MINISTRY OF TRANSPORT AND COMMUNICATIONS
Communications Policy Department, Communications Networks

MEMORANDUM
1.12.2008

EXPLANATORY MEMORANDUM CONCERNING THE GOVERNMENT RESOLUTION ON NATIONAL INFORMATION SECURITY STRATEGY

"Everyday security in the information society – a matter of skills, not of luck"

Background to the Strategy

In Finland today, the information society has reached the stage at which information and communications technologies are no longer separate sectors of society but have become part of people's everyday lives. In the ubiquitous information society the diversity of IT solutions is increasing and these solutions are becoming an integral part of people's daily activities and normal business operations. It is therefore important that everyone has easy access to information society services, and that the electronic services are felt to be reliable. This is a collective responsibility, so people's awareness of information security and their competence in dealing with it are particularly important. The aim of everyday security in the information society will be achieved through everybody's skills and good judgment, not just by luck. The confidentiality, integrity and accessibility of data are very important elements of today's information society.

The previous government resolution on national information security strategy was adopted in 2003 and it brought actors in both the private and the public sectors together in an almost unprecedented way. Above all, it drew attention to and encouraged discussion about information security. Awareness and competence in information security have grown and Finland has been one of the leading countries in the field, both within the EU and internationally. The strategy was the first of its kind in Europe and possibly in the world. The term of office for the National Information Security Advisory Board that coordinated the implementation of the strategy expired in spring 2007. The most significant results of the information security strategy of 2003 included an increase in information security awareness (for example by establishing a national Information Security Day), the compiling of a review of the national information security situation, and the results of a development programme entitled "Trust and information security in electronic services".

The operational environment changes quickly, so information security strategy has to be updated. It is important that the national strategy is realistic and focused, and that it includes prioritised objectives. Information security must be made an integral and natural part of everyday life. The National Information Security Strategy is not addressed to experts only. It is not just a strategy of passive reaction but of actively influencing the future and encouraging bold pioneering. The Strategy does not affect the existing division of responsibilities for information security or the existing organisational structures. The Strategy set out in the government resolution and the State Information Security Guidelines coordinated by the Ministry of Finance complement one another. The Strategy is also linked to the Internal Security Programme.

The National Information Security Strategy is an essential element of the Government's information society policy. The Action Programme 2008-2011 of the Ubiquitous Information Society Advisory Board states that

> *"Trust is one of the most important information society issues. Trust in the information society requires technically efficient and secure services. Trust, broadly understood, is the user's experience or view of service quality. The goal is to maintain and strengthen this trust.*
>
> *Trust is strengthened by easy-to-use services, adequate consumer protection, and confidence in content authenticity as well as protection of consumer privacy and other interests. Improving the position of consumers requires responsibility to be exercised by all parties, including consumers themselves.*
>
> *Society's functions depend almost entirely on the reliability of information networks and systems. Systems are vulnerable to various information security threats and internet crime. Operating environment information security must therefore always be taken into consideration in order to safeguard the operation of critical infrastructure and ensure the integrity of data."*

The Strategy was drawn up in 2008, with the aid of numerous workshops, conferences and rounds of interviews, by the Information Security Group that works under the Ubiquitous Information Society Advisory Board. The tasks of the Information Security Group are to promote information security in the information society, monitor the progress that is made, and suggest improvements.

Strategic aims

The National Information Security Strategy aims to make everyday life in the information society safe and secure for everyone in Finland – for people as individuals and for businesses, administrative authorities, and all other actors in society. The Strategy's vision is that people and businesses will be able to trust that their information is secure when it is processed in information and communications networks and related services. There must be a high overall level of information security skills and knowhow, and the different actors in society need to work seamlessly together to improve information security. By 2015 Finland will be the leading country in the world in terms of information security.

Priority 1: Basic skills in the ubiquitous information society

Information security involves more than just technology. In the ubiquitous information society, people need new kinds of basic skills that they did not possess before. Information security is still too often seen as being a disconnected part of overall ICT development. There are many kinds of information, and information security risks should be evaluated on the basis of the type of data concerned. Trust in the information society is built upon the service providers’ and users’ understanding of their rights and responsibilities. It is also important to improve the skills of business owners and corporate information security professionals.

Priority 2: Information risk management and process reliability

Electronic services and communications are increasingly to be found at the heart of the service system in both the public and private sectors. At the same time, dependence on information technology is making services more vulnerable. People must be able to trust that the services they use are secure and that no confidential data will end up in the wrong hands. When a breach of information security occurs, for example in identity theft, people and businesses must be able to rely on adequate support from the authorities.

Priority 3: Competitiveness and international network cooperation

Finland is part of the global information network economy, which means that a significant percentage of information security threats and attacks (e.g. denial-of-service attacks) originate outside the country’s borders. Finland must be active in international cooperation between national authorities to prevent information security threats and minimise any possible damage. As well as making its own national regulatory environment simpler and more predictable for businesses, Finland must actively seek ways of influencing international regulation.

Measures

1.1. Increasing information security awareness and competence

Secure operations call for basic skills from both the providers and users of the services. The Strategy aims to ensure that everyone in Finland possesses a basic general competence in the 21st century skills needed in the information society, particularly the “information security literacy” related to use of network services, storage of confidential data (passwords, credit card and bank account details, personal data), recognition of common cases of phishing, and ways of ensuring the security of one’s own data terminal equipment. Concrete ways of improving people’s information security awareness and skills must be explored and developed.

1.2 Providing secure electronic services and ensuring confidentiality

The aim is to make Finnish network services as secure as possible throughout their entire life span, starting right from the beginning at the design and planning stage. In this way, information security will become an integral part of service quality. This means in practice that information security aspects are also to be taken into consideration in the processes for purchasing systems and making service agreements.

Information security development cannot be left to IT experts alone: the role of senior management is of prime importance in the integration of information security into business and administrative processes. Attention must also be paid to information security in each phase of training throughout the service provision chain. Services must be made simple, concrete and easy to understand, but without forgetting safeguards for confidential information. Simplicity also promotes security.

2.1 Improving risk management and service reliability

Risk management is the cornerstone of data security in the information society. It ensures the reliability of systems and the continuity of business operations. Risk management perspectives must always be taken into account in designing new products and services. In businesses, risk management is not just the IT experts' responsibility but must be firmly integrated into business planning, management and operations. The creation of a risk management system for a company is a responsibility of that company's senior management. Each stage of service development should include risk evaluation and minimization. One of this Strategy's main tasks is to promote the use of risk management procedures. This must be carried out in seamless cooperation between the authorities, businesses and citizens.

2.2 Safeguarding functions that are vital to society in all circumstances

Today's society is highly dependent on ICT systems and this dependence is steadily increasing. At the same time, however, competition and efforts to improve cost-efficiency may result in a decrease of investment in security. In the ubiquitous information society, the reliability of increasingly complex networks and the management of possible risks pose ever greater challenges. The control of electronic equipment and systems through the Internet (for example online control of traffic lights and street lighting) is just one area that involves serious risks in terms of service disruptions. Joint training exercises improve preparedness for disruptions under normal conditions, and ensure the continuity of service even in emergency conditions. The training emphasises the creation and testing of optimal ways of joint cooperation. The training is also being increasingly oriented towards concrete activities.

3.1 Increasing Finland's attractiveness and competitiveness through better predictability

The clarity and predictability of the regulatory environment is of great importance to companies. Finland should develop its legislation so that the regulatory framework for information security is as light as possible and at the same time comprehensive in scope. The administrative authorities must critically observe the impacts of legislation on the operating conditions for businesses and on people's rights as citizens and as consumers, paying particular attention to any aspects that may be contradictory. More and more businesses are multinational organisations that operate in the global market. In practice, the fact that different countries have different national regulations and implement EU directives in different ways has proved to be a problem. It also complicates the operating conditions for Finnish companies that are active in several countries.

3.2 Intensifying forward-looking and influential international cooperation

Forward-looking and influential international cooperation calls for good national coordination and prioritisation. It is important that influence starts to be exerted in the international arena at a sufficiently early stage (for example through active participation in preparatory working groups and unofficial networks). It is also important to identify good international practices and to be able to export Finnish information security knowhow to other countries. The progressive nature of Finland's legislation and regulatory environment must be adequately "marketed" in forums of international cooperation. By doing this, Finland can also influence the regulatory practices of other countries in a way that benefits Finnish businesses operating in the global market.

Success in international cooperation also depends on playing an active part in developing guidelines for EU information society policy and for the information security policy of international organisations. The establishment of an efficient and effective National Communications Security Authority (NCSA) would promote Finland's participation in international cooperation as well as Finnish IT operators' participation in international tendering procedures. The role of the NCSA in promoting international cooperation would give Finnish information security skills and knowhow better visibility in the eyes of governmental organisations and the business world.

Implementation of the Strategy

Starting points

Under the current legislation and division of responsibilities, information security and its development are the responsibility of a number of parties, and a responsibility of both the private and public sectors. The responsibilities of each Ministry are set out in the Government Rules of Procedure (262/2003, amended 1 January 2008).

Arrangements for implementation

The overall responsibility for the National Information Security Strategy lies with the Government, which monitors the Strategy's implementation and updates it when necessary. The Information Security Group of the Ubiquitous Information Society Advisory Board appointed by the Ministry of Transport and Communications supports the coordination of the measures required to implement the Strategy and monitors its implementation. The Information Security Group includes representatives of both private and public sectors on a broad basis. The working group reports annually to the Government on the implementation of the Strategy and on needs for updating it. It also reports to the Ubiquitous Information Society Advisory Board on the progress of the work being done.

The Information Security Group of the Ubiquitous Information Society Advisory Board was appointed on 31 August 2007 by Ms Suvi Lindén, Minister of Communications, for the period from 1 September 2007 to 28 February 2011. The Group's task is to promote, monitor and suggest improvements for information security in the information society. The group deals with broad, cross-sectoral issues about information security and works in close cooperation with other parties and organisations that promote information security.

Economic and social impacts

The aims set out in the Resolution can be achieved within the framework of decisions on spending limits and the annual Budget. The Strategy will help to increase information security awareness and competence among all users, and to increase and strengthen national cooperation in the whole field of information security.