Implementation Programme for Finland's Cyber Security Strategy for 2017–2020

Turvallisuuskomitea
Säkerhetskommittén
The Security Committee

Implementation Programme for Finland’s Cyber Security Strategy for 2017–2020

Table of Contents

Introduction

Finland’s first Cyber Security Strategy was published on 24 January 2013 in the form of a Government Resolution. It defined the central objectives and policies for meeting challenges in the cyber domain and for securing its functioning. The Strategy described the vision and strategic policy settings of cyber security and noted that an implementation programme was needed to execute the strategic policy settings and achieve the desired end state of the Cyber Security Strategy Vision. On 11 March 2014 the Security Committee adopted the first Implementation Programme and since then has regularly evaluated the realisation of the Programme.

The new Implementation Programme for 2017–2020 addresses the development of cyber security within the service complex comprising the state, counties, municipalities, the business sector and the third sector in which the individual citizen is the customer. The business community provides most digital services and their cyber security through international service complexes and networks.

Since the publication of the Cyber Security Strategy the operating environment of the cyber domain has changed as a result of new service production models and technologies and the new threats directed at them. According to the February 2017 Government research project “Finland’s cyber security: the present state, vision and the actions needed to achieve the vision” (later: Finland’s cyber security report 2017), the most noteworthy cyber threat trends in recent years have been the growth of ransomware, the exploitation of vulnerabilities, threats against devices as well as hacking business operations or breaches of personal data. Also, hoaxes, phishing, denial-of-service attacks and targeted attacks are still relevant threats. The most attacked branches particularly include the health sector, manufacturing and production, banking and financing, the public administration as well as the transport and haulage sector. We will likely see increasingly sophisticated cyber-attacks and more leaks of information in the future. The volume of devices connected to the network is increasing, which means that future attackers will gain a vast amount of new targets in conjunction with the expansion of the Internet of Things.

Moreover, Finland’s cyber security report 2017 stated that ‘even though in recent years Finland has better grasped the political nature of matters in the cyber domain and the need for political awareness in reaching the Cyber Security Vision, the strengthening of political commitment can still be considered as a goal. Political commitment is also about promoting and communicating the national ambition (Cyber Security Vision) internationally’. According to the report Finland’s international action in cyber related matters needs further strengthening: ‘Finland needs to prepare a distinct “cyber agenda”, i.e. publicly declare the goals it aims to advance in international cooperation’.

On the basis of evaluations provided by administrative branches, the business community, the academia and NGOs the Secretariat of the Security Committee prepared an assessment on the progress of the Implementation Programme for Finland’s Cyber

Security Strategy in January 2016. The assessment emphasised the need to develop strategic management models for cyber security. On 14 March 2016, on the basis of the assessment, the Security Committee decided to update the Implementation Programme for Finland's Cyber Security Strategy as an expression of the national ambition. The ambition will be demonstrated through leadership and by re-allocating resources.

The first Implementation Programme for Finland's Cyber Security Strategy, adopted in 2014, comprised altogether 74 measures assigned to ministries and, partly, to individual actors. The assessment identified significant impacts resulting from the following measures:

- The Government Security Network (TUVE) project and the development of sector-independent ICT tasks,
- The National Cyber Security Centre established at the Finnish Communications Regulatory Authority (FICORA) and the development of associated CERT activities,
- The Development Project for the Central Government 24/7 Information Security Operations (SecICT) and the related improvement of monitoring and warning,
- The Development Project for Jyväskylä Security Technology (JYVSECTEC), and
- Cyber security courses organised by the National Defence Training Association of Finland.

As a consequence of digitalisation and the required change management, business intelligence, artificial intelligence, robotisation and the Internet of Things, cyber security also plays an increasingly important role in securing society's vital functions in the national and international operating environment. Digitalisation is a cross-cutting theme of the Government Programme and it is being implemented in several different projects. The Public Sector ICT unit at the Ministry of Finance is responsible for implementing the Government Programme's key project "Public services will be digitalised". In this context cyber security is viewed as an enabler of digitalisation; it must be built into all action and services. This will be accomplished by implementing two of the nine principles of digitalisation: "We will build easy-to-use and secure services" and "We will also serve in case of disruptions".

According to the vision of the of the Information Security Strategy for Finland, published by the Ministry of Transport and Communications in 2016, 'the world's most trusted digital business comes from Finland'. Finland is viewed as being in a good position to become known as a competent, successful and reliable country where it is safe to take hold of the opportunities brought about by digitalisation. By developing, offering and testing new models of business services and income generation that are based on the utilisation of digital information, it is possible to foster and accelerate economic growth. It is estimated that this will require trust in the new services, business models and market actors as well as there being a strong grip on the development of information security expertise and market development.

Owing to globalisation and digitalisation, Finland's security environment has rapidly transformed. Along with the changes in the security and operating environment national threats, such as phenomena and undertakings associated with espionage and terrorism, are increasingly occurring in networks. This change also calls for the authorities to have powers that extend to the cyber domain. As a consequence of the new situation Finland, too, has started preparing intelligence legislation in the administrative branches of the Ministry of the Interior and the Ministry of Defence.

The Implementation Programme for 2017–2020 was compiled from recommendations for action gathered during the drafting process. Recommendations were gathered through a targeted request to ministries and government agencies and by arranging interviews and discussions with the scientific and research community, the public administration and the business community. The preparation for the Implementation Programme took into account the strategy documents adopted as Government Resolutions as well as other strategy documents and, when possible, other strategy documents being prepared during the time of the drafting process, such as the updating of the Security Strategy for Society. The selection criteria for the action items were that they promote the achievement of the Vision and comply with the strategic guidelines. The selection emphasised the standpoint of effectiveness, highlighting the individual as a customer of public services, securing the vital functions and cooperation among the public sector, the business community and the scientific and research community. The Implementation Programme gathers together the public sector's wide-ranging and significant internal projects and actions that aim to improve information and cyber security which are to be implemented together with the business community and NGOs. It also brings them into the public view as coherent and properly delegated processes. When the projects and actions are included in the Implementation Programme it is possible to regularly monitor and measure their progress, which also provides a better overall situation picture of cyber security development. The measurement methods must be continually developed, especially as regards monitoring the quality of actions. In addition to the far-reaching measures selected for the Implementation Programme cyber security is also constantly being improved through other administrative branch-specific actions as well as by the work associated with developing cyber and information security and continuity management.

The Implementation Programme is evaluated and measured annually and, in that context, measures can be changed, added or removed. The updating of the Implementation Programme has be prepared in a working group chaired by Pentti Olin, Senior Advisor, Secretariat of the Security Committee and Tuija Kuusisto, Security Manager, Adjunct Professor, Ministry of Finance, Kimmo Rousku, General Secretary of VAHTI, Ministry of Finance, Rauli Paananen, Deputy Director, Finnish Communications Regulatory Authority (FICORA), and Nadja Nevaste, Advisor, Secretariat of the Security Committee as members.

Content of the Implementation Programme 2017–2020

Finland's Cyber Security Strategy defines the Cyber Security Vision as well as ten strategic guidelines according to which the national cyber security will be developed. According to the Vision:

- Finland can secure its vital functions against cyber threats in all situations.
- Citizens, the authorities and businesses can effectively utilise a safe cyber domain and the competence arising from cyber security measures, both nationally and internationally.
- By 2016, Finland is the global forerunner in cyber threat preparedness and in managing the disturbances caused by these threats.

As regards the third item of the vision, the goal set for 2016 will now become a standing goal: Finland will be the global forerunner in cyber threat preparedness and in managing the disruptions caused by them.

According to available international comparisons and evaluations Finland is at present among the top ten countries in terms of cyber security preparedness and the progress of its implementation.

The strategic guidelines of cyber security preparedness are:

1. Create an efficient collaborative model between the authorities and other actors for the purpose of advancing national cyber security and cyber defence.

2. Improve comprehensive cyber security situation awareness among the key actors that participate in securing the vital functions of society.

3. Maintain and improve the abilities of businesses and organisations critical to the vital functions of society as regards detecting and repelling cyber threats and disturbances that jeopardise any vital function, along with their recovery capabilities, as part of the continuity management of the business community.

4. Make certain that the police have sufficient capabilities to prevent, expose and solve cybercrime and those that benefit from it.

5. The Finnish Defence Forces will create a comprehensive cyber defence capability for their statutory tasks.

6. Strengthen national cyber security through active and efficient participation in the activities of international organisations and collaborative fora that are critical to cyber security.

7. Improve the cyber expertise and awareness of all societal actors.

8. Secure the preconditions for the implementation of effective cyber security measures through national legislation.

9. Assign cyber security related tasks, service models and common cyber security management standards to the authorities and actors in the business community.

10. The implementation of the Strategy and its completion will be monitored.

The Implementation Programme is divided into three topics which address the following issues:

1) **Leadership will ensure that the Cyber Security Vision is achieved**
What kind of management and steering structures, models and legislation should be created to achieve the Cyber Security Vision? What kind of models for compiling and disseminating joint situational awareness among the public administration, the business community and NGOs should be established and developed?

2) **Society's vital digitalised functions will be assured**
What kind of far-reaching administrative and technological actions are needed to retain confidence in the cyber domain in normal conditions, during disruptions in normal conditions and emergency conditions?

3) **The cyber competence of citizens, the business community and the public sector will contribute security to digitalisation**
What kind of curricula for developing expertise should be available to citizens, the business community and the public administration? Who will provide the curricula and generate scientific information?

The following matrix describes the action items of the Implementation Programme, complying with the strategic guidelines. They are grouped along the lines of the Programme's three topics.

	Action/Guideline	1	2	3	4	5	6	7	8	9	10
1	Strategic leadership will be defined	x			x	x	x			x	
2	The leadership model for state cyber security will be established and organised	x	x	x							
3	The public administration's major cyber security incident management model will be implemented and active	x	x	x	x	x				x	
4	The public administration's strategic information and cyber security guidelines will be confirmed	x		x						x	
5	Finland will actively and effectively participate in international cyber security cooperation				x	x	x				
6	Finland's cyber security forum will provide a collaborative platform for the public administration, the business community and the academia	x	x				x			x	x
7	Instruments for monitoring the progress of the Implementation Programme will be established									x	x
8	The preconditions for influencing the cyber domain will be secured					x					
9	The provision of sufficient and relevant information to the state leadership as regards countering threats to national security will be assured	x	x			x			x		
10	The preconditions of fighting cybercrime will be assured				x						
11	Legislation on information security and data protection will be clarified and amended, and the EU's general data protection regulations will be enacted in national legislation								x		
12	The digital services of the public sector and the needed infrastructure, indispensable for the vital functions of society, will be identified and under control			x	x	x	x			x	

	Action/Guideline	1	2	3	4	5	6	7	8	9	10
13	The continuity of functional processes as well as information and cyber security will be assured in the health, social services and regional government reform			x						x	
14	The Government will have access to solutions and services for telecommunications, information management as well as preparedness and readiness management in all security situations		x	x	x	x	x				
15	The integrity and availability of critical basic registers and information resources will be assured in all security situations			x							
16	Electricity supply management and power distribution to society's key targets will be assured to the sufficient level			x							
17	Cyber security will improve among businesses critical to the security of supply			x							
18	Data protection and cyber and information security for elections will be studied								x	x	
19	The preparedness arrangements and disruption management of systems and processes associated with taxation, budget proposals, the state's funding and payments will be improved		x	x						x	
20	A limited national cyber security audit with which organisations can make certain that they achieve the minimum security level will be prepared							x		x	
21	A secure growth environment will be created for digital business	x	x	x	x		x	x	x	x	
22	Training and exercises will be planned and carried out	x	x				x	x			

I Leadership will ensure that the Cyber Security Vision is achieved

Finland's cyber security report 2017 states that: 'The research strongly highlighted the ambiguity and lack of comprehensive cyber security which encompasses and amalgamates the different cyber functions of the whole of society. In conclusion, it can be said that clarifying and strengthening strategic management is essential in order to ensure the achievement of Finland's Cyber Security Vision.'

1) Strategic leadership will be defined

Associated with strategic guidelines: 1,4,5,6,9

Responsibility: Secretariat of the Security Committee, Prime Minister's Office, Ministry of Finance and other required actors

Implement a project which defines the clarification and strengthening of strategic management in cyber security. The project will also take into account the realisation of the crisis management model during information security incidents.

2) The leadership model for state cyber security will be established and organised

Associated with strategic guidelines:1,2,3

Responsibility: Ministry of Finance

The Ministry of Finance will create a new framework for the central government's cyber security management as part of the implementation of the Financial Administration 2020 Project.

3) The public administration's major cyber incident management model will be implemented and active

Associated with strategic guidelines: 1,2,3,4,5,9

Responsibility: Ministry of Finance, Ministry of Transport and Communications, Government ICT Centre (Valtori)

Finland's cyber security report 2017 states that: 'In recent years Finland has developed a cyber security situation picture as well as an exchange of information compiled by different actors. However, improving the exchange of information and detection are still areas of cyber security in which Finland needs to improve. It is also important to actively disseminate, for example, situational awareness on identified vulnerabilities among different actors, and to confidentially report possible data breaches so as to prevent similar data breaches elsewhere in society.'

Valtori, led by the Ministry of Finance and working together with the Ministry of Transport and Communications, FICORA and other actors, will plan a further operational version of an intersectoral virtual incident response team (VIRT). It will include a description of information flows and operating processes between the public administration and the business community during significant information security incidents and information security deviations involving the central government. A research project for developing the cyber situation picture and analysis capability will be implemented.

As regards actors that do not have the obligation to notify of violations of information security pursuant to the directive on network and information security (NIS), the Ministry of Finance will ensure that ministries, administrative branches and service centres as well as counties and municipalities, and the businesses owned by them, will notify of any information security incidents and information security deviations involving the public administration to FICORA. The obligation to notify must be included in contracts signed with subcontractors. The Ministry of Finance will provide more detailed guidelines on the obligation. In addition, contractually based preparedness arrangements with the private sector will be implemented.

4) The public administration's strategic information and cyber security guidelines will be confirmed

Associated with strategic guidelines:1,3,9

Responsibility: Ministry of Finance

The Ministry of Finance will appoint the Government Information Security Management Board (VAHTI) for the 2017–2019 period. VAHTI will handle and harmonise all essential strategic policy guidelines of information security for the public administration. Moreover, the Ministry of Finance will assess the need for and the possibilities of reviewing the present information security legislation. VAHTI will submit annual progress reports.

5) Finland will actively and effectively participate in international cyber security cooperation

Associated with strategic guidelines:4,5,6

Responsibility: Ministry for Foreign Affairs and other ministries within their administrative branches

Finland will actively influence the handling of international cyber security issues within the scope of the EU, the UN, the OSCE, NATO, the OECD, the Council of Europe and other key organisations, as well as bilaterally. The Ministry for Foreign Affairs has the key role in identifying foreign and security policy aspects in questions associated with the cyber domain.

For its part, the Ministry for Foreign Affairs coordinates Finland's positions in international forums on matters involving the cyber domain. The Ministry for Foreign Affairs will also help advance the international prospects of Finnish cyber security companies as part of export promotion and internationalisation.

6) Finland’s cyber security forum will provide a collaborative platform for the public administration, the business community and the academia

Associated with strategic guidelines:1,2,6,9,10

Responsibility: Secretariat of the Security Committee

Finland’s cyber security forum strives to improve cooperation and exchange of information among the scientific and research community, the public administration, businesses and NGOs. The forum monitors the progress of the Cyber Security Strategy and this Implementation Programme and evaluates their up-to-datedness. In addition to the members of the Security Committee, the forum will invite professors of cyber security as well as CEOs and presidents of NGOs to its events. The forum will receive reports on the progress of the Implementation Programme, Finland’s cyber security situation and the results of research projects.

7) Instruments for monitoring the progress of the Implementation Programme will be established

Associated with strategic guidelines:9,10

Responsibility: Secretariat of the Security Committee and the Ministry of Finance

The implementation of cyber security is being monitored through presently existing instruments. The Secretariat of the Security Committee and the Ministry of Finance will carry out a research project to create an updated maturity model and instrumentation for the purpose of monitoring the status of Finland’s cyber security and the achievement of the goals of this Implementation Programme. The maturity model and the instruments will be used to provide regular reports on the status of the Programme to the Security Committee, the Government, the cyber security forum and other stakeholders. The Implementation Programme will be evaluated annually and in that context measures can be changed, added or removed.

8) The preconditions for influencing the cyber domain will be secured

Associated with strategic guideline:5

Responsibility: Ministry of Defence, Ministry of the Interior

In accordance with the Cyber Security Strategy the Defence Forces will develop and maintain a comprehensive cyber defence capability for their statutory tasks. This also includes a cyber-attack capability. The Ministry of Defence, together with other relevant stakeholders, will determine the process associated with the cyber-attack capability. Among other things, the process entails powers, practices associated with executive assistance, methods for cooperating across administrative branches, the exchange of information among different authorities, lines of authority and legal mandates.

9) The provision of sufficient and relevant information to the state leadership as regards countering threats to national security will be assured

Associated with strategic guidelines:1,2,5,8

Responsibility: Ministry of the Interior, Ministry of Defence, Ministry for Foreign Affairs

In order to meet the changes brought on by digitalisation legislation must be reviewed so as to make it possible for the national security authorities to satisfactorily carry out their statutory tasks. A Government proposal on new intelligence legislation in Finland is presently being prepared. The purpose of the legislation is to make it possible to better respond to changes in the security environment and to new kinds of threats against Finland.

The Ministry of Defence, together with the Ministry of the Interior and the Ministry of Justice, will continue drafting legislative proposals for intelligence in accordance with the Government's guidelines.

10) The preconditions of fighting cybercrime will be assured

Associated with strategic guideline:4

Responsibility: The Police and other authorities

The Ministry of the Interior will see to it that the police and other authorities have sufficient capabilities to prevent, expose and solve cybercrime. The situation picture of cybercrime and the exchange of information will be developed to improve the authorities' joint situational awareness and to guarantee better preparedness for actors in the private sector. Moreover, the police will develop the handling and analysis of digital evidence by means of a quality programme.

11) Legislation on information security and data protection will be clarified and amended, and the EU's general data protection regulations will be enacted in national legislation

Associated with strategic guideline:8

Responsibility: Ministry of Justice, other ministries

The Ministry of Justice, together with other ministries, will incorporate European network and information security directives into national law. Each organisation will implement the requirements of legislative amendments in its action.

II Society's vital digitalised functions will be safeguarded

Finland's cyber security report 2017 states that 'The Finnish networked information society must better identify targets that affect vital functions and critical infrastructure and, in particular, identify the critical services and functions that are indispensable to them and the stakeholders that rely on these critical services and functions. The identification of critical stakeholders and functions in the cyber domain also entails the consideration of "cyber self-sufficiency", i.e. securing a sufficient autonomous capability for maintaining the critical infrastructures. Legislative review is an important subtopic in developing and strengthening state cyber security.'

12) The digital services of the public sector and the needed infrastructure, indispensable for the vital functions of society, will be identified and under control

Associated with strategic guidelines: 3,4,5,6,9

Responsibility: Ministry of Finance, Government ICT Centre Valtori, other service centres and businesses providing services to the public administration

The Ministry of Finance will determine the need for legislative amendments on the central government's shared new digital services and associated technologies. The Ministry of Finance will guide the Government ICT Centre Valtori to implement a control system containing descriptions of the digital services and the interdependencies which are inevitably needed for the vital functions of society. These digital services are included in the national critical infrastructure. The relevant partners in the value chains linking the public administration and the business community will be identified and the security of functional processes will be guaranteed. Critical services and interfaces that the services rely on will be identified.

A research project on describing the critical infrastructure and cyber self-sufficiency as an element of national cyber resilience necessary for society's vital pubic services will be carried out.

13) The continuity of functional processes as well as information and cyber security will be assured in the health, social services and regional government reform

Associated with strategic guidelines: 3,9

Responsibility: Ministry of Social Affairs and Health, Ministry of Finance, Ministry of Interior, other ministries, counties

As a result of the health, social services and regional government reform, counties and service utilities owned by them as well as the companies that provide services, communities, foundations and municipal services form an ecosystem. Its continued functioning, information and cyber security included, is essential to the counties' customers/citizens.

Counties, as well as the ministries within their administrative branches, are responsible for continuity management as well as the information and cyber security of the services they provide and the ICT services they use. This will be achieved through statutory measures and in accordance with the guidelines provided by the Ministry of Social Affairs and Health, the Ministry of Interior, the Ministry of Finance and the other ministries that steer the counties.

Furthermore, the administrative branch of the Ministry of Social Affairs and Health is planning to carry out an extensive study of the present state of cyber security and the required further measures from 2017 onwards. Also, national guidelines for the preparedness and continuity management of social welfare and health will be established during 2017–18.

14) The Government will have access to solutions and services for telecommunications, information management as well as preparedness and readiness management in all security situations

Associated with strategic guidelines: 2,3,4,5,6

Responsibility: Prime Minister's Office

The Prime Minister's Office will harmonise and implement the Government's solutions and services associated with preparedness management, the continuity of which will be guaranteed, as applicable, for all security situations. Ministries will have access to a joint terminal device solution in the Government network that will also be available during disruptions and emergency conditions. Separate solutions, such as the restricted information network of the central government authority, will be used for preparedness and for materials requiring high protection levels.

15) The integrity, availability and confidentiality of critical basic registers and information resources will be assured in all security situations

Associated with strategic guideline:3

Responsibility: Ministry of Finance, Population Register Centre, Ministry of Agriculture and Forestry, National Land Survey of Finland and Finnish Patent and Registration Office

The Ministry of Finance will determine and together with the competent organisations analyse the integrity and availability of information resources in all security situations. The assessment will take into account the availability of data and the required technology as well as the required encryption of classified information. The goal is to ensure access to key information resources and their integrity to all organisations in compliance with the classification criteria.

16) Electricity supply management and power distribution to society's key targets will be assured to the sufficient level

Associated with strategic guideline:3

Responsibility: Ministry of Economic Affairs and Employment

In accordance with the energy and climate strategy, a sufficient level of security of electricity supply at the national level will be ensured. The joint criteria for prioritising customers as regards power distribution during disruptions will be determined, taking especially into account the growth of increasingly ICT critical systems.

17) Cyber security will improve among businesses critical to the security of supply

Associated with strategic guideline:3

Responsibility: National Emergency Supply Agency

The National Emergency Supply Agency (NESA) manages and allocates resources to the CYBER 2020 programme which improves cyber security among businesses critical to the security of supply. The programme amalgamates all actions of NESA in the area of cyber security and creates permanent structures for developing and supporting cyber security in the long term. CYBER 2020 will commit key cyber security expert organisations to the coordination and implementation of the programme in the long term. From 2016–2020 NESA will allocate approximately EUR 20 million and 10 person-years to launching the programme and to the first development projects to be financed. This includes the resources that are already earmarked to the National Cyber Security Centre Finland (NCSC-FI) at FICORA.

Moreover, as part of the programme NESA will support a project to create a cyber security glossary using the principles of terminology. The goal of the project is to identify the content assigned to the most important information and cyber security concepts, to build a glossary of the terms, and provide the required recommendations for using the terminology.

Special attention must be paid to harmonising the other measures that supplement the cyber security of companies and the authorities' cyber security development, and to cyber security in the energy sector. NESA will also generate reports on the goals, actions and results of the CYBER 2020 programme as part of the Implementation Programme's annual reporting and monitoring.

18) Data protection and cyber and information security for elections will be studied

Associated with strategic guidelines: 8,9

Responsibility: Ministry of Justice

The Sipilä Government has outlined that electronic voting will be introduced in all elections in Finland as an alternative to traditional ballot voting. The Ministry of Justice will commission a feasibility study on internet voting in general elections and appoint a working group to prepare a report on the possibilities of introducing online voting in Finland. The report will consider the introduction of internet voting, technological options, costs and impacts on the election system. The goal is to complete the report by the end of 2017. The report must pay particular attention to information security and cyber security in elections.

19) The preparedness arrangements and disruption management of systems and processes associated with taxation, budget proposals, the state's funding and payments will be improved

Associated with strategic guidelines: 2,3,9

Responsibility: Ministry of Finance

The continuity of digital processes used in taxation as well as the preparation of the general government fiscal plan, spending limits and the budget, and supporting ICT systems as well as the availability of information needed in the processes will be assured in all security situations and at all workplaces. When it comes to the state's funding and payments, cooperation and preparedness management will be strengthened and the preconditions for the effective management of disruptions will be improved.

a) The capability to monitor and counter cyber-attacks and cybercrime against the state's funding and payments processes and systems will be improved.

Responsibility: Ministry of Finance, Ministry of Interior, State Treasury, Finnish Government Shared Services Centre for Finance and HR (Palkeet)

The State Treasury will conduct a preliminary study (2016–2017) on developing cyber resilience for the state's funding and payments processes. A more detailed proposal will be prepared in 2017 on the basis of the results as regards developing the required administrative and technological functions for different actors and processes.

b) The preparedness of electronic processes and ancillary ICT systems needed in taxation will actively be developed.

Associated with strategic guidelines: 2,3,9

Responsibility: Ministry of Finance, Tax Administration

The Tax Administration will plan and execute the development of preparedness expertise for electronic processes and ancillary ICT systems.

20) A limited national cyber security audit with which organisations can make certain that they achieve the minimum security level will be prepared

Associated with strategic guidelines: 7,9

Responsibility: JAMK University of Applied Sciences

The FINCSC (Finnish Cyber Security Certificate) operating model, built in the Cyber Scheme Pilot in Finland at the JAMK (Jyväskylä) University of Applied Sciences, is particularly designed for SME cyber security assessment and accreditation and further development. The introduction of the model will be promoted and supported by means of national action.

III Cyber competence among citizens, the business community and the public sector will contribute security to digitalisation

Finland's cyber security report 2017 states that 'Cyber security is the enabler of digitalisation. Finland has strong international trust capital and it is essential to utilise this trust and Finnish cyber expertise. Without credible private-sector business in this field Finland cannot be a forerunner in cyber security. In order to achieve the Cyber Security Vision significant extra investments in resources are needed, for example to strengthen the activity of the National Cyber Security Centre.'

21) A secure growth environment will be created for digital business

Associated with strategic guidelines: 1,2,3,4,6,7,8,9

Responsibility: Ministry of Transport and Communication and other ministries

As part of the 2015 action plan for the implementation of the Strategic Government Programme, the Information Security Strategy for Finland, adopted by the Ministry of Social Affairs and Health, will be implemented to boost confidence in the internet and digital practices.

The Information Security Strategy emphasises better competitiveness and export promotion, the development of the EU's digital single market, strengthening the protection of privacy and other basic rights, and fostering innovation. The Strategy aims to achieve a change which results in inbuilt security features in systems, terminal devices and services. The Strategy also obliges the authorities to help communities and citizens to improve their information security.

As part of implementing the Information Security Strategy the following measures, among others, will be seen to:

- Enacting the EU Network and Information Security Directive nationally. The Ministry of Transport and Communications has set up a working group to assess the adequacy of present provisions and the possible need for legislative amendments for each branch of the directive's scope of application.
- Improving the functioning of the National Cyber Security Centre Finland (NCSC-FI) at FICORA: Maintain a cyber security situation picture through the exchange of information based on trust among FICORA, companies and other communities.

22) Training and exercises will be planned and carried out

Finland's cyber security report 2017 states that 'General awareness and knowledge of the basic elements of cyber and information security are considered to be basic civic competences in the present-day digitalised information society in Finland. General awareness of the basic elements of cyber security and incorporating them into everyone's daily routine must be actively improved in Finland. The training of experts requires better coordination between the fragmented education and research that exists among educational establishments as well as extending research even wider.'

a) The competence of the public administration's information and cyber security personnel will be improved

Associated with strategic guideline:7

Responsibility: Secretariat of the Security Committee, Ministry of Finance

The Secretariat of the Security Committee will monitor the effectiveness of cyber security exercises in conjunction with the annual progress reports on the Implementation Programme.

The Ministry of Finance, as part of the VAHTI activities, will plan and execute projects and services for improving the public servants' competence in information and cyber security. The Ministry of Finance, together with the other authorities, will determine the required level of self-sufficiency in cryptology.

b) Citizens will have better information and cyber security skills

Associated with strategic guidelines: 7

Responsibility: National Defence Training Association of Finland, Finnish Association for the Welfare of Older People

The National Defence Training Association of Finland will annually organise a cyber security curriculum which consists of basic courses open to all citizens as well as continuing education and special training for professionals.

The Finnish Association for the Welfare of Older People will create a national peer-to-peer learning model intended for senior citizens and extend it to those that need it. This model will maintain and disseminate general learning methods on information technology for the aged on a nationwide basis. One of its syllabi will focus on information security and cyber issues so that older people can safely carry out online transactions (telemedicine, pharmacy, online banking, etc), and that interest in e-services, as well as an awareness of their associated risks, would increase among the elderly.

c) A national information and cyber security week will be organised annually

Associated with strategic guidelines: 6,7

Responsibility: Confederation of Finnish Industries, Ministry of Finance, Secretariat of the Security Committee

The Confederation of Finnish Industries together with the Ministry of Finance, companies and the Secretariat of the Security Committee will organise a national information and cyber security week every October as part of the European Cyber Security Month (ECSM). During the week information and cyber security will be communicated to citizens, companies and the public administration by means of information plugs and events. The week will culminate in the national information and cyber security day.

d) Basic skills in cyber security and the digital environment – general education and professional training will progress

Associated with strategic guideline:7

Responsibility: Ministry of Education and Culture, Finnish National Agency for Education

As a part of multiliteracies, teachers' continuing education will develop and advance contents associated with information and cyber security. By producing supplementary materials the Finnish National Agency for Education will advance multiliteracies as well as the basic skills of information and cyber security.

e) Cyber security research will improve collaboration among the authorities, research organisations and the business community

Associated with strategic guidelines: 1,7

Responsibility: Secretariat of the Security Committee

Finland's cyber security report 2017 states that further research is needed at least on the following topics: strategic management of cyber security in Finland (actions 1 and 2); the development of a cyber security situation picture and analysis skills (action 3); and the definition of the vital functions of society, critical infrastructure and cyber self-sufficiency as part of national cyber resilience (action 12).

Cyber security research demands a situation picture and coordination. The Secretariat of the Security Committee, together with other stakeholders, will construct a model for research cooperation.

Preparation group for the Implementation Programme:
Nadja Nevaste, Rauli Paananen, Pentti Olin, Tuija Kuusisto and Kimmo Rousku.

www.turvallisuuskomitea.fi/en