NATIONAL INFORMATION SECURITY STRATEGY PROPOSAL

November 25, 2002

Proposal of the Advisory Committee for Information Security

1 Summary

The development and competitiveness of Finland's information society are largely dependent on the ability to protect the nation's knowledge capital. Rapid technological development, extensive use of IT equipment and networking have brought new information-related risks and threats to the operating environment. This requires *active and anticipatory action* on our part. In the future, simply improving risk management and increasing the level of security will not be enough. Openness must also be improved in order to safeguard development and competitiveness.

In setting up the Advisory Committee on Information Security, the Government emphasized that increasing citizens' and businesses' confidence in the information society as part of everyday life and daily commercial activity will require broad-based cooperation to improve information security. The Government set up the Advisory Committee as a liaison body for citizens, companies, organizations and authorities in issues of information security under normal conditions. The Government excluded from the work of the Advisory Committee all matters concerned with exceptional circumstances in society and with information security within public administration.

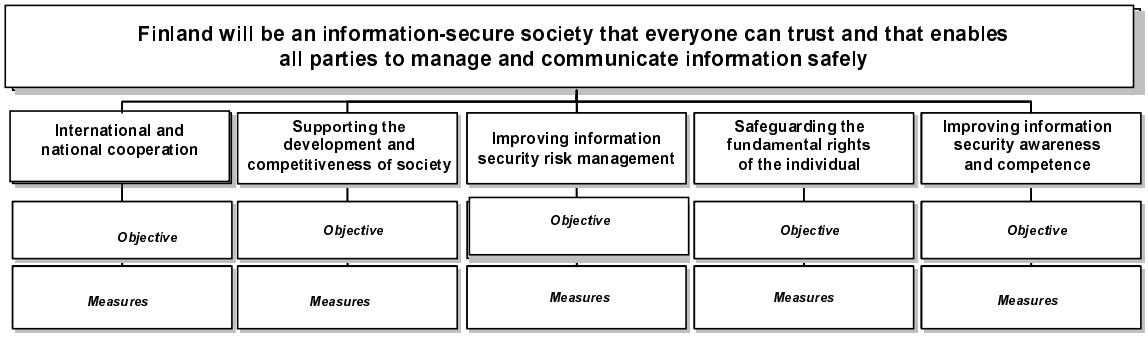
The first stage of the Advisory Committee's work was the publication in June 2002 of the Information Security Review (http://www.ficora.fi). The Review evaluated the most important information security threats affecting Finland and the standard of information security in society in general and for groups using information network services. The Review stated that the standard of information security varies considerably between different sectors and actors. It was also found that significant work on information security has already been carried out in many different fields.

The National Information Security Vision sets out a common goal: *Finland will be an information-secure society that everyone can trust in and that enables all parties to manage and communicate information safely.* Building an information-secure society involves the cooperation of many different actors. To attain the Vision, the following five focus areas will require further attention:

1. *International and national cooperation*
2. *Supporting the development and competitiveness of society*
3. *Improving information security risk management*
4. *Safeguarding the fundamental rights of the individual*
5. *Improving information security awareness and competence*

Our aim is to actively engage in *international cooperation* in order to define the necessary standards and policies. *Nationally,* we will invest in more effective cooperation between actors and in focused development of information security. We will support *the development and competitiveness of society* by promoting the establishment of information-secure procedures, products/services and structures, and by increasing the safe availability and usability of information. Information security must be an essential part of the service to the user. *Information security risk management* will be developed by improving society's ability to cope with disruptions. This will be achieved by advance recognition of information security risks, sufficient monitoring

of the situation and protecting the critical infrastructure. In order to *safeguard the fundamental rights of the individual and other actors*, we will create an operating environment that provides citizens with information security and protection of privacy. We will ensure sufficient information security in all communications and transactions between different actors, and we will support the development of user-friendly information security solutions. We will improve *information security awareness and competence* so that the different actors are conscious of the importance of information security and of its risks. We will also develop the introduction of information-secure procedures and competence in the use of information-secure products/services.



The policies derived from the Vision are translated into objectives in the National Information Security Strategy and further divided into measures. The Advisory Committee for Information Security considers that the Strategy complements existing policies on the development of information security. It also provides a basis for directing resources towards the implementation of the objectives and measures outlined here.

Implementation of the Strategy will begin with existing cooperation frameworks and organizations. The Information Security Strategy is the property of the Government, which is also responsible for its implementation. The Advisory Committee for Information Security has the task of drawing up a proposal for the National Information Security Strategy and of monitoring the implementation of the approved Strategy through the development programme structure. It is also responsible for drawing up regular submissions for updating the Strategy.

In order to ensure that the Strategy is implemented, it is proposed that the Advisory Committee for Information Security continue its work under the next Government. When approving the Strategy the Government shall also determine the way in which its implementation is to be organized.

Helsinki, November 25, 2002

Rauni Hagman, Finnish Communications Regulatory Authority, chairman

Kristiina Laurila, TEKES, deputy chairman

Juhapekka Ristola, Ministry of Transport and Communications, general secretary

Reijo Aarnio, Data Protection Ombudsman's office

Erkki Heliö, TietoEnator Oyj

Ari Hyppönen, F-Secure Oyj

Jari Jokinen, Ministry of Education

Jouni Keronen, Fortum Oyj

Kaarlo Korvola, Ministry of the Interior

Kari Kyttälä, Fujitsu Invia Oy

Lassi Väisänen, Sonera Oyj

Kari Oksanen, Nordea Oyj

Kalevi Tiihonen, Confederation of Finnish Industry and Employers

Tapio Virkkunen, Ministry of Transport and Communications

Kalevi Halonen, Defence Staff

Juha Härkönen, Fortum Oyj

Timo Rinne, SSH Comm. Security Oyj

Petri Kaurinkoski, SSH Comm. Security Oyj

Mikael Kiviniemi, Ministry of Finance

Tero Kuitunen, Ministry of Trade and Industry

Leena Meisalo, Association of Finnish Local and Regional Authorities

Kaisa Nyberg, Nokia Oyj

Liisa Vesanen, OKOBANK Group Central Cooperative

Kari Wirman, Elisa Communications Oyj

CONTENTS

2 Background and objectives

2.1 The Advisory Committee for Information Security and the Information Security Strategy proposal

In setting up the Advisory Committee for Information Security, the Government emphasized that increasing citizens' and businesses' confidence in the information society will require broad-based cooperation to improve information security. The Government set up the Advisory Committee as a liaison body for citizens, companies, organizations and authorities in issues of information security under normal conditions. The Advisory Committee was given the task of monitoring the state of information security and developments in the field in Finland and abroad, promoting the development of information security technology, and improving general awareness of information security. The Government excluded from the work of the Advisory Committee all matters concerning exceptional conditions and information security within public administration.

The first stage of the Advisory Committee's work was the publication in June 2002 of the Information Security Review (http://www.ficora.fi). The Review evaluated the most important information security threats affecting Finland and the standard of information security in society in general and for groups using information network services. The Review stated that the standard of information security varies considerably between different sectors and actors. It was also found that significant work on information security has already been carried out in many different fields. Binding legal provisions on information security have also been in force in some of these fields. In addition, general guidance has been issued by, for example, the Governmental Board of Information Security set up under the Ministry of Finance, the Advisory Committee for Data Management in the Public Administration, and the
National Board of Economic Defence.

As the second stage of its work, the Advisory Committee for Information Security *has drawn up a National Information Security Strategy proposal*. The National Information Security Strategy is subject to approval by the Government.

2.2 The importance of the National Information Security Strategy

2.2.1 Background and definition of information security

The development and competitiveness of the information society and protection of privacy within it in Finland depends largely on the capacity to protect the nation's knowledge capital. The importance of information security has increased now that knowledge, whether possessed by individuals or organizations, has become an essential resource. Rapid technological development and the widespread use of networked IT equipment has generated risks that are difficult to foresee. At the moment, it is even possible to paralyze central functions in society using information networks.[1]

Information security is understood to refer to protecting information, services, systems and communications in whatever form with appropriate measures to manage the risks threatening them. Information security is a concept wider than the technical security of IT and communications technologies. Information security is considered to have been implemented when 1) the confidentiality, 2) the integrity and 3) the availability of information are ensured. Information security is a component of all functions of society. In this Strategy it also covers information and services that may comprise material protected by intellectual property rights.

---

[1] Information security review, May 9, 2002, HM&V Research Oy; *Riskien hallinta Suomessa*, preliminary report, Sitra, 2002; The national strategy to secure cyberspace (for comment), The President's Critical Infrastructure Protection Board, September 2002.

2.2.2 Objectives and delimitation of the National Information Security Strategy

The National Information Security Strategy contains the shared view of Finland's leading information security actors regarding the measures to be implemented to improve information security in Finland. The Strategy sets a goal (Vision) and proposes policies and objectives for achieving that goal. The objectives are further itemized into measures, and the Advisory Committee has the task of ensuring that these measures are implemented. The Advisory Committee considers that in the near future resources should be focused on the implementation of the objectives and measures outlined in this Strategy.[2]

The National Information Security Strategy will not replace the information security policies of public administration or other actors. The Strategy does, however, take account of development work already under way and the existing official guidelines and best practice. The Strategy is conceived as a supportive tool for all actors in society and it presumes that the responsibility for the measures will be widely distributed across the different parties involved. The Strategy is restricted to considering only those areas on which authorities and companies should focus under normal conditions; it does not address issues related to exceptional conditions or information security within public administration.

2.3 Drafting the Strategy

The Strategy was drafted by the Advisory Committee for Information Security in cooperation with Accenture from May 15 to November 25, 2002. First, domestic and international developments in information security were analysed.[3] This analysis identified 'megatrends', which summarize the essential changes in the operating environment.[4]

Seven megatrends affecting information security were identified:[5]

- Globalization and global competition, promotion of integration and transparency (e.g. EU)
- Expansion of networking and interaction
- Greater emphasis on information as a factor of production, and increasingly less balanced distribution of competence and capital
- Changes in (working) life
- Rapidly changing technology and growing dependence on technology
- Growing need for standardization and harmonized regulation
- Changes in methods of doing business and in the related expectations

Threats and opportunities were identified for each of the megatrends. Their likelihood and importance were also evaluated to verify that the trends identified really are of central importance and illustrate well the changes in the operating environment.

Trend analysis was used to identify factors of central importance for information security. The goal (Vision) and policies (Chapter 3, Strategic choices) were formulated on the basis of this. The objectives outlining the policies, and the measures to support these objectives, were then identified. Finally, organization of the Strategy's implementation was outlined (Chapter 4, Strategic objectives and implementation).

---

[2] The responsibilities for the measures, and the timetable for further action, are given in Appendix 2.

[3] The present situation, threats and steps taken were described and analysed in the Information Security Review prepared as background material for the Strategy. (May 9, 2002, HM&V Research Oy).

[4] Sources in Appendix 3.

[5] More than 50 trends were assessed as the basis for identifying megatrends.

3 Strategic choices

3.1 National Information Security Vision

The Information Security Vision sets out succinctly the desired state to be attained by the year 2010:[6]

- **Finland will be an information-secure society that everyone can trust in and that enables all parties to manage and communicate information safely .**

3.1.1 Elaboration of the National Information Security Vision

In Finland, *information security* is considered a component of all functions of *society*; it is not managed or developed as a separate entity. The Information Security Vision focuses on *trust*. Trust here indicates that *information management and communication* in society are functioning as they are expected to. From the user's point of view, the aim is that information security solutions should be transparent and reliable.

The *safe management and communication of information* includes the production, storage, communication, use and deletion of information. The aim is to ensure this for *every actor* in society. This highlights social equality and the fundamental rights of the individual.

3.1.2 Domain of the National Information Security Vision and the roles of actors

The measures undertaken to build an information-secure society (Vision 2010)

In the future, the various actors in society will have roles as both information suppliers and clients (supply and demand of information). Measures under the Strategy will promote the safe management and communication of information through a variety of channels for all actors in society.

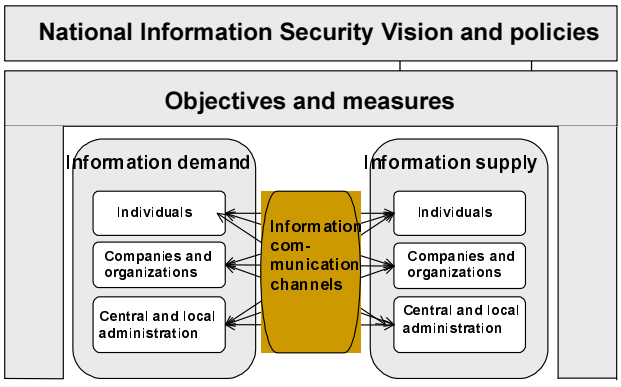


Figure 1. Domain of the Information Security Vision and the roles of actors

3.2 Policies of the information-secure society

Finland as an information-secure society (see Vision on previous page) will require common policies shared by all actors.[7] The following five policies will form the foundation of the information-secure society.

---

[6] The Advisory Committee for Information Security adopted the Vision on August 13, 2002.

[7] The policies enable the joint development of information security by several actors in parallel. The policies were formulated through identification of essential changes in the operating environment ('megatrends') by examining over 50 information security trends.

1. International and national cooperation

Globalization has progressed more rapidly in the production, processing and use of information than in other areas.[8] New IT tools for communicating and managing information support this development. International and national cooperation can influence the emergence of standards and policies, create the necessary common procedures and ensure appropriate roles for various actors. At the national level, the development of information security and cooperation between actors must be actively managed. Particular attention must be paid to publicizing information security.

2. Supporting social development and national competitiveness by improving information security

Converting information and knowledge into capital reinforces the economic importance of information security. Social development and national competitiveness can be boosted by supporting the availability and usability of information. Also, innovative solutions and the identification and development of commercial and/or widely usable applications must be supported.

3. Information security risk management development

Information security risks are becoming increasingly diverse, and wholly new risks and threats continue to emerge. Identifying and managing risks in advance is a requirement for national security. When risks are reliably identified, their adverse effects can be minimized by developing information security. This will focus on anticipation, not reaction. Risk management also requires sufficient and regular monitoring of the national situation.

4. Safeguarding the fundamental rights of the individual and other actors

Among the fundamental rights to be protected are the right to privacy and the protection of confidential messages, freedom of speech and the right to information. An information-secure society will support the freedom of speech of both individual citizens and organizations, the freedom to produce information, and protection of information ownership rights. For companies in particular, essential capital to be protected includes business secrets, client information and product development information.

From the information security point of view, this means that every Finnish citizen must be able to trust that the transmission, processing and recording of his or her information and messages is done confidentially. Information must be protected well enough to avoid it falling into the wrong hands. The process must be so simple that it is available to everyone. Everyone must also be entitled to select user-friendly information security solutions. All actors shall also have easy access to the information that they are entitled to use.[9]

5. Improving awareness of and competence in information security

Competence in information security has become a new civic skill. At the moment, there are shortcomings in the public awareness of and competence in information security.[10] Information security will be developed cost-effectively by investing in competence, and the preconditions for the different actors to function correctly will be improved. Competition will be purposefully improved by expanding the special expertise of information security professionals and developing the information security knowledge of other actors.

The National Information Security Vision and policies are guidelines for all actors in society, who must build on and expand the policy content as required in their own practical work (for example, focusing

---

[8] Other areas being mobility of capital, corporate internationalization, etc.

[9] The publicity and protection of private information is provided for in more detail in the Act on Protection of Privacy and Data Security in Telecommunications and by decree.

[10] Information Security Review, May 9, 2002, HM&V Research Oy; Riskien hallinta Suomessa, preliminary report, Sitra, 2002.

on the meaning of improving information security awareness and competence or developing information security risk management in their own organization).

4. Strategic objectives and implementation

The Vision and policies are shared by all actors. Each policy is further itemized with objectives, which in turn guide practical measures. The objectives are a tool for the responsible authorities[11] to guide and monitor the development of information security and the implementation of the information-secure society set out in the Vision.

4.1 Summary of policies and policy objectives

Table 1 contains a summary of the policies and the objectives corresponding to them.

Policy	Policy objectives
1. International and national cooperation	1. a) Active international cooperation to determine standards and policies; b) strengthen and coordinate cooperation between various actors; and c) manage and support the development of information security matters at the national level.
2. Supporting social development and national competitiveness by improving information security	2. a) Promote and support the formation of information-secure procedures, products/services and structures (development aspect); b) support the availability and usability of information (openness aspect).[12]
3. Developing information security risk management	3. a) Identify risks reliably in advance; b) maintain sufficient and regular monitoring of the national situation and actively publicize the risks; c) minimize risk occurrence and eventual adverse effects of risks; and d) protect the critical infrastructure.
4. Safeguarding the fundamental rights of the individual	4. a) Create an operating environment ensuring information security and protection of privacy for the individual and other actors; b) ensure a sufficient level of information security from the point of view of the individual and other actors in all transactions; and c) support the development of user-friendly information security solutions.
5. Improving awareness of and competence in information security	5. a) Increase awareness of information security so that citizens, companies, organizations and the public administration are conscious of the importance of information security, of information security risks and of their role in combating these risks; b) support competence in the use and development of information-secure procedures and products/services.

Table 1. Policies and objectives.

[11] Overall responsibility for the development of the information-secure society rests with the Government, which owns the Information Security Strategy and is responsible for its implementation. The Advisory Committee for Information Security monitors the achievement of the Strategy through the objectives.

[12] While ensuring the correct identification and classification of the information to be protected.

4.2 Objectives and measures

Implementation of each of the objectives is the responsibility of several actors, ensuring the broad-based implementation of the Strategy in Finnish society. The measures presented here were identified and chosen on the basis of gaining the greatest possible benefit. Some of these measures are already being implemented; closer cooperation will be pursued, and communication further improved. Some of these measures are new, and they will need to be put into action as soon as the Strategy is approved.

Objectives	Action
Objective 1: a) Active international cooperation to determine standards and policies; b) strengthen and coordinate cooperation between various actors; and c) manage and support the development of information security matters at the national level.	• The Government owns the Information Security Strategy and is responsible for its implementation. • The Advisory Committee for Information Security draws up the National Information Security Strategy proposal, monitors the implementation of the approved Strategy and makes proposals for updating the Strategy. • Ensure that the roles and responsibilities of the various actors in developing information security are clear and correspond to the resources available to those actors.[13] • Participate in the preparation of EU legislation and international cooperation (e.g. OECD and international CERT activities, ASEM and other international organizations). Influence the content of international legislation and standards so that they promote information security and safeguard national competitiveness. Promote information exchange between parties. • Ensure sufficient attention to the information security aspect in domestic legislation, standards and instructions from authorities. Establish necessary sanctions and monitoring practices. • Support cooperation between companies and organizations and the creation of competence networks in information security issues.
Objective 2: a) Promote and support the formation of information-secure procedures, products/services and structures (development aspect); b) support the availability and usability of information (openness aspect).[14]	• Ensure that information security aspects are considered in international and domestic projects. • Identify national development and funding programmes and the potential for adjusting their decision-making criteria and evaluation models so as to support information security innovations. • Support and encourage new information security companies and networks to commercialize their information security innovations and disseminate best practices. • Support the extensive use of e-services and e-transactions. • Support the use of reliable and simple encryption and authentication methods. • Found and implement partnership programmes together with actors in the private sector. • Support the compatibility of IT-based processes between the public and private sectors.[15] • Agree on the infrastructures and fundamental technology affecting the functioning of telecommunications.[16]

[13] *Riskien hallinta Suomessa*, preliminary report (Sitra, 2002), highlights this aspect in suggesting '*control structures of the information society of the future*' as a research topic.

[14] While ensuring the correct identification and classification of the information to be protected.

[15] This measure was also proposed in the statement of the Information Industry Committee dated June 12, 2002.

Objectives	Action
Objective 3: a) Identify risks reliably in advance; b) maintain sufficient and regular monitoring of the national situation and actively publicize the risks; c) minimize risk occurrence and eventual adverse effects of risks ; and d) protect the critical infrastructure.	• Ensure potential of authorities and private actors to undertake sufficient information security measures under normal circumstances. • Specify information security risks and identify any new internal and external information security risks.[17] • Actively publicize observed risks and applicable countermeasures. • Maintain sufficient and regular monitoring of the national situation via the information sources and status reports of various actors. • Prepare to combat threats in cooperation with various actors, and correct any shortcomings noted in operating schemes. • Monitor the effectiveness of information security risk management. • Support cooperation between actors responsible for the critical infrastructure.
Objective 4: a) Create an operating environment ensuring information security and protection of privacy for the individual and other actors; b) ensure a sufficient level of information security from the point of view of the individual and other actors in all transactions; and c) support the development of user-friendly information security solutions.	• Ensure the implementation of freedom of speech, confidentiality of communication and protection of privacy — safeguarded by the Constitution — in legislation, standards and official instructions.[18] • Ensure sufficient level of information security in all transactions for the individual. • Ensure that it is possible to protect knowledge capital that is essential in regard to business secrets, client data, product development information and other aspects of a company's operations. • Support the development of anonymous transactions. • Ensure that the electronic services of the public administration and the private sector respect the fundamental rights of the individual. • Actively monitor the observance of fundamental rights. • Support the development of user-friendly and simple information security solutions. • Promote the consumer's potential for making the right choices regarding information security products/services.

[16] This measure was also proposed in the statement of the Information Industry Committee dated June 12, 2002.
[17] *Riskien hallinta Suomessa*, preliminary report (Sitra, 2002) contains a largely similar measure proposal.
[18] Including online communications.

Objective 5: a) Increase awareness of information security so that citizens, companies, organizations and the public administration are conscious of the importance of information security, of information security risks and of their role in combating these risks; b) support competence in the use and development of information-secure procedures and products/services.	• Chart the present situation in information security awareness and competence. Define the objective level and found the projects required to improve competence. • Increase individual awareness of information security issues by distributing relevant information, preparing media campaigns and introducing information security into the curriculum at all levels of education. Disseminate best practices among the various actors. • Improve information security awareness among businesses and particularly among SMEs, in local authorities and in small organizations. Distribute information and offer expertise and services in information security to these actors through a natural service provider network. • Support the media (press, etc.) in communicating factual information and actively provide information security information for distribution.

4.3 Organizing the implementation

Strategy implementation will begin using existing cooperation frameworks and organizations. The Government owns the Information Security Strategy and is responsible for its implementation. The Advisory Board for Information Security draws up the National Information Security Strategy proposal, monitors the implementation of the approved strategy and makes regular proposals for updating the Strategy. Various actors participate in implementing the Strategy. The responsibilities of the Government, the Advisory Committee for Information Security and the other parties involved are defined as follows:

Actors	Responsibilities
Government	• Owns the Information Security Strategy • Is responsible for implementation of the Information Security Strategy
Advisory Committee for Information Security	• Monitors the state and development of the information security field in Finland and internationally • Promotes information security technology development and increases public awareness of information security • Draws up the National Information Security Strategy proposal and makes proposals for updating the Strategy • Monitors implementation of the objectives and measures of the development programme • Makes development recommendations to the responsible parties • Reports to the Government on the implementation of the Strategy • Provides an information security forum for the various actors in society
Owner of development project or measure	• Is responsible for detailed planning of the development project, drawing up a cost-benefit analysis and monitoring the project using agreed indicators • Reports to the Advisory Committee or an objective-specific group appointed by it • Implements the project or guides its implementation • Is responsible for the effectiveness of the project

The Advisory Committee for Information Security will manage the Strategy by means of a development programme in which projects are monitored and guided with the aid of common indicators and procedures. The Advisory Committee reports to the Government.

The development programme will be monitored through objective-specific groups subordinate to the Advisory Committee. The task of these groups is to monitor progress with the measures, to report their conclusions to the Advisory Committee and to disseminate best practices. The groups will draw up proposals for indicators suitable for monitoring measures, and the Advisory Committee will approve them.

Representatives of the municipal sector and various organizations will participate in the activities of the groups in each objective and in implementing the various measures in the manner required for the measures in question. To ensure that the Strategy adequately supports the development of information security in the corporate sector, companies must also actively participate in the activities of the groups, undertake to promote the measures and disseminate the best practices.

Information security development will proceed in the form of parallel projects for which the project owners will be responsible. The project owners will draw up cost-benefit analyses of their projects or measures. Conclusions of these analyses will be presented to the Advisory Committee. On the basis of these results, the measures will be further detailed as necessary, and the overall costs of the development programme assessed. A provisional outline of the parties responsible for the measures is given in Appendix 2.

In order to ensure the implementation of the Strategy, it is proposed that the Advisory Committee on Information Security continue its work during the next Government.

APPENDIX 1: Duties of the Advisory Committee for Information Security

Duties of the Advisory Committee for Information Security
Description and background give in the Decision to appoint the Advisory Committee for Information Security (Government, 1700/04/2001):

The duties of the Advisory Committee for Information Security are in particular:

1. To monitor the state of information security and projects in the field in Finland and to submit proposals for information security measures.
2. To monitor international developments in information security and to submit proposals regarding international developments and cooperation in information security.
3. To increase cooperation between citizens, companies and the authorities with regard to issues of security in communications and IT systems.
4. To draw up a National Information Security Strategy proposal and to monitor its implementation. The Strategy is intended to evaluate the present situation and future developments in the security of telecommunications and IT systems, and to define the central issues that the authorities and companies should address.
5. To promote the improvement of information security technology and competence by proposing measures for enhancing the competitiveness of the industry and the information security cluster.

Finnish citizens, companies and authorities actively use IT and telecommunications technology for acquiring information and for performing transactions. However, the fundamental reform of procedures enabled by the information society has not yet been completed. Full-scale exploitation of information networks and systems requires that citizens, companies and authorities have trust in the tools, actors, procedures and rules of the information society. Information networks and IT systems constantly generate new opportunities for harmful activities, and so information security will play a crucial role in building a dependable information society. At their extreme, such harmful activities could even threaten national security.

The Cabinet Economic Policy Committee and the Committee of Ministries for Public Administration and Regional Development have determined the division of duties regarding information security: the Ministry of Transport and Communications shall be responsible for overall guidance of telecommunications security, and the Finnish Communications Regulatory Authority (FICORA) shall manage the related administrative duties. FICORA shall also be the responsible authority in issues concerning the observation and resolution of information security breaches (CERT duties), together with the police. These decisions also include the decision to set up the Advisory Committee for Information Security.

The Government considers that increasing citizens' and businesses' confidence in the information society as a part of everyday life and commercial activity requires extensive cooperation to improve information security. The Government shall set up the Advisory Committee for Information Security as a liaison body for citizens, companies, organizations and authorities in issues of information security under normal conditions. Issues related to exceptional conditions and to information security within the public administration shall be handled by other bodies.

APPENDIX 2. Measures and provisional outline of responsibilities

The responsibilities for the measures (owners and implementers) and the proposed timetable for their implementation presented here are intended as a basis for further discussion. The *owner* has *administrative responsibility*, while the *implementer* has *responsibility for implementation*.[19] If no single owner was identified, the Advisory Committee for Information Security (ACIS) was entered as owner. The ACIS is responsible for the detailed organization of the measures in the implementation of the Strategy. This means, a) specifying the owners, or b) appointing a working group to prepare the implementation of the measure in question.

The timing of the measures has been entered by quarter (e.g. Q3-04 = 3rd quarter 2004). The measures listed here include only those expected to produce the greatest possible benefit.[20] Added value was evaluated on a scale of one to five (1 = no added value; 5 = vital and urgent), and all measures included here received a high or extremely high evaluation (variation 3–5, average approx. 4).

Objective 1	Measure	Owner	Implementer	Timetable
1. a) Active international cooperation to determine standards and policies; b) strengthen and coordinate cooperation between various actors; and c) manage and support the development of information security matters at the national level.	The Government is the owner of the Information Security Strategy and is responsible for its implementation.	Government	ACIS	Q1-03
	The ACIS will draw up the National Information Security Strategy proposal, monitor the implementation of the approved Strategy, make proposals for updating the Strategy and manage the information security development programme.	Ministry of Transport and Communications	ACIS	Q1-03 (Q4-05 strategy update)
	Ensure that the roles and responsibilities of the actors in information security development are clear and match the resources and potential of the actors Government.	Government	ACIS (sub-committees)	Q4-03

[19] Owners (administrative) and implementers (practical) are distinguished from one another because it was found in the owner analysis that nearly all the measures were concentrated within central government and that there were only isolated cases where a single owner was identified for the implementation.

[20] During the Strategy drafting, the added value of various measures was evaluated. This list only includes those measures that received a high or extremely high evaluation for added value.

	Participate in preparatory work for EU legislation and international cooperation (e.g. OECD, international CERT, ASEM and other international organizations), and influence the content of international legislation and standards so as to promote information security and safeguard national competitiveness. Promote exchange of information between parties.	Government	International legislation preparation work at Ministry of Transport and Communications, Ministry of Justice, Ministry of Education, Ministry of the Interior, Ministry of Finance, Ministry of Trade and Industry, FICORA	Continuous
	Ensure sufficient attention to the information security aspect in domestic legislation, standards and official instructions, introduce necessary sanctions and monitoring procedures.	Government	International legislation preparation work at Ministry of Transport and Communications, Ministry of Justice, Ministry of Education, Ministry of the Interior, Ministry of Finance, Ministry of Trade and Industry, FICORA, Data Security Ombudsman's office	Continuous

Objective 2	Measure	Owner	Implementer	Timetable
2. a) Promote and support the formation of information-secure procedures, products/services and structures (development aspect); b) support the	Ensure inclusion of information security considerations in international and domestic projects	ACIS	Ministries, companies, organizations, TEKES	Immediate and continuous
	Identify national development and funding programmes and revised decision-making criteria and evaluation models that support innovation	Ministry of Trade and Industry	TEKES, Confederation of Finnish Industry and Employers, companies	

availability and usability of information (openness aspect).	Support and encourage new innovative information security companies and networks to commercialize their information security innovations and disseminate best practices	Ministry of Trade and Industry	TEKES, Confederation of Finnish Industry and Employers, companies	
	Support the extensive use of e-services and e-transactions	ACIS	Ministries, companies, organizations, TEKES, employment and economic development centres, Confederation of Finnish Industry and Employers	
	Support the use of reliable and convenient (encryption and) authentication methods	ACIS	Ministries, companies, organizations, TEKES, employment and economic development centres, Confederation of Finnish Industry and Employers	
	Found and implement partnership programmes together with and between leading actors in the private sector	Ministry of Trade and Industry	Ministries, companies, organizations, TEKES, employment and economic development centres, Confederation of Finnish Industry and Employers	
	Support compatibility of IT-based processes between the public and private sectors[21].	ACIS	Ministries and other public sectors	
	Agree on the infrastructures and basic technologies influencing the functioning of telecommunications[22]	ACIS	Ministries and other public sectors	

[21] This measure was also proposed in the statement of the Information Industry Committee, June 12, 2002.
[22] This measure was also proposed in the statement of the Information Industry Committee, June 12, 2002.

Objective 3	Measure	Owner	Implementer	Timetable
3. a) Identify risks reliably in advance; b) maintain sufficient and regular monitoring of the national situation and actively publicize information security risks; c) minimize risk occurrence and their eventual adverse effects of risks; and d) protect the critical infrastructure.	Ensure that authorities and private actors have sufficient potential for ensuring information security under normal conditions	ACIS	FICORA and various actors	Open
	Specify information security risks and identify eventual new internal and external information security risks	ACIS	FICORA and various actors	Open
	Actively communicate information on risks observed and on applicable countermeasures	ACIS	FICORA and various actors	Open
	Maintain sufficient and regular monitoring of the national situation using the sources and status reports of various actors	ACIS	FICORA and various actors	Open
	Prepare to combat threats in cooperation with various actors and rectify any shortcomings observed	ACIS	FICORA and various actors	Open
	Monitor the effectiveness of information security risk management	ACIS	FICORA and various actors	Open
	Support practical cooperation between actors responsible for critical infrastructure	ACIS	FICORA and actors responsible for critical infrastructure	Open

Objective 4	Measure	Owner	Implementer	Timetable
4. a) Create an operating environment ensuring information security and protection of privacy for the individual and other actors; b) ensure a sufficient level of information security from the point of view of the individual and other actors in all transactions; and c) support the development of user-friendly information security solutions.	Ensure the safeguarding of freedom of speech, confidentiality of communication and protection of privacy, as guaranteed by the Constitution, in legislation, standards and official instructions	ACIS	Ministry of Transport and Communications, Ministry of Finance, Ministry of Justice, FICORA, Data Protection Ombudsman's office	Continuous
	Ensure sufficient level of information security for the individual and other actors in all transactions	ACIS	All network service providers (e.g. central and local government, Social Insurance Institution, organizations, companies), Data Protection Ombudsman's office	Open
	Support the development of anonymous transactions	ACIS	All network service providers (e.g. central and local government, Social Insurance Institution, organizations, companies), Data Protection Ombudsman's office	Open
	Ensure that e-services in the public administration and the private sector safeguard the fundamental rights of the individual and other actors	ACIS	All network service providers (e.g. central and local government, Social Insurance Institution, organizations, companies), Data Protection Ombudsman's office	Continuous

	Actively monitor the safeguarding of fundamental rights	ACIS	Ministries in their respective purviews, and authorities with monitoring responsibility	Continuous
	Support the development of user-friendly and simple information security solutions	Ministry of Trade and Industry	TEKES, Ministry of Transport and Communications, FICORA, Confederation of Finnish Industry and Employers, Data Protection Ombudsman's office, service providers, developers of information security solutions	Open
	Promote the consumer's potential for making the right choices regarding information security products/services	Ministry of Trade and Industry	TEKES, Ministry of Transport and Communications, FICORA, Confederation of Finnish Industry and Employers, Data Protection Ombudsman's office, service providers, developers of information security solutions	Open

Objective 5	Measure	Owner	Implementer	Timetable
5. a) Increase awareness of information security so that citizens, companies, organizations and the public administration are conscious of the importance of information security, of information security risks and of their role in combating these risks; b) support competence in the use and development of information-secure procedures and products/services.	Chart the present situation in information security awareness and competence, define objective levels and set up the projects required	Ministry of Education	Schools, universities, other educational institutions, labour market organizations, FICORA, Ministry of Finance, local authority actors	Open
	Increase individual awareness of information security issues by distributing factual information, preparing media campaigns and including information security in the curriculum at all levels of education, disseminate best practices	Ministry of Education	Schools, universities, other educational institutions, FICORA, police, companies, organizations, Data Protection Ombudsman's office, Confederation of Finnish Industry and Employers, local authority actors	Open
	Improve information security awareness in business, particularly in SMEs, local government and small organizations by distributing information and providing knowledge/expertise in information security and services to these actors through a natural service provider network	Ministry of Trade and Industry	Employment and economic development centres, FICORA, Confederation of Finnish Industry and Employers, companies, Finnish Confederation of Private Entrepreneurs, Employers' Confederation of Service Industries (member organizations), local authority actors	Continuous

	Support the media etc. (press etc.) in conveying factual information, and actively provide material on information security	FICORA	Ministry of Finance, Ministry of Transport and Communications, Ministry of the Interior, police, Confederation of Finnish Industry and Employers, Data Protection Ombudsman's office, companies	Open

APPENDIX 3 Sources

Written sources:

The information security guidelines of the Governmental Board of Information Security, www.vm.fi/vahti

- Bulletin from the Ministry of Transport and Communications, October 25, 2001
- *Kohti hallittua murrosta – julkiset palvelut uudella vuosituhannella. Julkisen hallinnon sähköisen asioinnin toimintaohjelma 2002-2003.* (Public administration e-transactions action plan) Advisory Committee for Information Society Issues 2002.
- *Network and Information Security: Proposal for a European Policy Approach,* June 6, 2001. Communication from the EU Commission.
- Government Resolution on State information security, November 11, 1999
- Government Resolution on national emergency supply security
- Information Security Review, May 9, 2002, HM&V Research Oy.
- *Riskien hallinta Suomessa*, preliminary report, Sitra, 2002.
- *The national strategy to secure cyberspace* (for comment), The President's Critical Infrastructure Protection Board, September 2002.
- *OECD Guidelines for the Security of Information Systems and Networks: Toward a Culture of Security.* Organization for Economic Co-operation and Development.
- In-house publications and sources of Accenture

Interviews:

- Bo Harald, deputy manager, Nordea
- Erkki Virtanen, Secretary General, Ministry of Trade and Industry
- Markku Linna, Secretary General, Ministry of Education
- Olavi Köngäs, Chief Information Officer, Ministry of Finance

Work seminars and meetings:

- Meeting of the Advisory Committee for Information Security, June 12, 2002
- Work seminar of the Advisory Committee for Information Security, August 13, 2002
- Meeting of the Advisory Committee for Information Security, September 5, 2002
- Work seminar of the Advisory Committee for Information Security, September 30, 2002
- Meeting of the Advisory Committee for Information Security, October 21, 2002
- Meeting of the Advisory Committee for Information Security, November 25, 2002

APPENDIX 4: Vocabulary

Infrastructure = Considered to consist of the following: 1) energy networks (power stations, transmission grids, gas pipelines); 2) telecommunications networks and IT systems; 3) mass media (digital and print); 4) financing and payment transfers; 5) water supply and civil engineering; 6) transport by road, sea, air and rail; and 7) food supply.[23]

Development programme = A joint control or management mechanism for several projects. In this document, this refers to a tool used by the Advisory Committee for Information Security to implement its Strategy and to monitor the implementation.

Critical infrastructure = Infrastructure that is vital to the functioning of society. Focus areas: communications, data processing and electricity distribution (energy transmission grids).

Risk = Combination of the frequency or probability of a specific dangerous event and its effects.[24] Mathematically, a risk is shown as the product of the probability of the event causing the damage and the magnitude of the damage.

Risk management = The systematic use of management principles, procedures and practices to analyse risks, evaluate their impact and monitor them; systematic risk analysis, evaluation and management measures.[25]

Information security = Refers to the protection of information, services, systems and communications in various forms using measures applicable to managing the risks that threaten them. Information security is considered to have been implemented when the confidentiality, integrity and availability of information has been guaranteed. Information security is thus a broader concept than IT or communications security in the technical sense.

Policy = A principle or guideline to which all actors are expected to conform (guiding principle).

Strategy = A plan of the manner and measures with which the Vision is to be attained.

Vision = The desired state of the nation's information security. A goal that is to be achieved by the year 2010. An expression of a desire that is usually in a non-measurable form.

---

[23] Government Decision, May 8, 2002, based on the goals set for national emergency supply security.
[24] Source: Finnish Standards Association SFS, SFS-IEC 60300-3-9.
[25] Source: Finnish Standards Association SFS, SFS-IEC 60300-3-9.