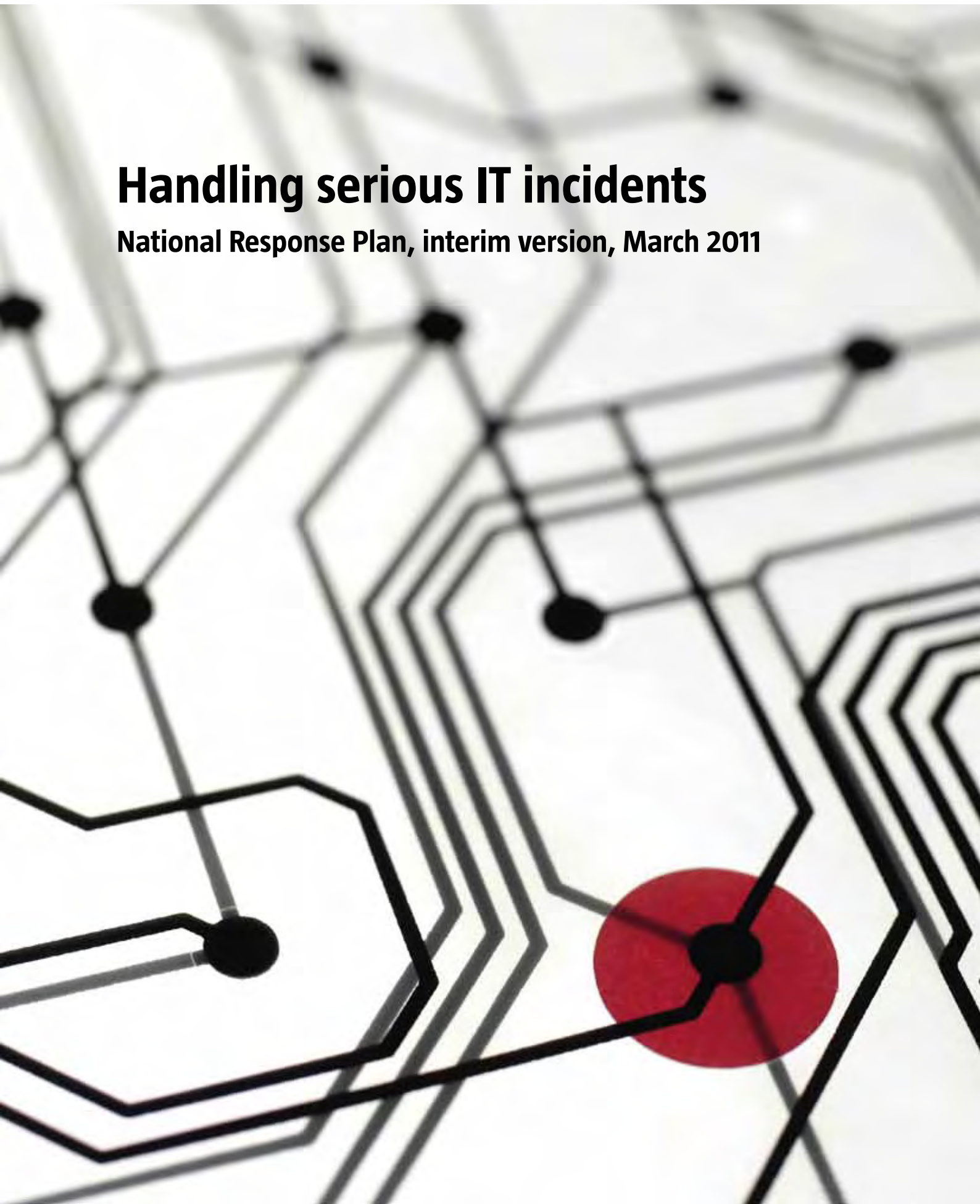




Myndigheten för
samhällsskydd
och beredskap

Handling serious IT incidents

National Response Plan, interim version, March 2011



Handling serious IT incidents

**National Response Plan,
interim version, March 2011**

Handling serious IT incidents
National Response Plan, interim version, March 2011

Swedish Civil Contingencies Agency (MSB)

MSB contact: Lars-Göran Emanuelson

Layout: Advant Produktionsbyrå AB
Print: DanagårdLiTHO

Publ.no: MSB339 - December 2011
ISBN: 978-91-7383-183-3

Foreword

Information security is an increasingly important component in the work for a Safer society. This involves both basic prevention and creating a capability to deal with incidents and emergencies. This capability must exist both with individual actors and on societal level as a whole.

In this publication the MSB presents the national plan for the handling of serious IT incidents, known as the National Response Plan. It should be used to support societal handling of major IT incidents. We reflect here, the key elements of the report that the MSB, on commission from the Government, produced in March 2011.

The National Response Plan is provisional until it has been tested and revised in line with the results. By 2012 at the latest, the first exercise will have been completed.

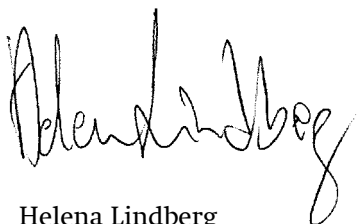
The National Response Plan is based on four main components:

- Situation Awareness at National Level
- Information Coordination
- Overall impact and handling assessment, and
- Technical operational collaboration.

The National Response Plan is activated at the discretion of the MSB and defines what is expected of other actors in the form of information sharing and collaboration.

The MSB has also been commissioned by the government to create technical competence networks that can lend societal support during serious IT incidents, in order to create an enhanced capability for response. This document presents concrete proposals for how such technical competence networks should be created and maintained.

Stockholm, 1st November 2011



Helena Lindberg
Director General
Swedish Civil Contingencies Agency (MSB)

Summary

In this publication, the Swedish Civil Contingencies Agency (MSB) will present its national plan for the handling of serious IT incidents, (the National Response Plan). This plan is intended to improve the country's prerequisites for limiting and preventing the direct consequences of a serious IT incident for society, through collaboration and coordinated decision making. A comprehensive collaboration between several parties is required to solve this task.

Objectives

The National Response Plan is to ensure the country's ability to

- maintain joint, qualified situation awareness
- convey coordinated information to the public
- make use of society's common resources in a fast and efficient manner
- support the use of effective technology
- reach qualified and coordinated decisions
- work in a coordinated manner at the international level
- evaluate and follow up experiences in a systematic manner.

Starting points

The definition of a serious IT incident is an event that

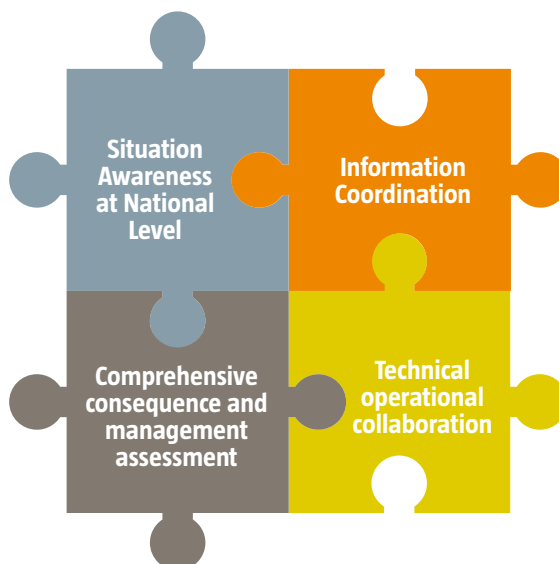
- diverts from the norm
- causes a serious disturbance in vital societal functions
- requires a quick response at the national level
- requires a coordinated response at the national level.

The definition is based on legislation regarding extraordinary events in times of peace and increased preparedness, and on the definitions of vital societal functions.

The National Response Plan is focused exclusively on the handling of serious IT incidents. It is based on the basic prerequisites available in the Swedish crisis management system, i.e. the governing principles and the responsibilities of individual actors.

Focus on collaboration processes

The National Response Plan is based on four central collaboration processes: Situation awareness at national level, information coordination, comprehensive consequence and management assessment, and technical operational collaboration.



The MSB will decide if and when the plan is put into practice. This will be decided in the event of an evident threat of (or immediate risk of) a serious IT incident or if such an incident has already occurred. If the plan were to be activated, however, this does not mean that the MSB will dictate how the incident is handled at other government agencies. That remains the responsibility of those government agencies. On the other hand, the plan does specify what is expected of the relevant government agencies in terms of sharing of information and collaboration.

A general description of the four main components of the National Response Plan are presented on page 7.

The plan will be considered an interim version until it has been exercised and revised according to the results. The first exercise is to be completed before the end of 2012, after which the plan is to be confirmed. The MSB are responsible for planning and carrying out this exercise in collaboration with the SAMFI (the collaboration group for information security) authorities.

Supporting the development of technical competence networks

In the event of a serious IT incident, the regular staff at the different authorities will constitute the main resource in the practical handling of the incident. This main resource is at risk of being severely strained during a serious IT incident. Therefore, there might be a need for additional support, in the form of expert competence. With this in mind, it is important to support the development of technical competence networks that can contribute to improving society's ability to handle the consequences of serious IT incidents.

**SITUATION
AWARENESS AT
NATIONAL LEVEL**



**INFORMATION
COORDINATION**



**COMPREHENSIVE
CONSEQUENCE AND
MANAGEMENT
ASSESSMENT**



**TECHNICAL
OPERATIONAL
COLLABORATION**



Objectives	The creation of a common situation awareness is intended to enable coordinated action, in order to make suitable use of society's resources to handle serious IT incidents	Coordinated and validated information to the public.	An in-depth and complete consequence-based situation awareness from a societal perspective	Restoring important functions
Course of action	Collaboration conferences, actor-specific activities	Conferences on information coordination, communicative activities	Analysis by the MSB (with the help of NOS, the National Operational Collaboration Function for Information Security) based on the actors' status reports	Collaboration between affected parties through national and international networks
Responsibility	The MSB	The MSB	The MSB	Responsible actors
Affected parties	SAMFI, central government agencies, county administrative boards, municipalities, collaboration forums, the private sector, others	Networks for information officers and other relevant parties	SAMFI authorities, relevant national and international networks, actors in charge of vital societal functions	SAMFI authorities, affected actors
Examples of tools	WIS, RAKEL, SOS Alarm, support systems for mandatory incident reporting, systems for global monitoring	Krisinformation.se, information services, press conferences, teletext, radio, RAKEL, SGSI, VMA, authority announcements	Dependency simulation, RSA-db, others	Available communication channels, secure cryptographic functions

A general description of the four main components of the National Response Plan.

The government agencies with special responsibilities in the field of information security will play an important role with regard to a national expert resource, but technical competence networks will be required at all levels of society. We have proposed the following:

- The MSB intends to, in consultation with the SAMFI authorities, investigate the possibility of organizing a technical competence network consisting of technical operational SAMFI experts.
- The MSB intends to carry out a pilot study together with other affected parties in order to develop methods and tools to support the work with technical competence networks at the municipal, regional and national level.
- The MSB intends to work actively towards a developed private-public collaboration between experts and between experts as well as between the providers and recipients of expert support, in order to increase society's ability to handle serious IT incidents. The MSB intends to achieve this through seminars, conferences and exercises.

Contents

1. Introduction	11
1.1 Background and starting points	11
1.2 Why do we need a plan for serious IT incidents?	12
1.3 Conceptual structure – vision, objective and plan	14
1.4 Delimitations	14
1.5 Central concepts	15
2. What is a serious IT incident?	17
2.1 Definition of a serious IT incident	17
2.2 Example of a serious IT incident	19
2.2.1 <i>IT attacks on Estonia</i>	19
3. Prerequisites for the National Response Plan	23
3.1 The Swedish crisis management system	23
3.2 Governing principles	23
3.2.1 <i>The principle of responsibility</i>	23
3.2.2 <i>The principle of proximity</i>	24
3.2.3 <i>The principle of equality</i>	24
3.3 Responsibilities and roles	25
3.3.1 <i>Basic requirements for all actors with regard to emergency preparedness</i>	25
3.3.2 <i>Special responsibility in emergency preparedness</i>	25
3.3.3 <i>Special responsibility for information security</i>	27
3.3.4 <i>Private actors in charge of vital societal functions</i>	27
4. National Response Plan for serious IT incidents	29
4.1 Focus on collaboration processes	29
4.2 Framework for the National Response Plan	31
4.2.1 <i>Activation of the National Response Plan</i>	31
4.2.2 <i>Deactivation of the plan</i>	32
4.2.3 <i>Evaluation of the plan</i>	32
4.2.4 <i>Routines connected to the framework of the National Response Plan</i>	32
4.3 Situation Awareness at National Level	34
4.4 Information Coordination	36
4.5 Comprehensive Consequence and Management Assessment	37
4.6 Technical Operational Collaboration	40
5. Administering the National Response Plan for serious IT incidents	43
5.1 Ownership	43
5.2 Validity	43
5.3 Revision, evaluation and follow-up	43
5.4 Contact person	43
6. References	45
Appendix A: Abbreviations and certain concepts	49
Appendix B: Tables regarding roles and responsibilities	51
Appendix C: Technical competence networks	59

Introduction

1. Introduction

The functionality of the Swedish society requires a functioning IT infrastructure. Increasingly more functions are critically dependent of IT and communication technology for its daily activities. Vulnerabilities in the system could have serious consequences, both for individuals and for society as a whole.

The national plan for the handling of serious IT incidents is intended to improve the country's prerequisites for limiting and preventing the direct consequences of a serious IT incident for society, through collaboration and coordinated decision making. The definition of a serious IT incident is an event that

- diverts from the norm
- causes a serious disturbance in vital societal functions
- requires a quick response at the national level
- requires a coordinated response at the national level.

In order to ensure society's ability to handle serious IT incidents, joint efforts and a broad collaboration between different actors is required. A coordinated national handling of IT incidents requires a suitable framework. The National Response Plan for the handling of serious IT incidents is intended to provide us with such a framework.

1.1 Background and starting points

In April 2010, the Swedish Civil Contingencies Agency (MSB) was tasked by the Government to:

develop a national plan that elucidates how serious IT incidents are to be handled, and to create a technical competence network of experts to support society in the event of a serious IT incident, in order to improve the overall ability to respond to such an incident. The MSB is to carry out its assignment in consultation with the government agencies that are part of the collaboration group for information security, SAMFI. (Government assignment 2010/04/14, Fö2010/701/SSK)

The MSB's interpretation of the assignment is that the National Response Plan is to be based on the Swedish crisis management system's underlying principles; the principle of responsibility, the principle of proximity and the principle of equality. In addition, the plan should

- take into account the fact that serious IT incidents may have several different causes
- clarify roles and responsibilities at the national level, as well as connections to the international level
- list the processes and routines for the national handling of serious IT incidents.

A central point of reference has been that the plan should be closely connected to the principles of crisis management that are applied in society.

1.2 Why do we need a plan for serious IT incidents?

Sweden has structures and regulations for handling different types of accidents and crises at the local, regional and national level. The National Response Plan for serious IT incidents supplements these structures and regulations with regard to handling the consequences of serious IT incidents. There are five circumstances in particular that make a special national plan necessary:

1. Short time span
 - a. An IT incident often occurs within a short period of time, which means that it has to be clear which actors are supposed to act, and when.
 - b. These incidents are often difficult to foresee, as opposed to weather-related incidents, for example. Therefore, affected parties must coordinate their work quickly.
 - c. It is important to have access to well-established collaboration and information channels.
2. Cross-sector consequences and dependencies between different sectors in society
 - a. Disturbances can quickly come to affect many actors. The internet and other central information infrastructures are of crucial importance for a large number of sectors in society.
 - b. The dependencies between sectors in terms of electricity, telephone services and IT entail special requirements of collaboration during a crisis.
3. Geographic unboundedness
 - a. Threats, risks and vulnerability in the IT field are often not related to specific geographic areas. In order to approach this, we will need to set up suitable forms of collaboration at the national and international level.
4. Trust-related matters
 - a. The basic functions of society are dependent on, and dimensioned for, functioning IT support. IT-related disturbances could quickly have a negative impact on the public's trust in public services or central actors. Therefore, it will be necessary to send out a coordinated message in order to lessen these effects.
5. Competence-related needs
 - a. The handling of IT incidents will sometimes require specialist competence in order for affected actors to be able to prevent or lessen the effects of such a disturbance. Therefore, it will be important to make such competence available at all levels of society.



1.3 Conceptual structure – vision, objective and plan

The vision for the National Response Plan has been defined as creating prerequisites for limiting the consequences of a serious IT incident through collaboration and coordinated decision making.

The MSB, together with other actors who participated in the assignment, have divided this vision into a number of specific objectives. Through suitable processed and clearly defined roles and responsibilities, the plan will make it possible to

- create of a common and qualified situation awareness, taking into account the central role of information technology in society
- formulate and communicate a coordinated message to the public
- make use of society's common resources in a fast and efficient manner
- support an efficient, technical handling of the IT incident
- reach qualified and coordinated decisions
- coordinate Sweden's actions at the international level
- evaluate and follow up the experience in a systematic manner.

The MSB has developed the National Response Plan for serious IT incidents based on this vision and these objectives.

1.4 Delimitations

The main objective of the plan is to create prerequisites that ensure society's ability to handle serious IT incidents. As previously mentioned, this task will require joint efforts and a broad collaboration between different actors. In order to achieve this, it is important to clarify the responsibilities and the roles of various actors that are connected to the handling of serious IT incidents.

The foundation of the National Response Plan is the legal prerequisites and central principles such as principle of responsibility. Since the National Response Plan establishes a need for collaboration and coordination between actors, the responsibilities and roles elucidated in the plan are connected to these relationships. For example, the National Response Plan does not affect the type of support for measures connected to national crises with elements of IT which the intelligence and security services are in charge of.

The plan includes a run-through of the actors' responsibilities for crisis management and information security as stipulated in Swedish statutes, but does not specify in detail how individual actors should choose to carry out their tasks.

The National Response Plan is focused exclusively on the handling of serious IT incidents. This means that the preventive work in the field of information security has not been included, even though it is of vital importance for society's ability to handle serious IT incidents. However, there are references to important routines in the preventive work, which is intended to support the establishment of a common situation awareness, among other things.

The plan has been developed for the handling of serious IT incidents in times of peace, and does not apply during increased preparedness.

1.5 Central concepts

The National Response Plan uses a number of different concepts. Some of them are well-known, while others have to be explained further.

- *Serious IT incidents* is a central concept and is described in detail in chapter 2. This chapter also describes the MSB's definition of *vital societal functions*. The Swedish Government tasked the MSB with developing a comprehensive national strategy for protecting vital societal functions (Government assignment Fö2010/698/SSK). This task included clarifying the concept of vital societal functions. The assignment was presented to the Government on 1 March, 2011.¹

- A *coordinated* decision making is defined as when the actors share the same situation awareness and make their respective decisions based on this awareness.

- *Information security* is used in a broad sense. The concept is used both for administrative and technical aspects of confidentiality, accuracy and availability of the information and the resources used to handle this information. However, information security comprises more than simply securing information. Resources, not least people's abilities, are important components of the information security concept.

- *National Cybersecurity Coordination Function (NOS) at the MSB*. The IT-related situation awareness is mainly maintained through a collaboration between affected actors within NOS. NOS is a collaboration form which through

- suitable work methods
- participation by actors with good insight into matters relating to IT incidents
- sound physical prerequisites (premises, communications equipment, and more)
- makes it possible to greatly improve the prerequisites for a joint, national handling of serious IT incidents.

NOS is to ensure that society's common resources are used in the best way possible when handling serious IT incidents, as well as making sure that international assistance can be received safely and efficiently, should it be required. The work within NOS is based on the principle of responsibility. In other words, neither the MSB nor any other NOS member will assume another actor's responsibilities when handling an IT incident.

- *CERT* stands for Computer Emergency Response Team, and is the name of a function whose main task is to monitor and handle IT incidents. A national CERT is a contact point for information sharing and coordination at the national and international level. The MSB runs the Swedish CERT, known as CERT-SE, since 1 January 2001.

- The concept *emergency preparedness* has the same definition as in Section 4 of the Ordinance on Emergency Preparedness and Increased Preparedness, i.e. the ability to prevent, withstand, and manage crisis situations through training, practice, and other measures, as well as through the organizations and structures created before, during, and after a crisis.

1. The definition of vital societal functions, according to the National strategy for protecting vital societal functions, MSB registration number 2010-4547, page 5. A *vital societal function* is defined as a societal function of such importance that a reduction or serious disturbance of the function would entail great risk or danger to the life and health of the population, the functionality of society or the underlying values of society.

**What is a serious
IT incident?**

2. What is a serious IT incident?

Handling the consequences of *serious IT incidents* forms the point of reference for the assignment. Since there is no conventional definition of this concept, the MSB and the assignment's reference group have developed their own definition for the National Response Plan. This definition has been developed with the help of other countries' approaches towards handling IT incidents, which other fall outside "the norm". For example, the United States' response plan defines such incidents as cyber events of national significance (Homeland Security, *National Cyber Incident Response Plan*, Interim Version 2010, page. 1). However, the MSB has based its definition mostly on emergency preparedness legislation and definitions of vital societal functions.

2.1 Definition of a serious IT incident

The definition of a serious IT incident, as defined in the framework for the National Response Plan, is an IT-related event that

1. diverts from the norm
2. causes a serious disturbance in vital societal functions
3. requires a quick response at the national level
4. requires a coordinated response at the national level.

In other words, there are *four separate conditions, all of which must be met* in order for the incident to be defined as serious.

This definition is connected to how an extraordinary event is defined in Chapter 1, Section 4 of the Law on Extraordinary Events (LEH, SFS 2006:544), i.e.

[...] an incident that deviates from the norm, which entails a serious disruption or imminent risk of a serious disruption in important societal functions and which requires prompt efforts by a municipality or county council.

In addition, the definition² is based on how the concept of vital societal functions is defined. From a emergency preparedness perspective, a vital societal function is an activity that meets one or both of the following conditions (Government bill 2007/98:92 *Reinforced emergency preparedness – for safety's sake*)

1. *A shortcoming or serious disruption in the activity that alone or alongside similar incidents in other activities leads to a serious crisis occurring in society in a short period of time.*
2. *The activity is necessary or quite essential for a crisis already occurring in society to be manageable so that the harmful effects are as small as possible.*

2. The definition of vital societal functions, according to the National strategy for protecting vital societal functions, MSB registration number 2010-4547, page 5. *A vital societal function is defined as a societal function of such importance that a reduction or serious disturbance of the function would entail great risk or danger to the life and health of the population, the functionality of society or the underlying values of society.*

Examples of sectors in which there are functions that must be operational at all times: Energy provision, water provision, information and communication, financial services, social insurances, health and medical care, social care, protection and security, transportation, municipal technological provision, availability of food, commerce and industry, and public administration.

In addition, the definition has been inspired by the explanation of the concept given by the MSB in the project *Steering of electricity to prioritized users in the event of an electricity shortage* (Styrel) (MSB Styrel – *directions for the prioritization of electricity users*, reply to government assignment No. 13 in the letter of regulation of 2010, Registration No. 2009-3054, page 7). In this project, the following concept explanation is used to identify vital societal functions:

- *The function is of such importance for the lives and health of the population, society's functionality, and our basic values that it must be operational even in the event of serious incidents or crises.*
- *The function is of particular importance in order for a current serious incident or crisis to be manageable with as little damage as possible.*

The MSB is currently working on clarifying the concept of vital societal functions, as part of a government assignment and within the framework of the development of a joint, national strategy for the protection of such functions (Government assignment Fö2010/698/SSK). A proposal will be presented to the Government on 1 March, 2011. Since this proposal has yet to be completed, the National Response Plan's definition of a serious IT incident is based on the definitions currently applied.

In addition, the definition of a serious IT incident is based on the Swedish Agency for Public Management's guidelines *Handling IT incidents – Who does what, and when?* (the IT Commission, 2001) where an IT incident is defined as an "unwanted and unplanned disturbance [which] affects an IT system". In the National Response Plan, IT is regarded as a wide concept and is defined as technology for collection, storage, processing, production, searching, and for communication and presentation of information (data, text, audio, images). In other words, an IT-related incident could be an event that affects or disturbs different types of hardware, data or telecommunications, steering and monitoring systems, and more.

A serious IT incident is not necessarily the result of criminal intent. It may be caused by lacking competence, mistakes or technical malfunctions and natural events (MSB *Measures to improve society's joint ability to prevent and handle IT incidents*, Presentation of assignment, 2009-14471, page 4).

To sum up, the definition of a serious IT incident could be said to consist of five components, which are presented in Table 1.

COMPONENTS OF THE DEFINITION OF A SERIOUS IT INCIDENT

Components
An IT-related incident, where IT is regarded as a broad concept
A situation that diverts from the norm
A situation that causes a serious disturbance in vital societal functions
A situation that requires a prompt response at the national level
A situation that requires a coordinated response at the national level

Table 1. Components of the definition of a serious IT incident.

2.2 Example of a serious IT incident

In order to illustrate a serious IT incident, within the framework of the National Response Plan, the MSB has studied and analysed a number of actual IT incidents. One example of an IT-related incident that meets the criteria of a serious IT incident is the IT attacks against Estonia in 2007, an extensive denial of service attack. However, an IT incident comes in several other shapes and forms. IT incidents can have both a “logical” and “physical” nature. A short run-through of the IT attacks against Estonia is presented below. (KBM 2008 *Sweden’s preparedness for internet attacks* registration number 1104-2007)

2.2.1 IT attacks on Estonia

In April 2007, Estonia suffered political unrest and demonstrations, due to the relocation of a Soviet memorial statue. This also led to a number of serious DDoS attacks (Distributed Denial of Service attacks, where certain websites are made unavailable). These attacks hit Estonia in three waves, and went on for approximately three weeks. It started with simple denial of service attacks, which gradually turned into coordinated attacks.

The attacks were aimed at the Estonian parliament, ministries, central government agencies, banks and the media. The course of events is described in Figure 1, below.

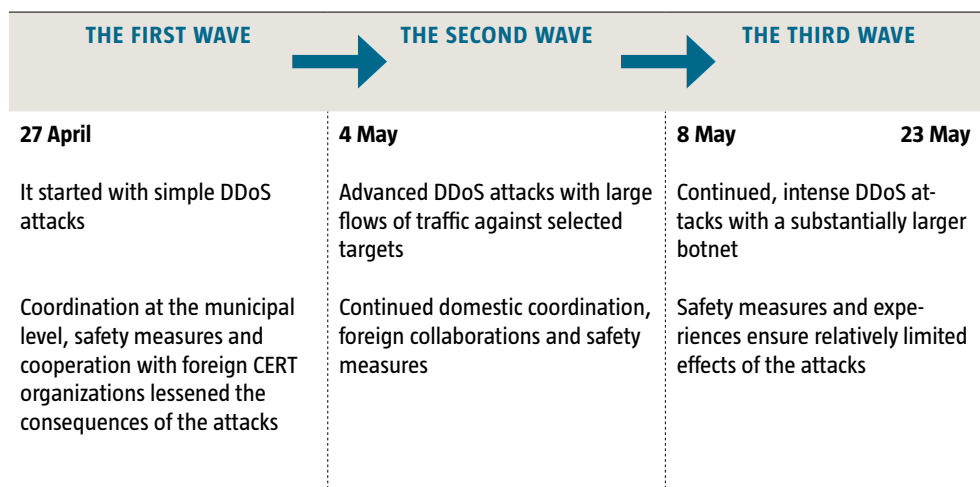
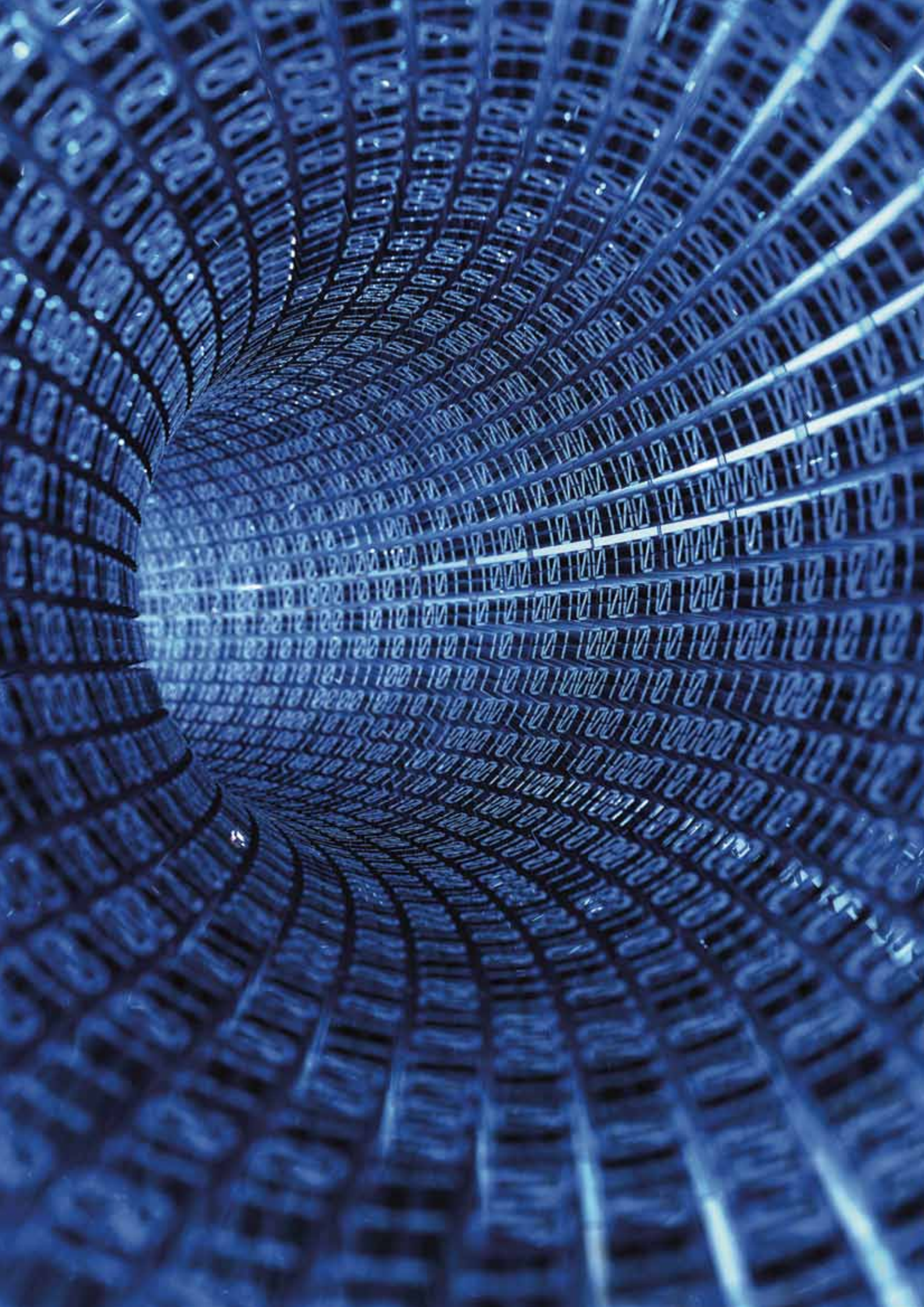


Figure 1. Course of events during the IT attacks against Estonia in 2007.



During the DDoS attacks, failed attempts were made at attacking the Estonian telecommunications network and the system used by the Estonian rescue services.

The attacks had several direct consequences. A number of Estonian websites suffered access-related issues. Political parties, the parliament, the president's office, the police, schools, municipalities and several central government agencies were affected by the attacks.

Hackers put out false information on the government's website, signed by the prime minister. In addition, the parliament was forced to shut down its e-mail service for 12 hours.

Online banking services were shut down, and their contact with the outside world was obstructed. Internet providers were forced to shut down all their customers' connections for 20 seconds, in order to restart their services.

In total, these attacks had several effects on society, and several vital societal functions were affected or at risk of being affected by the attacks. These functions include information and communication services such as the internet and telecommunications, payments, the rescue service's IT system and public administration at the national, regional and local level.

This attack is considered a serious IT incident since it

- was IT-related
- diverted from the norm
- caused a serious disturbance in vital societal functions
- required a quick response at the national level
- required a coordinated response at the national level.

Prerequisites for the National Response Plan

3. Prerequisites for the National Response Plan

The plan for handling serious IT incidents is based on the basic prerequisites available in the Swedish crisis management system, i.e. the prerequisites for collaboration and coordination with regard to governing principles and the responsibilities of individual actors.

3.1 The Swedish crisis management system

Swedish crisis management is based on collaboration. In the event of a crisis, all actors must be able to work together and collaborate on decisions and initiatives. This applies regardless of region or business area: private enterprise, the police, the rescue services, and decision makers in the municipalities, county administrative boards or the Government.

The crisis management system includes sector responsibility, regional responsibility and operative responsibility, divided into municipal level (local), county administrative board and county council level (regional) and central government agency and Government level (national level)

A crisis is initially handled in its immediate proximity, with resources on standby at the regional and national level should the incident at the local level become too large. This means that the municipalities form the foundation of more or less all crisis management. During a crisis, the county administrative board in charge of that geographic area should support the municipality at the regional level, with regard to the collaboration between government agencies, municipalities and other actors. The county administrative board's support does not change other actors' responsibilities with regard to crisis management.

The Government is responsible for crisis management at the national level. Strategic matters are handled by the Government. The Prime Minister's Office manages and coordinates the work, while the Government receives support from the crisis management office, which produces a common situation awareness of how individual events affect society as a whole. Each respective government agency is responsible for the management and coordination of the practical work.

3.2 Governing principles

Swedish crisis management is guided by three principles: *the principle of responsibility, proximity and equality*.

3.2.1 The principle of responsibility

The principle of responsibility is of crucial importance. In short, the principle of responsibility means that whoever is responsible for an activity under normal circumstances has the same responsibility during a crisis. The relevant actor's responsibility is not assumed by a special crisis management actor.

The principle of responsibility has been strengthened in recent years, among other things due to a number of incidents in the 2000s, and has come to incorporate an explicit collaboration requirement. Affected actors are obliged to support one another during a crisis, meaning that they have to assume a more active role in society's crisis management.

Each government agency whose area of responsibility is affected by a crisis situation must take the actions necessary to handle the consequences of that crisis. Government agencies are to cooperate and support one another during such a crisis situation (Section 5 of the Ordinance on Emergency Preparedness and Increased Preparedness).

Furthermore, Government Bill 2005/06:133 Cooperation in times of crisis – for a more secure society, formulates a cautiousness requirement that includes the obligation to act according to the principle of responsibility even in times of uncertainty:

All actors affected by a crisis, directly or indirectly, and who can contribute to handling its consequences have a responsibility to act even in times of uncertainty (Government Bill 2005/06:133, page 51).

This means that an actor cannot avoid taking action, or that the actor does not have to take precautionary action simply because someone else has the main responsibility (Government Bill 2005/06:133, page 51).

In order for the principle of responsibility to have an effect in times of crisis, the measures relating to emergency preparedness and protection against accidents and crises must be a part of the organization's activities during normal conditions.

3.2.2 The principle of proximity

The principle of proximity means that a crisis is to be handled in the area where it takes place, and be managed by those most closely affected and responsible. The crisis management should only be referred to higher levels if it is considered necessary.

A foundation for simple, clear and easy-to-understand communication channels and structures is created by having the operational management taking place in its closest geographical and organizational proximity, [...] (Government Bill 2005/06:133, page 51).

3.2.3 The principle of equality

The principle of equality means that an organization's activities and location should, as far as possible, be kept the same during a crisis. Changes to an organization should not be larger than what is necessary in order to handle the crisis.

[...] and that the organizational changes are not larger than necessary with regard to the crisis (Government Bill 2005/06:133, page 51).

3.3 Roles and Responsibilities

Swedish statutes state that government agencies, county councils and municipalities have a responsibility relating to emergency preparedness and information security.

3.3.1 Basic requirements for all actors with regard to emergency preparedness

There are requirements for both government agencies and for municipalities and county councils to take actions during a crisis situation if it is connected to the actor's area of responsibility or area of location (Section 5 of the Ordinance on Emergency Preparedness and Increased Preparedness and Chapter 5, Section 7 of the Law on Extraordinary Events). In addition, there are a number of specific government agencies with special responsibilities in the area of emergency preparedness (Section 11 of the Ordinance on Emergency Preparedness and Increased Preparedness). When it comes to private actors, the main tool is the private-public collaboration, since there are no stipulated legal requirements relating to emergency preparedness for this type of actor.

Section 30A of the Emergency Preparedness Ordinance (2006:942) stipulates that all government agencies have a responsibility with regard to information security.

Each government agency is responsible for making sure that its information management system meets the basic and special security requirements that ensure that the agency's activities can be carried out in a satisfactory manner. In addition, the need for secure management systems should be given special attention. (Section 30A of the Ordinance on Emergency Preparedness and Increased Preparedness)

3.3.2 Special responsibility in emergency preparedness

In order to meet different needs relating to emergency preparedness, certain government agencies must assume special responsibilities in addition to their basic requirements. This responsibility implies that the government agencies are to make plans and preparations to ensure their ability to handle a crisis, prevent vulnerabilities and withstand threats and risks (Section 11 of the Ordinance on Emergency Preparedness and Increased Preparedness). In order to promote an overall picture, the emergency preparedness planning at these government agencies should be carried out in collaboration. This collaboration is intended to create a mutual understanding among affected actors as to how emergency preparedness in one or several areas should be strengthened. The government agencies specified in the statute and their areas of cooperation are presented in Appendix B, Table 13. Table 14 in Appendix B describes each agency's special responsibility.



SIGNAL 1 ●
SIGNAL 2 ●
MODULE ●

Teletec

3.3.3 Special responsibility for information security

Some government agencies have a special responsibility for various aspects of information security. Most of these government agencies are part of the collaboration group for information security (SAMFI). SAMFI consists of

- The Swedish Civil Contingencies Agency (MSB)
- The Swedish Post and Telecom Authority (PTS)
- The National Defence Radio Establishment (FRA)
- The Swedish Defence Materiel Administration (FMV)
- The Swedish Armed Forces (FM)
- The National Police Board (RPS), represented by the National Criminal Investigations Department (RKP) and the Swedish Security Service (Säpo).

SAMFI is to support the relevant government agencies' assignments in the field of information security, through collaboration and information exchange. The vision is to *work to ensure information assets in society with regard to the ability to maintain desired confidentiality, accuracy and availability*. The SAMFI authorities and the Swedish Data Inspection Board's assignment is described in Table 15, Appendix B. This information is based on instructions and other relevant statutes.

3.3.4 Private actors in charge of vital societal functions

These days, most infrastructure and vital societal functions are owned and operated by the private sector. Sometimes these actors are located outside Sweden. Although these actors do not have any formal responsibilities with regard to emergency preparedness and information security, this does not mean that they do not have any responsibilities. In many cases there are specific regulations that dictate these actors' responsibilities, not least towards end consumers. One example of such a responsibility is Chapter 3, Section 9a of the Electricity Act (1997:857), which stipulates that a power failure must not exceed 24 hours.

**National Response
Plan for serious
IT incidents**

4. National Response Plan for serious IT incidents

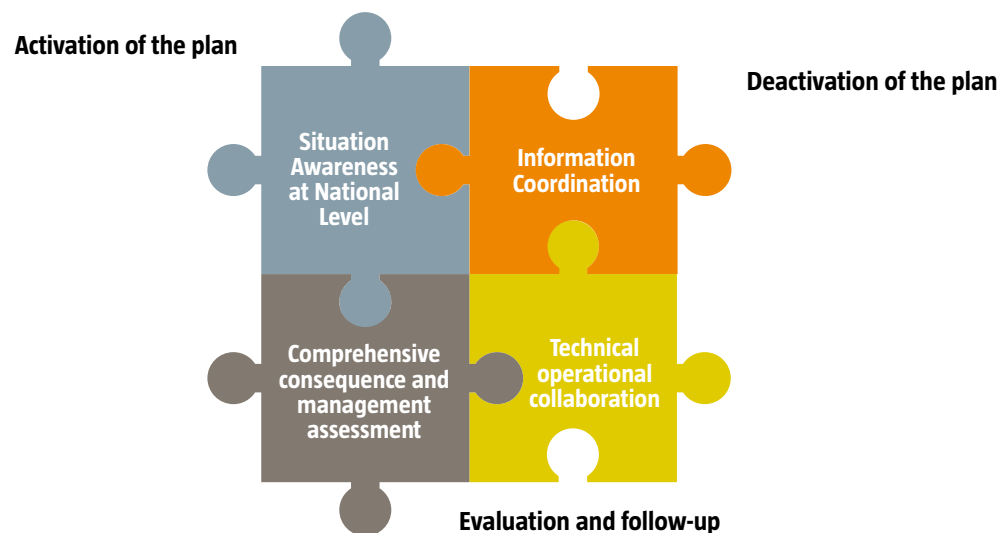
Sweden needs to have a framework that *guarantees a coordinated handling* of serious IT incidents. It is important to create sound prerequisites for government agencies and other actors to be able to coordinate their measures. According to the government principles of emergency preparedness, each individual actor is responsible for handling an incident. This plan is intended to help each actor form a picture of the situation and what prerequisites the incident brings about. This can be achieved by developing a common situation awareness together with other actors. Other activities that actors should preferably carry out together include informing the public about the incident and sharing information on how to approach the incident from a technical standpoint. There are many benefits for society and individuals when actors and sectors collaborate, which the MSB is tasked with supporting. Therefore, the National Response Plan's main part consists of four collaboration processes. These processes aim to create the best possible prerequisites in the fields where collaboration is assessed as being of greatest importance for the handling of a serious IT incident. The collaboration processes are

- situation awareness at national level
- information coordination
- comprehensive consequence and management assessment
- technical operational collaboration.

4.1 Focus on collaboration processes

The collaboration processes have been outlined with the previously mentioned basic prerequisites in mind. The processes are separate, but connected components, which is illustrated in Figure 2 below. The framework that covers the different processes in the illustration consists of routines for activation and deactivation of the National Response Plan, as well as evaluation and follow-up.

When handling a serious IT incident, these processes will mostly be carried out in tandem. A more in-depth description of the processes is given in chapters 4.3-4.6.



Situation Awareness at National Level

During a crisis situation that affects the entire nation, there are many sources and recipients of information. Situation awareness constitutes a necessary prerequisite in order for all involved actors to understand and handle the situation. In order for the actors to be able to plan measures and discuss the need for and distribution of resources in a coordinated manner, their individual situation awareness must be compiled into a common situation awareness. The Situation awareness at national level of serious IT incidents is developed within the current framework for collaboration processes relating to crisis management at the MSB. The objective of this process is to help affected actors reach a common situation awareness.

Information Coordination

A serious IT incident will inevitably generate interest from the media and the public, and there will be an evident need for information. In order to minimize the damage of the IT incident, and to minimize the amount of incorrect and possibly harmful speculation, it is important to coordinate the information given to the public and the media. For example, the damage can be reduced by issuing advice and recommendations to the public. The information coordination is intended to be conducted within the framework of the information coordination process which the MSB is in charge of, and which currently involves a number of thematically formed networks for information officers. The networks for information officers consist of information officers at central government agencies, and can be expanded when needed. The goal of this process is to convey a common message to the public within a short period of time.

Comprehensive Consequence and Management Assessment

There is a need to combine the IT-related situation awareness with the overall Situation awareness at national level of society which the MSB has been instructed to maintain and report on to the Government (Section 7 of Statute (2008:1002)). The IT-related situation awareness is mainly maintained through a collaboration between affected actors within the national operational collaboration function for information security (NOS) at the MSB.

Through NOS, the MSB meets the Government's directions as expressed in Government Bill 2010/11:1 expense area 6 (page 83):

In order to improve society's ability to prevent and handle serious IT incidents, the Government believes that a more coherent structure is needed. An important means to achieve this goal is the establishment of a national collaboration function for information security. Therefore, the Government believes that the Swedish Civil Contingencies Service should set up such a function, together with the relevant government agencies.

The NOS collaboration supports the work conducted at the MSB, where the MSB and actors affected by the crisis produce a joint quality consequence and management assessment with IT competence. This makes it possible to reach a conclusion that takes into account both the IT-related aspects and society as a whole. The consequence and management assessment may form the basis of the Government's decision making and contacts with the outside world. In addition, it might help actors when making decisions for their respective operational responsibilities. The goal of this process is to create an in-depth and complete consequence-based situation awareness from a societal perspective.

Technical Operational Collaboration

Collaboration is often a prerequisite for handling the technical aspects of serious IT incidents efficiently. Sharing information on identified vulnerabilities, harmful code and strategies for national and international support, among other things, can often reduce the timespan of the crisis. When it comes to international collaboration, the various CERT organizations are an important resource. CERT stands for Computer Emergency Response Team. It is important to emphasize that the responsibility for this process is shared by all actors that are obligated to handle the technical aspects of IT-related incidents. The goal of this process is to achieve acceptable functionality in an efficient way.

4.2 Framework for the National Response Plan

There are a number of activities and supporting routines that are relevant to the National Response Plan, but which are not part of the core collaboration processes. This includes the activation and deactivation of the plan, as well as evaluation and follow-up of the handling of a serious IT incident.

4.2.1 Activation of the National Response Plan

The decision to activate the National Response Plan for serious IT incidents is made when

- there is an evident threat or immediate risk of a serious IT incident
- a serious IT incident has occurred (and has not yet caused the National Response Plan to be activated).

This decision is made by the person in charge of the MSB's Department of Coordination and Intervention, within the framework of their authority. In order for such a decision to be made, the MSB must first receive information. This information might be submitted by a duty officer (TiB) or through a finding in the MSB's regular global monitoring, where something is identified which calls for such a decision. However, it is important to clarify that the need to activate the National Response Plan can be brought up by any actor. The international dimension is important, and information can also be submitted by the Government Offices' duty officer or through an European or international CERT organization to the CERT-SE.

If the MSB activates the National Response Plan, the MSB will increase its monitoring and inform all affected parties. Further actions will be taken if the situation calls for it³. If the plan is activated before a serious IT incident has occurred, the MSB will increase its monitoring through increased activity within the NOS collaboration, among other things. In addition, the MSB will collect information from relevant parties in order to gain a better understanding of the current IT incident. The purpose of this phase (which can be regarded as a limited escalation mechanism) is to, as far as possible, create prerequisites for proactive action.

3. Information will be sent to the relevant government agencies through their duty officer function.

If the plan was activated in response to a serious IT incident that has already occurred, the MSB will make an internal decision on a ‘coordination event’, after which the process known as Situation awareness at national level (Chapter 4.3) is started (see further description below).

A decision to activate the plan does not entail any requirements that other government agencies or actors activate their respective crisis management functions. Those decisions are to be made by each respective actor within the framework of their operational responsibility. On the other hand, the plan does specify what is expected of the relevant actors in terms of sharing of information and collaboration within the plan’s various processes.

4.2.2 Deactivation of the plan

When the parameters for a serious IT incident (see Section 2.1) are no longer met, the person in charge at the MSB will decide to deactivate the National Response Plan. However, even if the plan is deactivated, certain processes may still be active. For example, there is a general need for information about an incident long after its consequences have been subsided.

4.2.3 Evaluation of the plan

An important part of the plan is to create sound prerequisites for a systematic evaluation.

The evaluation should be proportional to the activities that are being evaluated. Therefore, the evaluation might be more or less comprehensive.

In order to ensure an ongoing, systematic evaluation, a special evaluation routine has been developed. When the MSB decides to activate the National Response Plan for serious IT incidents, they also decide to initiate an evaluation.

It is important that conclusions and experiences are conveyed to the relevant actors in the system after the evaluation has been completed. Furthermore, it is also important that the information is compiled, so that it can be used when revising the National Response Plan.

4.2.4 Routines connected to the framework of the National Response Plan

The table below describes the tasks connected to the plan’s framework and various actors’ roles.

FRAMEWORK PROCESSES

Supporting routines	Activation of the National Response Plan for serious IT incidents Informing relevant actors (via duty officers) about the activation of the plan Activation of the National Response Plan Decision on evaluation Evaluation and follow-up communicated to relevant actors
---------------------	---

Table 2. Routines connected to the framework processes of the National Response Plan.



ACTOR	TASKS CONNECTED TO THE FRAMEWORK OF THE NATIONAL RESPONSE PLAN
The Swedish Civil Contingencies Agency	Decision to activate the National Response Plan for serious IT incidents Evaluation of the coordination and follow-up communicated to relevant actors Decision to deactivate the National Response Plan for serious IT incidents Informing relevant actors (via duty officers) about the activation of the plan
Others	Incident reporting ⁴ When necessary, call for the need to activate the National Response Plan Support to the evaluation of the handling of the incident

Table 3. Tasks connected to the framework of the National Response Plan.

4.3 Situation Awareness at National Level

A Situation awareness at national level is one of the most fundamental collaboration processes in the National Response Plan, since it is often a prerequisite in order for actors to be able to make coordinated and well-founded decisions. A schematic list of purposes and the process's different components is presented below.

SITUATION AWARENESS AT NATIONAL LEVEL PROCESS

Main objective	Creating a common situation awareness in order to enable coordinated action, and to make possible suitable use of society's resources to handle serious IT incidents
Course of action	Collaboration conferences Actor-specific activities Other activities
Affected parties	SAMFI authorities Central government agencies County administrative boards Municipalities Existing collaboration forums The private sector Others
Convenor of the collaboration conferences	The MSB
Participants in the collaboration conferences	SAMFI authorities Central government agencies County administrative boards Invited experts, when needed Others
Examples of supporting tools	WIS RAKEL Summons via SOS alarm Support systems for mandatory incident reporting (in development) System for global monitoring etc.
Supporting routines	Information from technical competence networks Collaboration conferences Incident reporting Reporting to the Government Reporting to relevant actors (nationally and internationally)

Table 4. Summarizing table for the Situation awareness at national level process.

4. There are currently no requirements for mandatory incident reporting. However, a government assignment is currently under way, in which the outlining of a system for mandatory IT incident reporting is being examined. Therefore, this wording is included in the description of the assignment. Keep in mind that mandatory incident reporting does not replace Police reports.

In the National Response Plan, the process of creating a Situation awareness at national level is connected to the already established collaboration process for crises in society, which is maintained by the MSB. This means that actors can use already established routines. What separates the handling of a serious IT incident from other types of crises is mainly the *time aspect*, both with regard to the possible course of events and the demands for prompt action by the parties involved.

Another challenging aspect is connected to the possibility that a serious IT incident *spreads out across several sectors and geographical borders*, which also affects the situation awareness at national level. In order for a more complete situation awareness to be achieved, we will probably need a larger number of actors to attend the collaboration conferences.

An important prerequisite for the work on a situation awareness at national level is to clarify the roles of the actors in this process, and what they are expected to contribute. Table 5 below described the actors' roles in the collaboration process situation awareness at national level.

ACTOR	TASKS CONNECTED TO THE FRAMEWORK OF THE COLLABORATION PROCESS SITUATION AWARENESS AT NATIONAL LEVEL
The Swedish Civil Contingencies Agency	Decision on coordination Summons to and implementation of collaboration conferences Forming a Situation awareness at national level Reporting on the Situation awareness at national level to the Government Reporting on the Situation awareness at national level to the actors involved in the system Decision to inform relevant technical competence networks Decision to conclude the coordination
SAMFI authorities	The sharing of information with regard to situation awareness, consequences, taken actions and the need for resources Mandatory reporting of occurred IT incidents to the MSB Participation in the collaboration conferences Possible intensification of resources to the national collaboration function for information security
Central government agencies	The sharing of information with regard to situation awareness, consequences, taken actions and the need for resources Mandatory reporting of occurred IT incidents to the MSB Participation in the collaboration conferences
County administrative boards	Implementation of regional collaboration conferences Forming a regional situation awareness The sharing of information with regard to situation awareness, consequences, taken actions and the need for resources Voluntary reporting of occurred IT incidents to the MSB Participation in the collaboration conferences
Municipalities	The sharing of information with regard to situation awareness, consequences, taken actions and the need for resources Participation in regional collaboration processes
Existing collaboration forums	Sharing of information

Table 5. Tasks connected to the framework of the collaboration process Situation awareness at national level.

The private sector	Sharing of information via government agencies with sectoral responsibilities and the county administrative board Voluntary reporting of occurred IT incidents to the MSB Possible participation in the collaboration conferences Possible intensification of resources to the national collaboration function for information security (with regard to operators of vital societal functions and infrastructure)
Others	Sharing of information

Table 5. Tasks connected to the framework of the collaboration process Situation awareness at national level.

4.4 Information Coordination

Information is an important tool in the handling of all forms of crises. Being able to coordinate information to the public and provide a coherent picture of consequences, affects actors, required actions and course of action has shown to be of crucial importance. There are already well-established contacts between different thematic networks for information officers, consisting of information officers at several central government agencies. In the event of a crisis, the MSB will summon these to a conference on information coordination. This conference will usually be held at the same time as the collaboration conferences, and the information officers will often attend these as well in order to acquaint themselves with the situation.

MAIN OBJECTIVE	A COORDINATED QUALITY CONVEYANCE OF INFORMATION TO THE PUBLIC – A COHERENT AND TIMELY MESSAGE.
Course of action	Conferences on information coordination and communicative activities
Convenor	The MSB
Connected process	Situation awareness at national level
Affected parties	Networks for information officers and other relevant parties
Examples of supporting tools	www.krisinformation.se Information services for government agencies Press conferences Teletext Radio RAKEL SGSI VMA Authority announcements etc.
Supporting routines	FAQ Basis of the Situation awareness at national level

Table 6. Information coordination.

An important aspect that is connected to the information coordination is that information officers are the ones who are supposed to answer questions. In other words, those who are working on averting the IT relating crisis are not supposed to be the ones answering questions. If the technical operational staff is not relieved in this way, there is a risk that the work of informing other actors will compromise the actual work of averting and limiting the consequences of the crisis.

The information officers' responsibilities and activities within the framework of the information coordination process are described in table 7.

ACTOR	TASKS CONNECTED TO THE FRAMEWORK OF THE COLLABORATION PROCESS INFORMATION COORDINATION
The Swedish Civil Contingencies Agency	Summons to and implementation of conferences on information coordination Publication of agreed upon material via relevant channels, such as www.krisinformation.se Participation in various information-related activities together with relevant actors
Networks for information officers consisting of information officers at the central government agencies and the county administrative boards	Participation in the conferences on information coordination Participation in various information-related activities together with relevant actors Contribution of data for publication via www.krisinformation.se
Other relevant parties, when needed (such as affected private owners or operators of vital societal infrastructure)	Participation in the conferences on information coordination Participation in various information-related activities together with relevant actors

Table 7. Tasks connected to the framework of the collaboration process information coordination.

4.5 Comprehensive Consequence and Management Assessment

Besides the situation awareness at national level, which is formed at the collaboration conferences, an in-depth analysis of consequences and an assessment of the handling of the incident is also needed (including the need for specific resources). The process of a comprehensive consequence and management assessment is based on the information provided via the collaboration conferences. The analysis of the situation is made more in-depth by combining the IT-related situation awareness (which is developed within the NOS) with the actors' combined situation awareness. In order to analyse the more far-reaching societal consequences of the incident, tools provided by the MSB such as dependency simulation are also used. In total, this results in a more qualitative analysis and assessment, which will benefit the decision making of both the Government and other affected actors.

A natural part of the consequence and management assessment is to issue recommendations and warnings to the representatives of vital societal functions, as well as to the public.



COMPREHENSIVE CONSEQUENCE AND MANAGEMENT ASSESSMENT

Main objective	An in-depth and complete consequence-based situation awareness from a societal perspective
Course of action	Analysis conducted by the MSB with the aid of the national collaboration function for information security (NOS)
Connected process	Situation awareness at national level
Responsibility	The MSB
Affected parties	SAMFI authorities CERT-SE Relevant national and international networks Private actors in charge of the functionality of vital societal functions
Examples of supporting tools	Dependency simulations RSA-db Others
Supporting routines	Data for individual consequence assessments Contact person (liaison) with the process Situation awareness at national level

Table 8. Comprehensive consequence and management assessment.

ACTOR**TASKS CONNECTED TO THE PROCESS COMPREHENSIVE CONSEQUENCE AND MANAGEMENT ASSESSMENT**

The Swedish Civil Contingencies Agency	Continuous update and analysis of the Situation awareness at national level with regard to information security Comprehensive consequence and management assessment Warning and informing vital societal actors, and other affected parties Reporting on the comprehensive consequence and management assessment to the Government and other relevant actors Data for the person in charge of the information coordination process, for further discussions and decisions
SAMFI authorities	Sharing of information and analysis support When needed, intensification of resources to NOS
Relevant national and international networks	Sharing of information and analyses Expert support within the framework of existing technical competence networks When needed, intensification of resources to NOS
Private actors in charge of the functionality of vital societal functions	Sharing of information Expert support within the framework of existing technical competence networks

Table 9. Tasks connected to the process comprehensive consequence and management assessment.

The actors' assignments within the framework of the process comprehensive consequence and management assessment are described in table 9.

4.6 Technical Operational Collaboration

In the event of a serious IT incident, the regular staff at the different authorities will constitute the main resource in the practical handling of the incident. The main resource consists of technicians, operation staff, system developers and IT security experts, for example. This main resource is at risk of being severely strained during a serious IT incident, which necessitates various national resources that can support the handling of serious IT incidents (such as technical competence networks). Another aspect that is connected to the technical handling of serious IT incidents is the need for collaboration and sharing of information between actors that handle the technical operational aspects of the incident.

The technical operational collaboration is of crucial importance for averting serious IT incidents. Although each respective organization is in charge of the handling of technical aspects that fall within their operational responsibility, it is important to share information on, for example, identified vulnerabilities, what the harmful code looks like, possible patches, and so on. There may also be a need for extra resources (expert resources). The MSB works to facilitate the establishment of contacts between experts as well as between the providers and recipients of expert support. The MSB’s commitments to supporting the development of technical competence networks in order to improve society’s ability to handle serious IT incidents are described in appendix E. Furthermore, it is important to emphasize the significance of international collaboration, not least between CERT organizations.

MAIN OBJECTIVE	RESTORING IMPORTANT FUNCTIONS
Course of action	Collaboration between affected parties within the framework for national and international networks
Connected process	Situation awareness at national level Comprehensive consequence and management assessment
Responsibility	Actors in charge within the framework for their respective authority
Affected parties	SAMFI authorities CERT-SE Relevant actors (public and private) nationally and internationally
Examples of supporting tools	Available communication channels Secure cryptographic functions ⁵
Supporting routines	Sharing of information (TLP) Operational support Mediating contacts with technical competence networks

Table 10. Technical operational collaboration.

5. The sharing of sensitive information between collaborating government agencies should be protected with cryptographic functions, in order to maintain confidentiality and accuracy, but also to ensure that the information is provided by a trusted sender, which might be particularly important in this case.

Table 11 summarizes the expectations of different affected actors with regard to technical operational collaboration.

ACTOR	TASKS CONNECTED TO THE FRAMEWORK OF THE COLLABORATION PROCESS TECHNICAL OPERATIONAL COLLABORATION
The Swedish Civil Contingencies Agency	Providing continuous technical advice and support (CERT-SE) in order to avert serious IT incidents Being Sweden's point of contact with similar European and international organizations (CERT-SE) Warning and informing vital societal organizations and infrastructure, and other affected parties (NOS) Recommending certain types of action and resources
SAMFI authorities	Sharing of information Operational technical support (mainly the National Defence Radio Establishment, the Swedish Security Service and the Swedish Armed Forces. Assessments on a case-by-case basis.
Other actors in charge within the framework for their respective authority	Sharing of information

Table 11. Tasks connected to the framework of the collaboration process technical operational collaboration.

**Administering the
National Response
Plan for serious
IT incidents**

5. Administering the National Response Plan for serious IT incidents

5.1 Ownership

The National Response Plan for serious IT incidents is owned and administered by the MSB.

5.2 Validity

The plan will be considered an interim version until it has been exercised and revised according to the results. The first exercise is to be completed before the end of 2012, after which the plan is to be confirmed. The MSB and the information security department are responsible for planning and carrying out this exercise in collaboration with the SAMFI authorities.

The plan is proposed to be valid for three years after confirmation (or until there is a need to review the plan).

Exercises relating to the plan should be conducted continuously, in order to keep the plan adequate and up-to-date. It is suggested that these exercises take place every three years, starting with the year of its confirmation.

5.3 Revision, evaluation and follow-up

After the plan has been confirmed, it will be evaluated every three years, or when it is considered necessary. All SAMFI authorities may initiate an evaluation that falls outside the regular revision period. Revision of the plan's contents will be carried out after consulting with the SAMFI authorities and upon the decision of the MSB.

5.4 Contact person

The Head of the Information Security Department at the MSB is the contact person for matters regarding the National Response Plan for serious IT incidents.

References

6. References

Laws

The Police Act (1984:387)

The Security Protection Act (1996:627)

The Electricity Act (1997:857)

The Law on Extraordinary Events (2006:544).

Ordinances

Ordinance (1989:773) on Instructions for the National Police Board

The Security Protection Ordinance (1996:633)

The Personal Data Ordinance (1998:1191)

Ordinance (2002:864) on Instructions for the County Administrative Boards

Ordinance (2002:1050) on Instructions for the Swedish Security Service

Ordinance (2006:942) on Emergency Preparedness and Increased Preparedness

Ordinance (2007:854) on Instructions for the Swedish Defence Material Administration

Ordinance (2007:937) on instructions for the National Radio Defence Establishment

Ordinance (2007:951) on instructions for the Swedish Post and Telecom Authority

Ordinance (2007:975) on instructions for the Swedish Data Inspection Board

Ordinance (2007:1266) on Instructions for the Swedish Armed Forces

Ordinance (2008:1002) on Instructions for the Swedish Civil Contingencies Agency

Government bills

Government Bill 2005/06:133 Cooperation during crises – for a safer society

Government Bill 2007/98:92 Reinforced emergency preparedness – for safety's sake

Government Bill 2010/11:1 Budget proposal for 2011

Documents from government agencies

(KBM 2008 Sweden's preparedness for internet attacks registration number 1104-2007)

Directions for the prioritization of electricity users (MSB, 2010) reply to government assignment No. 13 in the letter of regulation of 2010, Registration No. 2009-3054

Measures to improve society's joint ability to prevent and handle IT incidents (MSB, 2010), The MSB's reply to government assignment 2009-14471,

Handling IT incidents – Who does what, and when? (The Swedish Agency for Public Management, 2010) The IT commission



Others

Government Decision Duty officer and management function according to the Ordinance (2006:942) on Emergency Preparedness and Increased Preparedness, (Fö2007/436/CIV, 2007/06/07)

Government Decision Duty officer and management function according to the Ordinance (2006:942) on Emergency Preparedness and Increased Preparedness (Fö2008/552/SSK, 2008/10/09)

(Government assignment 2010/04/14, Fö2010/701/SSK)

(Government assignment 2010/04/14, Fö2010/701/SSK)

The United States: National Cyber Incident Response Plan, Interim Version, Homeland Security, September 2010

WARP Homepage: <http://www.warp.gov.uk/index.html> (2010/12/03)

Appendix

Appendix A: Abbreviations and certain concepts

Botnet – A network of computers infected with harmful code, which makes it possible for a third party to remotely control them.

CERT (Computer Emergency Response Team) – Function for handling incidents.

CERT-SE – The Swedish CERT function at the MSB.

CCRA (Common Criteria Recognition Arrangement) – An international organization that recognizes mutually issued certificates. The Common Criteria standard is developed within the CCRA, as are methods and regulations that support the CCRA agreement.

CC (Common Criteria) – An international standard for how to make demands, declare and evaluate the security of IT products and systems.

CSEC (The Swedish Certification Body for IT Security) – Located at the Swedish Defence Materiel Administration and in charge of the structure, operation and administration of a system for evaluation and certification of IT security in products and systems in accordance with the Common Criteria standard.

DDoS attacks (Distributed Denial of Service) – An access-related attack which overloads or blocks certain IT resources, obstructing the access to resources in an IT system or delaying time sensitive operations.

FHS – The Swedish National Defence College.

FOI – The Swedish Defence Research Agency.

FORTV – The Swedish Fortifications Agency.

FM – The Swedish Armed Forces.

FMV – The Swedish Defence Materiel Administration.

FRA – The National Defence Radio Establishment.

KBF – The Ordinance (2006:942) on Emergency Preparedness and Increased Preparedness.

LAN (Local Area Network) – A local computer network.

LEH – The Law on Extraordinary Events (2006:544).

MSB – The Swedish Civil Contingencies Agency.

NOS (National Cybersecurity Coordination Function) – a collaboration instituted by the MSB. The NOS is intended to improve society's ability to handle serious IT incidents.

NTSG – The National Telecommunications Coordination Group.

PTS – The Swedish Post and Telecom Authority

PUL – The Personal Data Act.

Ping and SYN flooding – Different types of denial-of-service attacks.

Rakel – A common radiocommunications system for organizations that work with public order, security or health.

RKP – The National Criminal Investigations Department.

RPS – The National Police Board.

RSA – Risk and vulnerability analysis.

SAMFI (The collaboration group for information security) – SAMFI consists of representatives from the National Defence Radio Establishment, the Swedish Post and Telecom Authority, the Swedish Armed Forces, the National Police Board, the National Criminal Investigations Department and the Swedish Civil Contingencies Agency.

S-BIT – Coordination function for crime-related IT incidents, owned by the National Police Board and the Swedish Security Service.

SCADA system (Supervisory Control And Data Acquisition) – Computer-based system for the steering, adjustment and monitoring of physical processes such as electricity, gas, rail bound traffic and drinking-water provision.

SGSI (Swedish Government Secure Intranet) – A network service that functions independently of the internet, which Swedish government agencies can use to communicate.

Sitic (Sweden's IT Incident Centre) – The Swedish CERT function. Operated by the MSB under the name CERT-SE as from 1 January, 2011.

Secure cryptographic functions – Encryption systems that are approved nationally for protecting secret or sensitive information. Cryptographic solutions are used at all government agencies mentioned in chapter 3 in order to protect phone calls, faxes, computer files, video conferences or entire networks.

Säpo – The Swedish Security Service.

TiB – Duty officer.

TLP (Traffic Light Protocol) – A model for sharing sensitive information between organizations. This protocol has four levels of information. Red – the information is only conveyed verbally and to specific, named persons. Yellow – limited distribution within the organizations. Green – the information may be distributed within the organizations, but may not be published on the internet, for example. White – can be distributed without restrictions.

VMA – Important message to the public.

WAN (Wide Area Network) – A computer network that covers a large area. Can connect different local networks (LAN).

WARP (Warning, Advice and Reporting Point) – A British network model where organizations sharing advice and information on threats and vulnerabilities relating to information security.

WIS (Web-based information system) – A national web-based information system used for sharing information between the actors involved in Sweden's crisis management system before, during and after a crisis.

Appendix B: Tables regarding roles and responsibilities

Table 12 below describes the requirements relating to emergency preparedness that affects municipalities as well as government agencies at the central and regional level.

BASIC REQUIREMENTS IN EMERGENCY PREPAREDNESS

Actor	Responsibility
Central government agencies	Each government agency whose area of responsibility is affected by a crisis situation is to take the actions necessary for handling the consequences of said crisis. The government agencies are to cooperate and support one another during such a crisis situation. (Section 5 of the Ordinance on Emergency Preparedness and Increased Preparedness)
Municipalities and county councils	<p>Municipalities and county councils are to analyse which extraordinary incidents could happen in the municipality or county council in peacetime, and how these incidents might affect their own activities. The findings from this work are to be evaluated and compiled in a risk and vulnerability analysis. (Chapter 2, Section 1, first paragraph of the Law on Extraordinary Events).</p> <p>Furthermore, for each new term of office, municipalities and county councils are to establish a plan for how to handle extraordinary events, taking into consideration the risk and vulnerability analysis. (Chapter 2, Section 2, first paragraph of the Law on Extraordinary Events).</p> <p>Municipals and county councils are to have a committee that carries out tasks relating to extraordinary events in times of peace (a crisis management committee). [...] (Chapter 2, Section 2 of the Law on Extraordinary Events).</p> <p>Within their respective geographical area, and with regard to extraordinary events in times of peace, municipalities are to ensure that</p> <ol style="list-style-type: none"> 1. different actors within the municipality are cooperating and that they are coordinated in their planning and preparations, 2. the crisis management measures taken by different actors during an extraordinary event are coordinated, and 3. information to the public during extraordinary events is coordinated. <p>(Chapter 2, Section 7 of the Law on Extraordinary Events).</p> <p>Municipalities and county councils are to make sure that elected officials and civil servants receive the education and training necessary for them to be able to carry out their tasks during extraordinary events in times of peace. (Chapter 2, Section 8 of the Law on Extraordinary Events).</p> <p>Municipalities and county councils are to keep the agency appointed by the Government informed about the actions taken in accordance with this chapter, as well as how these actions have affect their emergency preparedness.</p> <p>During extraordinary events in times of peace, municipalities and county councils are to provide government-appointed government agencies with status reports and information on the course of events, the current situation and expected, future development, as well as taken and planned actions. (Chapter 2, Section 9 of the Law on Extraordinary Events).</p>
County administrative boards	<p>Within their respective geographical area, and with regard to situations described in Section 9, county administrative boards are to be a uniting function between local actors such as municipalities, county councils and the private sector, and the national level, and also ensure that:</p> <ul style="list-style-type: none"> • regional risk and vulnerability analyses are compiled, • necessary collaboration within the county and between nearby counties is seen to continuously, • the activities at municipalities, county councils and government agencies are coordinated during crises, • information to the public and the media during extraordinary events is coordinated, and • domestic and international resources that are made available are prioritized and directed in accordance with the Government's decision. <p>(Section 7 of The Ordinance (2006:942) on Emergency Preparedness and Increased Preparedness).</p>

Table 12. Basic requirements in emergency preparedness.

The government agencies specified in the ordinance and their areas of cooperation are presented in Table 13 below. Table 14 describes each agency's special responsibility.

GOVERNMENT AGENCIES IDENTIFIED BY SECTION 11 OF THE ORDINANCE (2006:942) ON EMERGENCY PREPAREDNESS AND INCREASED PREPAREDNESS

Areas of collaboration	Government agencies with special assignments within the area of collaboration
Technical infrastructure	The Swedish National Grid The National Electrical Safety Board The Swedish Civil Contingencies Agency The Swedish Post and Telecom Authority The Swedish Energy Agency The National Food Agency
Transports	The Swedish Maritime Administration The Swedish Energy Agency The Swedish Transport Administration The Swedish Transport Agency
Dangerous goods	The Swedish Coast Guard The National Food Agency The Swedish Civil Contingencies Agency The National Police Board The Swedish Institute for Communicable Disease Control The National Board of Health and Welfare The Swedish Board of Agriculture The National Veterinary Institute The Swedish Radiation Safety Authority Swedish Customs
Financial security	The Swedish Financial Supervisory Authority The Swedish Social Insurance Agency The Swedish Pensions Agency The Swedish National Debt Office The Swedish Tax Agency
Geographical responsibilities	County administrative boards The Swedish Civil Contingencies Agency
Protection, relief and care	The Swedish Coast Guard The Swedish Civil Contingencies Agency The National Police Board The Swedish Maritime Administration The National Board of Health and Welfare The Swedish Transport Agency Swedish Customs

Table 13. Government agencies with special responsibilities, as stipulated by Section 11 of the Ordinance (2006:942) on Emergency Preparedness and Increased Preparedness.

In addition to the government agencies that have been given special responsibilities by the Government in accordance with the Ordinance on Emergency Preparedness and Increased Preparedness, other government agencies also participate in the collaboration areas, such as the Swedish Armed Forces, the National Defence Radio Establishment, the Swedish Fortifications Agency, the Swedish Mapping, Cadastral and Land Registration Authority, SMHI and the Swedish Defence Research Agency.

SPECIAL RESPONSIBILITIES FOR GOVERNMENT AGENCIES ACCORDING TO SECTION 11 OF THE ORDINANCE ON EMERGENCY PREPAREDNESS AND INCREASED PREPAREDNESS

Actor	Responsibility
Appointed government agencies, central and regional	<p>In particular, the government agencies are to</p> <ol style="list-style-type: none"> 1. collaborate with the county administrative boards with regard to their area of responsibility 2. collaborate with other government agencies, municipalities, county councils, associations and businesses that are affected by the event, 3. heed the collaboration that takes place within the European Union and international forums with regard to matters regarding society's emergency preparedness, 4. take into consideration the need for research and development and other knowledge such as follow-up of already occurred events, 5. pay attention to the need for security and compatibility in the technical systems required for the agencies to carry out their assignments, 6. take into consideration the need for participation in common radio communications systems for protection and security (Rakel), which are administered by the Swedish Civil Contingencies Agency, and 7. inform the Swedish Civil Contingencies Agency about their exercises, so that they can be coordinated with the Agency's own exercises. Furthermore, the government agencies are to participate in exercises that fall within their area of responsibility. <p>(Section 11 of the Ordinance on Emergency Preparedness and Increased Preparedness)</p> <p>When needed, the Swedish Civil Contingencies Agency is to provide the Government Offices with suggestions on possible changes as regard which government agencies are to have a duty officer whose task it is to initiate and coordinate the initial work of discovering, verifying, alarming and informing during serious crises. (Section 12 of the Ordinance on Emergency Preparedness and Increased Preparedness)</p> <p>19 central government agencies have installed duty officers and management functions in accordance with government decision (Duty officers and management functions according to the Ordinance (2006:942) on emergency preparedness and Increased Preparedness, Fö2007/436/CIV, 2007/06/07), followed by an additional eight agencies after a supplementary decision (Fö2008/552/SSK, 2008/10/09). In addition, the county administrative boards have duty officers and management functions (in accordance with the Government decision of 29 March, 2007 on the Ordinance (2007:130) on Changing the Ordinance (2002:864) on Instructions for the County Administrative Boards).</p> <p>Government agencies with responsibilities stipulated in Section 11 are to, in the event of a situation as described in Section 9, paragraph 2, keep the Government informed about the course of events, the current situation, the expected development and available resources within each respective area of responsibility, as well as taken and planned actions.</p> <p>Section 15 Each government agency is to, upon request by the Government Offices or the Swedish Civil Contingencies Agency, provide the information necessary for the common situation awareness. (Section 14-15 of the Ordinance on Emergency Preparedness and Increased Preparedness)</p>

Table 14. The appointed government agencies' special responsibilities, according to the appendix to Ordinance on Emergency Preparedness and Increased Preparedness.

The SAMFI authorities and the Swedish Data Inspection Board's assignment is described in Table 15 below. This information is based on instructions and other relevant statutes.

GOVERNMENT AGENCIES WITH SPECIAL RESPONSIBILITY FOR INFORMATION SECURITY

Actor	Assignments and regulation rights connected to information security in accordance with instructions or other regulations
The Swedish Civil Contingencies Agency (MSB)	<p>Ordinance (2008:1002) on Instructions for the Swedish Civil Contingencies Agency</p> <p>Section 1 The Swedish Civil Contingencies Agency is responsible for matters relating to protection against accidents, emergency preparedness and civil defence, in the event that no other agency has already assumed responsibility. The Agency's responsibilities regard actions before, during and after an accident or crisis.</p> <p>Section 7 The Agency must be able to contribute with support during serious accidents and crises, and support the coordination of affected government agencies' actions during a crisis. During a crisis, the Agency is to make sure that affected actors are able to</p> <ol style="list-style-type: none"> 1. coordinate their crisis management measures 2. coordinate their information to the public and the media 3. make efficient use of society's common resources as well as international resources 4. coordinate the support to central, regional and local organs with regard to information and situation awareness. <p>The Agency must be able to provide the Government Offices with data and information during serious accidents and crises.</p> <p>Section 11a The Agency is to support and coordinate the work on society's information security, and analyse and assess the global development in the field. This includes providing other government agencies, municipalities and county councils as well as companies and organizations with advice and support relating to preventive work. Furthermore, the Agency is to report to the Government on circumstances in the field of information security that might necessitate actions at different levels and areas of society.</p> <p>In addition, the Agency is to make sure that Sweden has a national function that supports society's work on preventing and handling IT incidents. As part of this work, the Agency is to:</p> <ol style="list-style-type: none"> 1. act promptly during IT incidents by spreading information and, when needed, coordinating and assisting the work to avert and minimize the incident's effects, 2. collaborate with government agencies with special assignments in the field of information security, and 3. be Sweden's contact with similar functions in other countries, and develop collaborations and exchange of information with these functions. Ordinance (2010:1901) <p>The Ordinance (2006:942) on Emergency Preparedness and Increased Preparedness</p> <p>Section 31 The Swedish Armed Forces, the Swedish Defence Materiel Administration, the National Defence Radio Establishment, the Swedish Coast Guard, the Swedish National Defence College, the Swedish Defence Research Agency, the Swedish Fortifications Agency, the Swedish Defence Recruitment Agency, the Swedish Civil Contingencies Agency and the Government Offices must have secure cryptographic functions.</p> <p>The Swedish Civil Contingencies Agency decides which other government agencies are to have secure cryptographic functions.</p>

Table 15. Government agencies with special responsibility for information security.

In addition, the Swedish Civil Contingencies Agency decides which companies may, upon agreement, have secure cryptographic functions. Furthermore, the Swedish Civil Contingencies Agency may come to agreements with municipalities and organizations that are in need of secure cryptographic functions.

Section 34 The Swedish Civil Contingencies Agency may

1. issue the regulations necessary for the implementation of Section 9, regarding risk and vulnerability analyses,
2. issue regulations relating to the security requirements referred to in Section 30a, concerning a national and international standard, and
3. issue the regulations necessary for the implementation of Sections 16-20 and 33, with the exception of matters relating to the Swedish Defence Materiel Administration, the National Defence Radio Establishment, the Swedish Coast Guard, the Swedish Defence Research Agency and the Swedish Fortifications Agency.

The Swedish Post and Telecom Authority (PTS)

Ordinance (2007:951) on Instructions for the Swedish Post and Telecom Authority

Section 1 The Swedish Post and Telecom Authority is a public authority with responsibilities relating to postal and electronic communication.

Section 4 The Swedish Post and Telecom Authority is to

1. promote access to secure and efficient electronic communication, which includes seeing to that society-wide services are available, and to promote access to a wide selection of electronic communications services,
7. monitor the development of security in electronic communication and any possible environmental or health risks,
10. issue regulations in accordance with the Ordinance (2003:396) on Electronic Communication,
14. exercise supervision in accordance with the Act (2000:832) on Qualified Electronic Signatures, and issue regulations in accordance with the Ordinance (2000:833) on Qualified Electronic Signatures,
15. exercise supervision in accordance with the Act (2006:24) concerning National Top-level Domains for Sweden, and issue regulations in accordance with the Ordinance (2006:25) concerning National Top-level Domains for Sweden, and
16. work towards robust electronic communication and reduce the risk of disturbances, which includes procurement of services that strengthen communications, and promote increased crisis management ability.
17. work towards increased network and information security relating to electronic communication, through collaboration with government agencies with special assignments within the fields of information security, security and privacy, as well as other affected actors, and
18. provide other government agencies, municipalities and county councils as well as companies and organizations with advice and support relating to network security. Ordinance (2010:1913)

Section 7 The Swedish Post and Telecom Authority is to

3. have authority to request advice and support in accordance with the European Parliament and Council's regulation (EC) No. 460/2004 of 10 March, 2004 on the establishment of the European Network and Information Security Agency.
5. participate in international organs on matters regarding the administration of the internet by, when needed, representing Sweden and preparing matters with interested parties at the national level.

Section 8 The Swedish Post and Telecom Authority may procure services that

4. strengthen society's preparedness for serious disturbances in electronic communication and postal services in times of peace.

Table 15. Government agencies with special responsibility for information security.

The National Police Board (RPS) and the Swedish Security Service (Säpo)	<p>Ordinance (1989:773) on Instructions for the National Police Board</p> <p>Section 3 The National Police Board is in charge of the coordination of</p> <ol style="list-style-type: none"> 5. the Police's preparedness with regard to incidents in information technology systems (IT incidents) <p>Ordinance (2002:1050) on Instructions for the Swedish Security Service</p> <p>Section 2 The Swedish Security Service is tasked with running police operations that prevent and expose crimes against national security.</p> <p>In addition, the Swedish Security Service is to run police operations that concern</p> <ol style="list-style-type: none"> 1. fighting terrorism <p>The Police Act (1984:387)</p> <p>Section 2 It is the duty of the Police to</p> <ol style="list-style-type: none"> 1. prevent crime and other disturbances of public order or safety, 3. carry out investigations and surveillance in connection with indictable offences, 4. provide the public with protection, information and other kinds of assistance, whenever such assistance is best given by the Police, <p>Other government agencies are to support the Police in its work.</p> <p>The Security Protection Act (1996:627)</p> <p>Section 5 Organizations that are under Swedish law are to have security protection if needed with regard to the operation's nature, scope and other circumstances.</p> <p>This security protection is to be outlined with regard for individuals' right to obtain public documents, as stipulated by the Freedom of the Press Act.</p> <p>Section 6 Security protection refers to</p> <ol style="list-style-type: none"> 1. protection against espionage, sabotage and other crimes against national security, 2. protection of confidential information as stipulated by the Public Access to Information and Secrecy Act (2009:400) and which concern national security, and 3. protection against terrorism, in accordance with Section 2 of the Act (2003:148) on Criminal Responsibility for Terrorist Offences, including when the crime is not a threat to national security. Act (2009:464.) <p>Section 7 Security protection is indented to prevent</p> <ol style="list-style-type: none"> 1. the unauthorized publication, alternation or destruction of confidential data that concerns national security (information security), <p>In addition, security protection is to prevent terrorism.</p> <p>Section 9 When outlining information security, the need for protection in automatic processing of information should be given special attention.</p> <p>Section 33 The Government or the agency appointed by the Government is to issue further regulations, if it is needed for the implementation of the Act.</p> <p>The Security Protection Ordinance (1996:633)</p> <p>Section 43 The National Police Board may issue further regulations on the implementation of the Security Protection Act (1996:627), with regard to register controls. Such regulations regard the control of staff at the Swedish Armed Forces, which is decided in consultation with the Swedish Armed Forces.</p>
---	--

Table 15. Government agencies with special responsibility for information security.

	<p>Section 44 The National Police Board and the Swedish Armed Forces may issue further regulations on the implementation of the Security Protection Act (1996:627), with regard to their respective areas of operation, as stipulated in Section 39.</p> <p>The first paragraph does not apply to the scope of the stocktaking of secret documents as stipulated in Section 9, second paragraph.</p> <p>Section 44a In addition to the stipulations in Section 42, the National Police Board may issue further regulations on the implementation of the Security Protection Act (1996:627) for its area of operation, as stipulated in Section 40a.</p> <p>The first paragraph does not apply to the scope of the stocktaking of secret documents as stipulated in Section 9, second paragraph.</p> <p>Section 45 Government agencies are to issue further regulations on the implementation of the Security Protection Act (1996:627), with regard to security needs in their areas of operation, unless it is evidently superfluous. Before the new regulations have gained legal force, government agencies are to consult the agency which issues regulations according to Sections 43-44.</p> <p>The government agencies' regulations may divert from the original regulations as stipulated in Sections 43-44 only when this has been approved by the issuing agency.</p>
The National Defence Radio Establishment (FRA)	<p>Ordinance (2007:937) on Instructions for the National Radio Defence Establishment</p> <p>Section 4 The National Defence Radio Establishment is to have high technical competence in the field of information security. The National Defence Radio Establishment may, upon request, support government agencies and state-owned companies that handle information that is considered sensitive from a vulnerability perspective or from a security or defence perspective. In particular, the National Defence Radio Establishment is to be able to</p> <ol style="list-style-type: none"> 1. support actions during national crises with IT features, 2. help identify the actors involved in IT-related threats against vital societal functions, 3. carry out IT security analyses, and 4. provide other technical support. <p>The National Defence Radio Establishment is to collaborate with other organization in the field of information security, nationally and internationally.</p> <p>Ordinance (2006:942) on Emergency Preparedness and Increased Preparedness</p> <p>Section 32 The Swedish Armed Forces is to make sure that the Swedish Defence Materiel Administration, the Swedish National Defence College, the Swedish Defence Research Agency, the Swedish Defence Recruitment Agency and the Swedish Fortifications Agency are provided with secure cryptographic functions. The National Defence Radio Establishment is to make sure that the other government agencies who are to have secure cryptographic functions according to Section 31 are provided with these.</p>
The Swedish Defence Materiel Administration (FMV)	<p>Ordinance (2007:854) on Instructions for the Swedish Defence Materiel Administration</p> <p>Section 5 The Swedish Defence Materiel Administration has a certification organ which is to establish and operate a certification order for security in IT products and systems. The Swedish Defence Materiel Administration is to work towards international recognition of these certifications.</p>

Table 15. Government agencies with special responsibility for information security.

The Swedish Armed Forces (FM)	<p>Ordinance (2007:1266) on Instructions for the Swedish Armed Forces</p> <p>Section 3b In particular, the Swedish Armed Forces are to</p> <ol style="list-style-type: none"> 3. run and coordinate the signalling protection service, including the work on secure cryptographic functions that are intended to protect sensitive information, 4. assist the Government Offices in matters relating to cryptography and other signalling protection, <p>Section 33 The Swedish Armed Forces may instruct other government agencies on matters relating to signalling protection, including secure cryptographic functions within the overall Swedish defence, with the exception of matters relating to the implementation of Section 33 of the Ordinance (2006:942) on Emergency Preparedness and Increased Preparedness.</p> <p>The Security Protection Act (1996:627)</p> <p>Section 33 The Government or the agency appointed by the Government is to issue further regulations, if it is needed for the implementation of the Act. (1996:627)</p> <p>The Security Protection Ordinance (1996:633)</p> <p>Section 44 The National Police Board and the Swedish Armed Forces may issue further regulations on the implementation of the Security Protection Act (1996:627), with regard to their respective areas of operation, as stipulated in Section 39.</p> <p>The first paragraph does not apply to the scope of the stocktaking of secret documents as stipulated in Section 9, second paragraph.</p> <p>Section 45 Government agencies are to issue further regulations on the implementation of the Security Protection Act (1996:627), with regard to security needs in their areas of operation, unless it is evidently superfluous. Before the new regulations have gained legal force, government agencies are to consult the agency which issues regulations according to Sections 43-44.</p> <p>The government agencies' regulations may divert from the original regulations as stipulated in Sections 43-44 only when this has been approved by the issuing agency.</p>
The Swedish Data Inspection Board (DI), not a member of SAMFI	<p>Ordinance (2007:975) on Instructions for the Swedish Data Inspection Board</p> <p>Section 1 The Swedish Data Inspection Board is tasked with working for the protection of personal integrity through correct handling of personal data, and to make sure that best practice is used in credit information and debt collection businesses.</p> <p>In particular, the government agency is to inform about current rules and give advice and assistance to personal record representatives, in accordance with the Personal Data Act (1998:204).</p> <p>The agency is to monitor and describe the development in the field of IT in terms of matters relating to integrity and new technology.</p> <p>The Personal Data Ordinance (1998:1191)</p> <p>Section 2 The Data Inspection Board is the supervisory authority under the Personal Data Act (1998:204).</p> <p>The Data Inspection Board's right to issue regulations as stipulated by the Personal Data Act (1998:204) is described in the Personal Data Ordinance (1998:1191).</p>

Table 15. Government agencies with special responsibility for information security.

Appendix C: Technical competence networks

Suggestions for technical competence networks

In order to increase society's joint ability to handle serious IT incidents, the MSB suggests the following actions:

- The MSB is to, in consultation with the SAMFI authorities, investigate the possibility of creating a more formalized technical competence network consisting of technical operational SAMFI experts. This is intended to improve the prerequisites for sharing information, increasing competence levels and networking at the national level.
- The MSB is to initiate a pilot study together with other affected parties in order to develop methods and tools to support and maintain technical competence networks at the municipal, regional and national level.
- The MSB is to work actively to create prerequisites for private-public collaboration between experts as well as between the providers and recipients of expert support, in order to create and further develop relevant contacts. The MSB is to organize seminars, conferences and exercises.

Background

There is a lack of technical competence in various vital societal functions and infrastructure. This deficiency might bring about serious difficulties during crises in society. For example, there are relatively few people in Sweden who have sufficient experience of handling traffic flows at the operator level, or various types of specialized industrial control systems (SCADA). In addition, even fewer people have the contact network necessary for the practical operational handling of serious IT incidents. Furthermore, a large part of this technical competence is located in the private sector.

In order to get a better understanding of the need for competence networks, it is important to make an inventory of the different sectors' capacities and shortcomings, as well as already existing formal and informal networks. In addition, there needs to be prerequisites for various resources that can be used to support the national handling of serious incidents. These resources could, for example, be organized as technical competence networks at all levels of society (sector-specific, locally, regionally and nationally) and based on the current needs and prerequisites.

The overall goal with regard to the deficit of technical competence is to *increase society's joint ability to handle serious IT incidents*.

The assignment and important starting points

In April 2010, the MSB was tasked by the Government to create technical competence networks that can support society in times of crisis, which was to be done along with the development of the National Response Plan for handling serious IT incidents. The assignment was formulated as follows:

The Swedish Civil Contingencies Agency is to develop a national plan that elucidates how serious IT incidents are to be handled, and to create a technical competence network of experts to support society in the event of a serious IT incident, in order to improve the overall ability to respond to such an incident. The MSB is to carry out its assignment in consultation with the government agencies that are part of the collaboration group for information security.

Due to the limited amount of time, this work has focussed on producing suggestions that are intended to support the development and maintaining of technical competence networks, rather than de facto creating them.

Important starting points:

- The focus of the competence networks, as described in this report, is the handling of serious IT incidents.
- Governing principles for the Swedish crisis management system apply.
- Government agencies with an explicit responsibility for matters regarding information security play an important role (the 'SAMFI authorities').
- It is important to promote private-public collaboration within the framework of current and planned initiatives and activities.
- There is currently a large number of existing networks, both nationally and internationally. We should try to avoid initiatives that result in a duplication of efforts.

The overall purpose of improving society's joint ability to handle serious IT incidents entails that the focus will be on management-related issues rather than on competence networks to support the preventive work.

Similar to the main report on the National Response Plan, it is important to emphasize the importance of governing principles in the crisis management system (such as principle of responsibility) and what consequences this will have for the outlining of the proposals. *When outlining the proposals below, the emphasis has been on collaboration and networks, and on the development of common methods and tools, in accordance with these principles.* This emphasis is due to the fact that all actors have a different need for technical competence, as well as different prerequisites for creating and maintaining networks.

The SAMFI authorities, i.e. the Swedish Armed Forces, the Swedish Defence Materiel Administration, the National Defence Radio Establishment, the Swedish Civil Contingencies Agency, the Swedish Post and Telecom Authority and the National Police Board/Swedish Security Service, all have different responsibilities and authorities, but they have a common responsibility for matters relating to information security. All of these government agencies have technical experts who, in the event of a serious IT incident, will be involved in the handling of this incident to some extent. Given the special responsibility that these government agencies have with regard to information security, it is reasonable to expect that they also have a *special role with regard to competence networks*. Of course, the actual distribution of responsibility is a matter of discussion, which will be investigated together with the parties involved.

The importance of establishing a functioning collaboration between public and private actors to support the handling of serious IT incidents cannot be emphasized enough. It is without a doubt a matter that affects all parties, as well as a common success factor.

The proposals in short

Proposal 1:

The MSB intends to, in consultation with the SAMFI authorities, investigate the possibility creating a network based on mutual trust between the parties, consisting of technical operational experts at government agencies with special responsibilities relating to serious IT incidents (SAMFI authorities).

As previously mentioned, the collaboration groups for information security (SAMFI) consists of six government agencies which have a special responsibility in the field of information security. The SAMFI authorities collaborate on matters regarding information security, with the vision of *working to ensure information assets in society with regard to the ability to maintain desired confidentiality, accuracy and availability*. In addition, collaboration between government agencies takes place in the everyday work, outside the framework of these more formalized meetings. *In order to further strengthen this collaboration, we propose that the possibility of creating more formalized collaborations, including the technical, operational experts, is investigated further by the MSB together with affected parties.*

In 2011, the national operational collaboration function (NOS) will be created within the MSB. This function is planned to consist of CERT-SE and staff from the MSB's Information Security Department, as well as staff from the SAMFI authorities. NOS's assignment will include improving society's ability to handle serious IT incidents, among other things. It is important that the question of a possible technical operational network of experts is viewed with these initiatives and other relevant and existing networks in mind.

Proposal 2:

The MSB intends to create a "tool box" together with affected actors at the municipal, regional and national level, consisting of processes and methods that support the creation and maintaining of technical competence networks.

There are currently a number of formal and informal networks for information officers in the field of information security. It is important that these networks are supplemented by technical competence networks that are adapted to the needs of vital societal actors at the local, regional and national level – specifically with regard to the operational handling of IT incidents. Such technical competence networks contribute to improving society's joint ability to handle serious IT incidents by, among other things, creating contacts between relevant actors and increasing the technical competence with regard to the handling of such incidents.

In order to be successful in the creation of technical competence networks, the MSB suggests that it develops a "tool box" together with affected actors at the municipal, regional and national level, to support the creation and maintaining of technical competence networks. We suggested that this work is carried out within the framework for a pilot project, where relevant representatives from different levels of society participate (including both public and private actors).

The purpose is to develop useful tools that can then be provided to other interested parties through suitable channels. Support and inspiration for the work is available through previously disseminated concepts such as “WARP”, which has been a successful concept in England.

In the United Kingdom, the NISCC (National Infrastructure Coordination Centre, now part of the CPNI, Centre for the Protection of National Infrastructure) has developed a network model for sharing information on IT security, known as WARP – Warning, Advice and Reporting Point. The purpose of these networks is to increase information security for various actors’ systems, by having the members of the networks providing each other with warnings about vulnerabilities and threats, and sharing advice on how to reduce risks. These networks are relatively small, with 20-100 members, in order to build trust between the members. The concept for WARP that is used in the United Kingdom does not completely fulfil the purpose of the Swedish competence networks. The basic idea, however, could be reused for our purposes: to create a trustworthy network with the same interests in order to maintain open communications and to quickly be able to reach the right person in the relevant area of competence.⁶

Proposal 3:

The MSB is to initiate activities that promote private-public networks, in order to increase the ability to handle serious IT incidents.

This proposal involves supporting existing networks within the relevant fields and taking concrete initiatives for activities that promote contacts between private and public actors in a wider sense. Contacts are needed both between experts and between the experts and those who might need expert support during a serious IT incident. Examples of possible activities include organizing seminars and conferences, as well as organizing exercises, etc. Moreover, it is important to take into account the international dimension and the need for technical competence networks with a transboundary nature (such as the CERT networks).

6. <http://www.warp.gov.uk/index.html> (2010-12-03)

