



Helsinki, 4 September 2003

GOVERNMENT RESOLUTION ON NATIONAL INFORMATION SECURITY STRATEGY

A RESOLUTION ON NATIONAL INFORMATION SECURITY STRATEGY

The National Information Security Strategy aims to increase citizens' and companies' trust in the information society. It gathers up guidelines and measures that can improve information security and protection of privacy. On 4 September 2003, the Government submitted a resolution on the Finnish information security strategy.

According to the Strategy, an information-secure society can be achieved by better national and international cooperation. The operating environment for the Finnish ICT companies and the information security risk management will be improved; the fundamental rights and the nation's knowledge capital will be safeguarded; awareness of and competence in information security will be increased. The Strategy presents the most important measures to achieve these objectives.

Mrs. Leena Luhtanen, Minister of Transport and Communications of Finland, says that we should place the same emphasis on information security as on traffic safety. Security can be fostered through opinion forming, training, cooperation and continuous awareness.

- It means that more breaks and seatbelts need to be installed in "information network vehicles", i.e. services need firewalls and virus protection programmes, Minister Luhtanen says. Attention should also be paid to nuisance traffic on electronic "highways", such as spam email. The Ministry is currently examining how broadband "highways" could reach every household.

The Strategy formulates the efforts of the Government, trade, industry, organisations and private citizens into common information security objectives. On international scale, it is one of the first proposals that concern information security in the whole society.

- The development of information security has lacked a common goal and shared policies. This Strategy brings the actors in the field together and shows the direction, Minister Luhtanen stresses.

The adopted Strategy is an essential part of the Government's information society policy and is closely related to the Entrepreneurship Policy Programme as well. It is based on the proposal for national information security strategy of December 2002 by the Information Security Advisory Board that ended its work in spring 2003. It is proposed in the Strategy that a new advisory board be founded. The Ministry of Transport and Communications will appoint it this autumn.

For further information, please contact:

Mr. Juhapekka Ristola, Ministerial Adviser, tel. +358 9 160 28348, +358 400 788 530,
Email firstname.lastname@mintc.fi

Postal address	Visiting address	Telephone	Telefax
PO Box 31 FIN-00023 Government FINLAND	Eteläesplanadi 16-18 Helsinki	+358 9 160 02	+358 9 160 28596 +358 9 160 28590 (Information)

GOVERNMENT RESOLUTION ON NATIONAL INFORMATION SECURITY STRATEGY

Background

The information society is based on new technology, new procedures and new expertise, the use of which will improve the welfare of citizens, change practices of interaction and social participation, and promote equality and democracy. They will also improve the productivity and competitiveness of companies and open up new markets and business opportunities. For public administration, the information society enables reform of procedures, improvement of client service and conservation of resources.

To exploit the opportunities and eliminate the threats posed by the information society, all actors must have confidence in the course of development. The confidence of citizens and companies in the information society can be increased in particular through improvements in information security and privacy protection. 'Information security' refers to protection of information, services, systems and telecommunications in whatever form. Information security involves features of technical security, behaviour of individuals, procedures of organizations and social conditions.

Threats to information security include breaches of personal privacy, e-mail spam, industrial espionage, pirate copying, computer viruses, network terrorism and electronic warfare. Any of these can spread worldwide in an instant through information networks. But information security also presents opportunities. Properly implemented, it increases an individual's freedom of action, creates new business opportunities and reduces the costs of running a business and of interaction everywhere in society.

The National Information Security Strategy is an important part of the Government's information society policy. Its purpose is to combat threats to information security and to exploit related potential under normal and exceptional circumstances. The Strategy provides a common platform for the information security efforts of the Government, businesses, organizations and individual citizens. However, the Strategy does not affect the existing division of responsibility in information security or existing organizational structures.

The National Information Security Strategy is based on the Strategy Proposal drawn up by the Information Security Advisory Board, which sat from autumn 2001 to spring 2003. The Advisory Board first drafted a survey of the state of information security in Finland. The Strategy Proposal based on this survey was extensively circulated for comment. Those returning statements on the Proposal considered the Strategy an essential document and were of the opinion that its efficient implementation will require a forum for cooperation in the form of an advisory board. Several statements called for further detail and more clarity in the measures proposed. Taking into account the feedback from the first round of comments, the



Ministry of Transport and Communications prepared a draft Government Resolution on the National Information Security Strategy and circulated this for comment to all Ministries and other bodies participating in the work of the Information Security Advisory Board. Most statements noted that the draft Resolution had a satisfactory level of detail and clarity. Moreover, several statements noted that a new advisory board should be set up to ensure implementation of the Strategy and closer cooperation. The draft Resolution has been further revised on the basis of the statements received.

Strategic objectives

The national information security strategy helps Finland become an information-secure society. Objectives of the strategy are to:

1. promote national and international information security cooperation;
2. promote national competitiveness and the operating environment for Finnish information and communication operators;
3. improve information security risk management;
4. safeguard the fundamental rights and protect the nation's knowledge capital; and
5. increase awareness of and competence in information security.

The strategic objectives and the practical measures related to them are discussed below in more detail. They are not presented in order of priority.

Measures

1. Promotion of national and international information security cooperation

The production and use of information through new information and communications technology, unlimited by geographical distance, is the driving force behind globalization. The security implications of these new opportunities constitute a great challenge for authorities, companies, citizens and other actors. The purpose of the National Information Security Strategy is to influence the creation of standards, policy guidelines and cooperation for promoting information security and to ensure that the division of responsibilities between the various actors in the field of information security is clear.

To this end, the following measures will be implemented:

- Appoint a national Information Security Advisory Board, which will support the accommodation of the implementing measures of this Strategy, monitor the implementation of the strategy and make proposals to Government for updating the Strategy. (Ministry of Transport and Communications)

Postal address	Visiting address	Telephone	Telefax
PO Box 31 FIN-00023 Government FINLAND	Eteläesplanadi 16-18 Helsinki	+358 9 160 02	+358 9 160 28596 +358 9 160 28590 (Information)



- Actively participate in the preparation of legislation and standards and other information security cooperation in the European Union (EU), other international organisations and forums in trade and industry. (All parties important for information security.)
- Launch a research project on the importance of trust and information security in the new economy. Use the Finnish banking sector as a case study of investing in information security and of the benefits of such investments. There is an ongoing 'Economics of Trust' project in the OECD. National studies support this, and the project could be used as a channel for distributing Finnish information security practices more widely (Ministry of Transport and Communications, Ministry of Trade and Industry, Ministry of Finance).
- Further develop the functional capacity of national actors in promoting information security and submit proposals for improving this capacity and to enhance cooperation. (All parties important for information security.)

2. Promotion of national competitiveness and improvement of the operating environment for Finnish information and communications operators

Information is becoming an increasingly valuable form of capital thanks to the world-wide market for it. The National Information Security Strategy will ensure the open availability and safe use of information, and thus contribute to new business opportunities and a stable operating environment for companies that produce, use and protect information. This will in turn improve Finland's competitiveness and generate resources that can be used for other development in society.

Promoting the business potential for information security companies will improve national competitiveness and the availability of new diverse information security services.

To this end, the following measures will be implemented:

- Conduct a survey on information security clusters and launch any measures deemed necessary (Ministry of Transport and Communications, Ministry of Trade and Industry)
- Promote the availability and usability of appropriate information security information in companies and other organizations (Ministry of Transport and Communications, Ministry of Trade and Industry, Ministry of Finance and other parties important for information security)
- Use information society policy and technology policy to support innovative development trends related to information security, the formation of expertise networks between companies and organizations, and partnership programmes between public-sector and private-sector actors (Ministry of Transport and Communications, Ministry of Trade and Industry, Ministry of Finance)

- Encourage companies and research institutions to launch new information security products, to develop protection and identification methods that are compatible with other products and easy to use, and to distribute best practices for other actors to use (Ministry of Transport and Communications, Ministry of Trade and Industry)
- Guide public-sector actors to improve the compatibility of processes involving ITC both within the public sector and between the public and private sectors (Ministry of Finance, Ministry of the Interior)
- Perform regular evaluations on the impact of legislation and international agreements pertaining to information security and the information society on communications services, online banking services, electronic identification services, e-commerce and e-transactions in official matters, and submit proposals for action as required (Ministry of Transport and Communications, Ministry of Trade and Industry, Ministry of the Interior, Ministry of Finance)

3. Improve management of information security risks

The safe use of information is an increasingly great challenge for all actors, because the known risks are changing and new threats emerge all the time. The purpose of the National Information Security Strategy is to promote anticipatory identification and management of risks on the level of the individual, the company and society as a whole. Sufficient anticipation guarantees the best possible security and minimizes its costs.

To this end, the following measures will be implemented:

- Create a feasible system for monitoring the national situation in information security risks, maintained by FICORA (Finnish Communications Regulatory Authority) and constantly updated to provide timely information on the national situation to the major actors (Ministry of Transport and Communications, Ministry of Finance, Ministry of the Interior, Ministry of Trade and Industry, Ministry of Defence, National Board of Economic Defence, other parties important for information security)
- Perform regular evaluations of new information security risks and convey information on them and required counter-measures to all actors (Ministry of Transport and Communications, Ministry of Finance, National Board of Economic Defence, other parties important for information security)
- Develop methods for analyzing information security vulnerabilities and distribute the best practices created thereby for use by all organizations (Ministry of Transport and Communications, Ministry of Trade and Industry, other parties important for information security)
- Set up an information security working group for actors responsible for critical infrastructure under the Information Security Advisory Board in order to improve cooperation (Ministry of Transport and Communications, Ministry of



Finance, National Board of Economic Defence, other parties important for information security)

4. Safeguard fundamental rights and national information capital

Building an information society with information security cannot happen at the expense of the fundamental rights and liberties of individuals and other actors. In a secure information society, all actors must be able to trust that their information and messages are relayed, processed and stored with confidentiality and that they will not end up in the wrong hands. Furthermore, everyone must have easy access to information for which they have authorization. For companies, the information capital to be secured include most importantly business secrets, client data and product development data.

To this end, the following measures will be implemented:

- Ensure that freedom of speech, confidentiality of communications, protection of privacy and other fundamental rights are taken into account in the legislation, official instructions and standards relating to information society services, electronic communications and information security, and in e-transactions services provided by public authorities (All authorities)
- Estimate whether the legislation concerning the protection of business secrets, client data, product development data, immaterial rights and other information essential for a company's business should be revised, and submit proposals for new legislation to the relevant authorities (Ministry of Trade and Industry, Ministry of Education, Ministry of Justice, Ministry of Transport and Communications)

5. Increase awareness of and competence in information security

Competence in information security has become a new civic skill. In a secure information society, all actors must be aware of the information security risks of their actions and of their role in preventing these risks. The National Information Security Strategy is intended to raise the level of competence by investing in the expertise of information security professionals on one hand and in the general awareness of information security of all actors on the other.

To this end, the following measures will be implemented:

- Survey the present state of awareness of and competence in information security as broadly as possible (for instance in schools, in workplaces, in the everyday lives of citizens), determine the target level for competence and launch the necessary projects for improving general competence in information security and training for information security professionals (Ministry of Education, Ministry of Trade and Industry, Ministry of Finance, other parties important for information security)



- Increase the awareness of individuals regarding information security issues by distributing factual information, producing info spots and incorporating information security education at all school levels. Distribute best practices for raising awareness to all educational institutions. (Ministry of Education)
- Actively promote awareness of information security among companies, the municipal sector and other organizations (Ministry of Trade and Industry, Ministry of the Interior, Ministry of Finance, Ministry of Transport and Communications, other parties important for information security)
- Contribute to the development and use of quality certificates related to information security and increase user awareness of the importance of certificates in buying products and services (Ministry of Trade and Industry, Ministry of Finance, Ministry of Transport and Communications, other parties important for information security)

Strategy implementation

Basics

Implementation of information security and development of information security is the responsibility of several actors under the current legislation. Under normal conditions, general control and development of information security lies within the purview of the Ministry of Transport and Communications, FICORA (which is supervised by the former), and the Ministry of Trade and Industry. In public administration, control and development of information security is provided for separately. Development of information security in public administration is mainly the responsibility of the Ministry of Finance and the Ministry of the Interior. Electronic communications and information security in telecommunications services lie within the purview of the Ministry of Transport and Communications according to the Government Rules of Procedure (262/2003). The Ministry of Transport and Communications is also charged with control and development of telecommunications under the Communications Market Act section 119 and the Act on the Protection of Privacy and Data Security in Telecommunications (565/1999) section 23. FICORA acts as a national information security authority which under section 21 of the Act on the Protection of Privacy and Data Security in Telecommunications pursues CERT activities and supervises observance of both the Act on the Protection of Privacy and Data Security in Telecommunications and the Communications Market Act. FICORA also supervises information security in telecommunications (COMSEC) and can issue technical directives on regulations involving the Act on the Protection of Privacy and Data Security in Telecommunications and the Communications Market Act. Under the Government Decree on Communications Administration (697/2001) section 1, the duties of FICORA also include coordination and development of standardization in telecommunications and related information security. Under the Government Rules of Procedure, the Ministry of Trade and Industry is responsible for technology policy and technical security.

Postal address	Visiting address	Telephone	Telefax
PO Box 31 FIN-00023 Government FINLAND	Eteläesplanadi 16-18 Helsinki	+358 9 160 02	+358 9 160 28596 +358 9 160 28590 (Information)



Under the Government Rules of Procedure, the purview of the Ministry of Finance includes the general framework of government information management, data processing and information security, official e-transactions and the government's shared information management. Also, under the Act on Electronic Transactions in the Administration (13/2003) section 22, the Ministry of Finance is required to issue more specific instructions on provision of information security in official e-transactions. Under the Government Rules of Procedure, the purview of the Ministry of the Interior includes online transactions and information management between the central government and local authorities; the purview of the Prime Minister's Office includes securing the general operating environment and services needed by the Government.

The information security authorities are required to monitor compliance with the Personal Data Act (523/1999) and information security regulations and to promote good governance, which includes requirements concerning information security. Archiving institutions are required under the Archives Act (831/1994) to secure preservation of documents to be stored permanently and under the Act on Electronic Transactions in the Administration section 22 to issue more specific instructions on the recording and registration of official e-transactions. Other important and active actors involved in information security include the National Bureau of Investigation, the Security Police and other police authorities under the Act on Police Administration (110/1992), as well as Funet CERT and the Finnish Information Society Development Centre (TIEKE). Also, self-regulation by private enterprises and various information security measures implemented by companies are vital to the development and implementation of information security.

Information security cooperation is being pursued in bodies such as the advisory committee on corporate security, a joint body of the Confederation of Finnish Industry and Employers (TT), the Employers Confederation of Service Industries (Palvelutyöntajat) and their member companies. The Advisory Committee on Information Management in Public Administration (JUHTA) is a development forum for joint information management projects of the central government and local authorities. JUHTA aims to harmonize development of the information technology, information management and e-transactions service by the central government and local authorities, and to this end it produces recommendations and instructions related to this field, involving information security among other things. The Steering Committee for Data Security in State Administration (VAHTI) issues instructions concerning information security in the central government.

The information security work carried out under legislation concerning exceptional conditions is also crucial to the development and implementation of information security in peacetime. The leadership responsible for measures related to preparedness rests with the Ministry of Trade and Industry, which supervises the National Board of Economic Defence. The duties of the information systems division of the National Board of Economic Defence includes promoting information security in society, particularly in the business sector. Provincial State Offices and electronic communications preparedness groups assisting them also have also been assigned special preparedness tasks.

Postal address	Visiting address	Telephone	Telefax
PO Box 31 FIN-00023 Government FINLAND	Eteläesplanadi 16-18 Helsinki	+358 9 160 02	+358 9 160 28596 +358 9 160 28590 (Information)



Although sector cooperation and development projects promoting information security are pursued by all the above-mentioned parties, there is little extensive cooperation and coordination of measures at the moment. A lack of coordination on the national level results in unnecessary duplication and in inefficient use of limited resources. Also, there are no channels for distributing experiences and practices of information security matters to the various actors.

Arrangements for implementation

In a true information society, new information, expertise, technology and practices extend to all areas of life. Information security is an essential component of an information society and must likewise extend to all areas of life. This means that closer cooperation between all actors is needed. The National Information Security Strategy lays the foundation for improved cooperation, guiding information security efforts towards shared goals and promoting joint planning and implementation of information security projects and related exchange of information. However, implementation of the Strategy will not change the existing division of responsibility in information security or organization structures.

The Government owns the National Information Security Strategy and is responsible for its implementation and updating as needed. The Ministry of Transport and Communications appoints the Information Security Advisory Board, which supports the harmonization of measures required in the implementation of this Strategy and monitors its implementation. The Board reports annually to the Government on the implementation of the Strategy and on needs for updating it. The Board provides a broad-based forum for improving cooperation between various actors and organizations in information security issues, but does not change the existing division of duties or organization structures.

To enhance implementation of the Strategy, the Board may set up working groups focusing on special issues or specific sectors, in addition to the working group on information security for actors responsible for critical infrastructure referred to above.

The work of the Board is subject to the Act on the Openness of Government Activities (621/1999); under section 24 subsection 1, official documents shall be secret if they relate to security arrangements for data and communications systems and their implementation, to preparedness for exceptional conditions, to the maintenance of national security, to national defence or to business or professional secrets, unless it is obvious that access will not compromise these interests.

Economic and social impact

The goals set in this Resolution can be achieved through framework decisions and decisions to be made annually in connection with the State Budget.

Postal address	Visiting address	Telephone	Telefax
PO Box 31 FIN-00023 Government FINLAND	Eteläesplanadi 16-18 Helsinki	+358 9 160 02	+358 9 160 28596 +358 9 160 28590 (Information)



The Strategy will generate significant added value by increasing cooperation regarding information security between authorities and preventing overlapping measures, thus making the use of public funds more effective. The Strategy will contribute to a better business environment and promote the development of new easy-to-use products and services, thus boosting the competitiveness of Finnish companies. Furthermore, the Strategy will contribute to greater awareness of information security among all users, improve the expertise of professionals in the field and thus strengthen the opportunities for all actors to make full use of the potential of the information society.