent of network and information as referred to in the Article 5(2)b of the Network and Information Security Directive. However, all incidents impacting water utilities cannot be considered to have the significant disruptive effect referred to in Article 5(2)c of the Network and Information Security Directive. On the basis of the criteria in Article 6 of the Network and Information Security Directive, providers of essential services would be water utilities that supply at least 5000 cubic metres of water per day. Computer security disruptions affecting such services would always have the effect referred to in the Network and Information Security Directive. There are an estimated 40 water utilities in Finland that supply at least 5000 cubic metres of water per day and their customers include more than half of the Finnish population. In addition, theses utilities have been categorised as critical to emergency supply.

Security risk management obligations of water utilities concerning the supply and distribution of drinking water are laid down in the Water Services Act. The obligation to make preparations laid down in section 15a of the Water Services Act can be considered to also include risks associated with communications networks and data systems. With regard to risk management obligations, these obligations can be considered to directly fulfil the obligations of network and information system security for essential services as laid down in Article 14 of the Network and Information Security Directive. In contrast, the Water Services Act does not include an obligation to notify the supervisory authority of disruptions to the computer security of systems and hence a separate obligation should be added to the Act concerning water utilities that supply at least 5000 cubic metres of water per day.

Digital Infrastructure

The maintenance of a TLD name registry could be considered an essential service to societal activities as referred to in the Network and Information Security Directive. The Information Society Code also obliges maintainers of TLD registries to ensure computer security. Under the Code, the Finnish Communications Regulatory Authority is the authority maintaining the fi TLD registry. The Government of Åland maintains the ax TLD registry. The obligations laid down in the Information Society Code can be considered to meet the obligations of network and information system security for essential services as laid down in Article 14 of the Network and Information Security Directive.

Proposals:

1.

Act

on amending the Information Society Code

In accordance with the decision of Parliament,

section 275, section 304(1)(7) and (10), section 313(2)(2), section 304 as it partly stands in the Act (456/2016) of the Information Society Code (917/2014) are *amended*, and

a new section 247a, new subsection 3 to section 304, a new subsection 2 to section 308, whereby current subsections 2-4 become subsections 3-5, sections 308 and 318 as they partly appear in the Act (456/2016) are *added* as follows:

Section 247a

The obligation of operators of online marketplaces, search engine services and cloud services to ensure computer security

Operators of online market places, search engine services and cloud services must ensure that the computer security risks associated with the communications networks and information systems that they use are managed. Risk management must consider the following:

1) the security of systems and facilities;
2) the processing of computer security threats and disruptions:
3) business continuity management;
4) supervising, auditing and testing; and
5) compliance with international standards.

The risk management objective referred to above in subsection 1 does not apply to micro and small enterprises referred to in point (11) of Article 16 of the Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

Section 275

Disruption reports made to the Finnish Communications Regulatory Authority

Telecommunications operators must immediately report to the Finnish Communications Regulatory Authority of computer security incidents that affect or threaten their service and any other events that prevent the functioning of a communications service or materially disrupts it. A telecommunications operator must also report the estimated duration and effects of a disruption or threat thereof, corrective measures and the measures that will be taken to prevent the re-occurrence of the disruption. The Finnish Communications Regulatory Authority will submit an annual sum-

mary report of the reports to the Commission and the European Union Agency for Network and Information Security.

Providers of online marketplaces, search engine services and cloud services as referred to in section 247a of this Act must immediately report to the Finnish Communications Regulatory Authority of significant disruptions to the computer security of their service.

If announcing the disruptions is in the general interest, the Finnish Communications Regulatory Authority can oblige the service provider to announce the matter or, after consulting the party obliged to report, announce it itself.

The Finnish Communications Regulatory Authority may issue more detailed regulations on when a disruption referred to in subsection 1 is significant and on the content, form and delivery of the reports and announcements referred to in subsections 1 and 2.

The Finnish Communications Regulatory Authority must evaluate whether a disruption as referred to in subsection 2 concerns other EU Member States and if necessary, notify any Member State that is concerned.

Section 304

Special duties of the Finnish Communications Regulatory Authority

In addition to what is laid down elsewhere, it is the duty of the Finnish Communications Regulatory Authority to:

— —

7) collect information on computer security incidents and threats thereof to online services, communication services, added value services and information systems and on the faults and disruptions of communication networks and communication services;

— —

10) investigate computer security incidents and threats thereof to online services, communication services, added value services and information systems;

— —

Section 308

Co-operation between different authorities

— —

The Finnish Communications Regulatory Authority must co-operate with other Member States' authorities that supervise network and computer security, CIRTs and the Cooperation Group referred to in Article 10 of the Network and Information Security Directive. The Finnish Communications Regulatory Authority will submit an annual summary report referred to in point (3) of Article 10 of Network and Information Security Directive to the Cooperation Group.

Section 313

Processing of supervision matters at the Finnish Communications Regulatory Authority

— —

The Finnish Communications Regulatory Authority may prioritise its supervisory duties laid down in this Act. The Finnish Communications Regulatory Authority may decide not to investigate a matter if:

— —

2) if the matter has minor significance to the functioning of the communications markets, reliability of communications services or securing undisturbed electronic communications, and the interest of the users of the services or to the risk management of the services referred to in section 247a, the suspicion of fault or negligence notwithstanding;

— —

Section 318

Provision of information by the authorities

— —

Confidentiality provisions and other restrictions to providing information notwithstanding, the Finnish Communications Regulatory Authority is entitled to provide a document it has received or drafted in the process of carrying out its duties and to express the confidential information to the Transport Safety Agency, the Energy Authority, the Financial Supervisory Authority, the National Supervisory Authority for Welfare and Health and the Centre for Economic Development, Transport and the Environment if necessary in order for them to carry out their statutory duties concerning computer security.

— —

_____

This Act enters into force on ___ _____ 201__.

_____

2.

Act

on amending the Aviation act

In accordance with the decision of Parliament,
a new section 128a and b will be *added* to the Aviation act (864/2014) as follows:

Section 128a

Duty to ensure computer security

Providers of air navigation services and operators of airports that are essential to societal activities must ensure the risk management of the communications networks and information systems they use.

The Transport Safety Agency must evaluate the impact of the risk assessment referred to in subsection 1 to aviation safety. Providers of air navigation services and operators of airports that are essential to societal activities must provide the Transport Safety Agency with information that is needed for the evaluation. The Authority may oblige a provider of air navigation services or an operator of an airport that is essential to societal activities to take corrective measures in order to remove a significant risk to aviation safety,

Confidentiality provisions and other restrictions to providing information notwithstanding, the Transport Safety Agency is entitled to provide a document it has received or drafted in the process of carrying out its duties referred to in this section and to express the confidential information to the Finnish Communications Regulatory Authority if it is necessary for them to carry out their statutory duties concerning computer security.

Whether an airport referred to in subsection 1 is to be considered essential to societal activities will be provided by Government decree.

Section 128

Reporting computer security incidents

Providers of air navigation services and operators of airports that are essential to societal activities must immediately report significant computer security incidents concerning systems to the Transport Safety Agency.

If announcing a disruption is in the general interest, the Transport Safety Agency can oblige the service provider to announce the matter or, after consulting the party obliged to report, announce it itself.

The Transport Safety Agency must evaluate whether a disruption as referred to in subsection 1 concerns other EU Member States and if necessary, notify any Member State that is concerned.

The Transport Safety Agency may issue further regulations on the content, form and delivery of the announcement.

———

This Act enters into force on ___ _____ 201__.

_____

3.

Act

on amending the Railway Act

In accordance with the decision of Parliament,
a new section 41a will be *added* to the Railway Act (301/2011) as follows:

Section 41a

Duty to ensure computer security

Infrastructure managers of the state railway and companies providing traffic control services must ensure the risk management of the computer security of the communications networks and information systems that they use.

Operators of the state rail network and companies providing traffic control services must immediately report significant computer security disruptions concerning systems to the Transport Safety Agency.

If announcing a disruption is in the general interest, the Transport Safety Agency can oblige the service provider to announce the matter or, after consulting the party obliged to report, announce it itself.

The Transport Safety Agency must evaluate whether a disruption as referred to in subsection 1 concerns other EU Member States and if necessary, notify any Member State that is concerned.

Confidentiality provisions and other restrictions to providing information notwithstanding, the Transport Safety Agency is entitled to provide a document it has received or drafted in the process of carrying out its duties referred to in this section and to express the confidential information to the Finnish Communications Regulatory Authority if it is necessary for them to carry out their statutory duties concerning computer security.

The Transport Safety Agency may issue further regulations on the content, form and delivery of the announcement.

_____

This Act enters into force on ___ _____ 201__.

_____

4.

Act

on amending the Vessel Traffic Service Act

In accordance with the decision of Parliament,

A new subsection 5 will be added to section 16, a new section 18a will be added to the Act and a new subsection 4 will be added to section 28, as it appears in the Act (1307/2009), as follows:

Section 16

Operating vessel traffic services

— —

VTS authorities must ensure the risk management of the computer security of the communications networks and information systems that they use.

Section 18a

Reporting disruptions to computer security

VTS authorities must immediately report significant computer security incidents concerning their systems to the Transport Safety Agency.

If announcing a disruption is in the general interest, the Transport Safety Agency can oblige the service provider to announce the matter or, after consulting the party obliged to report, announce it itself.

The Transport Safety Agency must evaluate whether a disruption as referred to in subsection 1 concerns other EU Member States and if necessary, notify any Member State that is concerned.

The Transport Safety Agency may issue further regulations on the content, form and delivery of the announcement.

Confidentiality provisions and other restrictions to providing information notwithstanding, the Transport Safety Agency is entitled to provide a document it has received or drafted in the process of carrying out its duties referred to in this section and to express the confidential information to the Finnish Communications Regulatory Authority if it is necessary for them to carry out their statutory duties concerning computer security.

Section 28

Supervision

— —

The Transport Safety Agency must evaluate the impact of the risk assessment referred to in section 16, subsection 5 to maritime navigation safety. The Transport Safety Agency may oblige measures to be taken to remove a significant risk to the safety of maritime navigation. A penalty payment may be imposed to enhance the obligation. Penalty fines are prescribed on in the Act on Penalty Payments (1113/1990).

— —

———

This Act enters into force on ___ _____ 201__.

_____

5.

Act

on amending the Act on Security Measures on certain Ships and in Ports Serving them concerning port operators

In accordance with the decision of Parliament,

a new section 7e and f will be *added* to the Act on Security Measures on certain Ships and in Ports Serving them Concerning Port Operators (485/2004), as follows:

Section 7e

Port operators' duty to ensure computer security

Operators of ports that are essential to societal activities must ensure the risk management of the computer security of the communications networks and information systems that they use.

The Transport Safety Agency must evaluate the impact of the risk assessment referred to in paragraph 1 to the safety of maritime navigation. The Agency may oblige an operator referred to in subsection 1 to take measures to remove a significant risk to the safety of maritime navigation. A penalty payment may be imposed to enhance the obligation. Penalty fines are prescribed on in the Act on Penalty Payments (1113/1990).

Confidentiality provisions and other restrictions to providing information notwithstanding, the Transport Safety Agency is entitled to provide a document it has received or drafted in the process of carrying out its duties referred to in this section and to express the confidential information to the Finnish Communications Regulatory Authority if it is necessary for them to carry out their statutory duties concerning computer security.

Whether a port referred to in subsection 1 is to be considered essential to societal activities will be provided by Government decree.

Section 7

Reporting computer security disruptions

Operators of ports that are essential to societal activities must immediately report significant computer security disruptions concerning the computer security to the Transport Safety Agency.

If announcing a disruption is in the general interest, the Transport Safety Agency can oblige the service provider to announce the matter or, after consulting the party obliged to report, announce it itself.

The Transport Safety Agency must evaluate whether a disruption as referred to in subsection 1 concerns other EU Member States and if necessary, notify any Member State that is concerned.

The Transport Safety Agency may issue further regulations on the content, form and delivery of the announcement.

_____

This Act enters into force on ___ _____ 201__.

_____

6.

Act

on amending the Act on traffic services

In accordance with the decision of Parliament,
a new section 7 will be *added* to Part III, chapter 2, of the Act on traffic services (320/2017), as follows

Section 7

Port operators' duty to ensure computer security

Operators of intelligent transport systems must ensure the risk management of the computer security of the communications networks and information systems that they use.

Operators of intelligent transport systems must immediately report significant computer security disruptions in their systems that may form a significant safety risk to an intelligent transport system to the Transport Safety Agency.

If announcing a disruption is in the general interest, the Transport Safety Agency can oblige the service provider to announce the matter or, after consulting the party obliged to report, announce it itself.

The Transport Safety Agency must evaluate whether a disruption as referred to in subsection 1 concerns other EU Member States and if necessary, notify any Member State that is concerned.

Confidentiality provisions and other restrictions to providing information notwithstanding, the Transport Safety Agency is entitled to provide a document it has received or drafted in the process of carrying out its duties referred to in this section and to express the confidential information to the Finnish Communications Regulatory Authority if it is necessary for them to carry out their statutory duties concerning computer security.

The Transport Safety Agency may issue further regulations on the content, form and delivery of the announcement.

_____

This Act enters into force on ___ _____ 201__.

_____

7.

Act

on amending the Electricity market act

In accordance with the decision of Parliament,
section 62 of the Electricity market act (588/2013), as it appears in the Act (590/2017), will be *amended*, and
a new section 29a will be *added* to the Act as follows:

Section 29a

system operators' duty to ensure computer security

System operators must ensure the risk management of the communications networks and information systems that they use.

System operators must immediately report to the Energy Authority any significant data security disruption affecting its system that may lead to an interruption of a significant scale in electricity supply in the distribution system.

If announcing a disruption is in the general interest, the Energy Authority may oblige the service provider to announce the matter or, after consulting the party obliged to report, announce it itself.

The Finnish Communications Regulatory Authority must evaluate whether a disruption as referred to in subsection 2 concerns other EU Member States and if necessary, notify any Member State that is concerned.

The Energy Authority may issue further regulations on the content, form and delivery of the announcement.

What is laid down in subsections 1 and 2 above will not apply to the operators of high-voltage distribution systems whose electricity system is not connected to a distribution system.

Section 62

Special provisions on closed distribution systems

Subsections 23 and 26a, subsection 3 of section 27, sections 28, 29, 29a, 50-53, 53a, 54-57, 57a, 58 or 59 will not apply to closed distribution systems and operators of such systems.

_____

This Act enters into force on ___ _____ 201__.

_____

8.

Act

on amending the Natural gas market act

In accordance with the decision of Parliament,
a new section 34a will be *added* to the Natural gas market act (add number) as follows:

Section 34a

Transmission network operators' duty to ensure computer security

Transmission network operators must ensure the risk management of the communications networks and information systems that they use.

Transmission network operators must immediately report to the Energy Authority any significant data security disruption affecting its system that may lead to an interruption of a significant scale in natural gas transmission in the transmission network. If announcing a disruption is in the general interest, the Energy Authority may oblige the service provider to announce the matter or, after consulting the party obliged to report, announce it itself.

The Finnish Communications Regulatory Authority must evaluate whether a disruption as referred to in subsection 2 concerns other EU Member States and if necessary, notify any Member State that is concerned.

The Energy Authority may issue further regulations on the content, form and delivery of the announcement.

_____

This Act enters into force on ___ _____ 201__.

_____

9.

Act

on amending the Act on supervising the electricity and natural gas markets

In accordance with the decision of Parliament,

section 28, the heading, initial sentence and paragraph 1 of subsection 1, and subsections 2 and 3 of section 28, of the Act on supervising the electricity and natural gas markets (590/2013) will be *amended* as follows:

Section 27

Supervisory co-operation between the authorities

With regard to matters that fall within the scope of its competence, the Energy Authority is entitled to carry out supervision in collaboration with the Financial Supervisory Authority, the Finnish Competition and Consumer Authority, the Finnish Communications Regulatory Authority, the Consumer Ombudsman, the Agency for the Cooperation of Energy Regulators, supervisory authorities of other ETA member states and the European Commission and provide executive assistance on request in their supervisory or inspection duties concerning electricity or natural gas sector enterprises.

Section 28

The right of the Energy Authority to provide information to other authorities

In addition to what is laid down in the Act on the Openness of Government Activities (621/1999), the Energy Authority is entitled, confidentiality provisions notwithstanding, to provide information:

1) the Financial Supervisory Authority, the Finnish Competition and Consumer Authority and the Consumer Ombudsman as needed in their duties, and to the Finnish Communications Regulatory Authority if necessary in order to carry out duties related to computer security;

— —

The Energy Authority is entitled to provide only information that is needed by the authority in question to carry out its duties, and if information is provided to a foreign authority or an international body, the corresponding obligation to confidentiality shall apply to them with regard to the information in question as is the Energy Authority.

The Energy Authority may not disclose information it has received from a foreign authority or an international body to another party unless the providing authority has granted its express consent to this. Such information may only be used to carry out duties in accordance with this Act or for the purposes for which the consent has been given.

_____

This Act enters into force on ___ _____ 201__.

_____

10.

Act

on amending the Water Services Act

In accordance with the decision of Parliament,
a new section 15b, and a new paragraph 3 to subsection 2 of section 35, will be *added* to the Water Services Act (119/2011) as follows:

Section 15b

Reporting computer security incidents

A water utility that supplies at least 5000 cubic metres of water or collects at least 5000 cubic metres of wastewater per day must immediately report to the Centre for Economic Development, Transport and the Environment of significant computer security disruptions affecting the communications and information networks that it uses.

If announcing a disruption is in the general interest, the Centre for Economic Development, Transport and the Environment can oblige the service provider to announce the matter or, after consulting the party obliged to report, announce it itself. The Finnish Communications Regulatory Authority must evaluate whether a disruption as referred to in subsection 2 concerns other EU Member States and if necessary, notify any Member State that is concerned.

The provisions of subsection 1 and 2 on water utilities will also apply to plants that supply water to water utilities.

The Ministry of Agriculture and Forestry may issue more detailed regulations on the content, form and delivery of the announcement.

Section 35

Obligation to confidentiality

— —

The obligation to confidentiality laid down in the Act on the Openness of Government Activities notwithstanding, information gained in the process of carrying out the duties as referred to in this Act on the financial standing, business or trade secrets of an individual or a corporation or the private circumstance of an individual may be provided to:

— —

3) the Finnish Communications Regulatory Authority if necessary for the carrying out of duties related to computer security.

———

This Act enters into force on ___ _____ 201__.

THIS IS AN UNOFFICIAL ENGLISH SUMMARY OF THE PROPOSALS, THE OFFICIAL PROPOSAL CAN BE FOUND IN FINNISH AND IN SWEDISH HERE:
http://valtioneuvosto.fi/paatokset/paatos?decisionId=0900908f8057a85c

11.

Act

on amending the Act on the Financial Supervisory Authority

In accordance with the decision of Parliament,
a new section 50n and section 52a will be *added* to the Act on the Financial Supervisory Authority

Section 50n

Operating as a competent authority as referred to in the Network and Information Security Directive

The Financial Supervisory Authority operates as a competent authority as referred to in point (1) of Article 8 of the Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union with regard to the sectors 3 and 4 referred to in Annex II of the Directive.

Section 52a

Co-operation and exchange of information in carrying out duties as referred to in the Network and Information Security Directive

The Financial Supervisory Authority must co-operate with the Finnish Communications Regulatory Authority and other relevant authorities in carrying out the duties referred to in the Network and Information Security Directive. For this purpose, the Financial Supervisory Authority is entitled to provide information to the Finnish Communications Regulatory Authority and other relevant authorities, confidentiality provisions notwithstanding.

_____

This Act enters into force on ___ _____ 201__.

_____