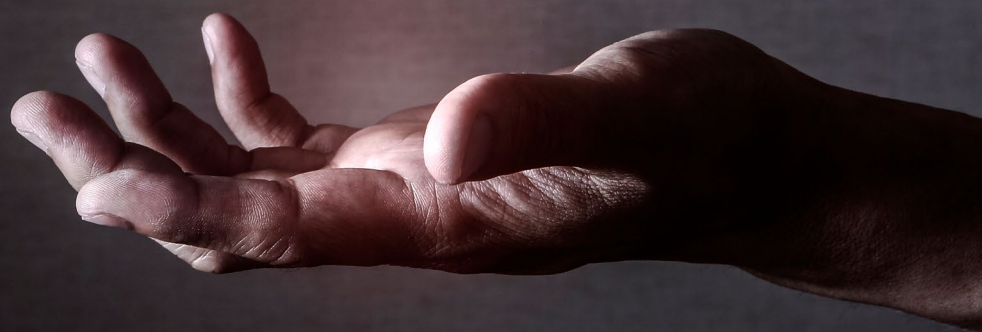
Comprehensive cyber security action plan 2019–2022

March 2019



Swedish Civil Contingencies Agency

FRA

FMV

SWEDISH ARMED FORCES

PTS

Polisen
Swedish Police

Säkerhetspolisen
Swedish Security Service

Comprehensive cyber security action plan 2019–2022

March 2019

Swedish Civil Contingencies Agency (MSB)
National Defence Radio Establishment (FRA)
Swedish Defence Materiel Administration (FMV)
Swedish Armed Forces
Swedish Post and Telecom Authority (PTS)
Swedish Police Authority
Swedish Security Service

Comprehensive cyber security action plan 2019–2022 – March 2019

Swedish Civil Contingencies Agency (MSB)

Photo: Shutterstock
Production: Advant

Publication number: MSB1393 - May 2019 ISBN: 978-91-7383-944-0

This publication is also available in Swedish
Samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022 – 1 mars 2019
Publication number: MSB1351 - March 2019 ISBN: 978-91-7383-918-1

Contents

Summary

Summary

The comprehensive cyber security action plan contains measures that the Swedish Civil Contingencies Agency (MSB), the National Defence Radio Establishment (FRA), the Swedish Defence Materiel Administration (FMV), the Swedish Armed Forces, the Swedish Post and Telecom Authority (PTS), the Swedish Police Authority and the Swedish Security Service individually, together or in collaboration with other actors intend to undertake in order to increase information and cyber security in society. The majority of the measures in this year's report of the action plan are planned to be implemented or begun in 2019. The action plan will thereafter be updated annually.

The measures in the action plan all fall within the scope of the areas of responsibility of each authority. However, the plan shall not be seen as a complete account of all of the measures that the authorities intend to carry out within their respective areas to promote information and cyber security in society.

All 77 measures in the action plan connect to one or more of the six strategic priorities that the Swedish Government has established in the National Cyber Security Strategy (Skr. 2016/17:213). The majority of the measures aim to

- securing a systematic and comprehensive approach in cyber security efforts,
- enhancing network, product and system security, and
- enhancing capability to prevent, detect and manage cyberattacks and other IT incidents.

The report states which authority is responsible for the respective measure, who contributes and what the measure covers.

Introduction

Introduction

As the Swedish Government describes in the national cyber security strategy, digital transformation is a global phenomenon impacting virtually every part of society. It is one of the biggest changes of our times, and the rapid development of information and communications technology has a major impact on our future. Sweden is at the forefront of technological development. It presents us with major opportunities, but also risks.

The demands on society's cyber security are increasing at an accelerating pace. This development and changes in the use of new technology and new innovations make threats more difficult to detect, risks more difficult to assess and dependencies more difficult to survey.

In order to increase cyber security, there is a need for all the parties concerned to increasingly work together towards common objectives.

National strategy

In the national cyber security strategy, the Swedish Government expresses overarching priorities intended to constitute a platform for Sweden's continued development work within the area. The main aims of the strategy are to help to create the long-term conditions for all stakeholders in society to work effectively on cyber security, and raise the level of awareness and knowledge throughout society. The strategy also aims to support the efforts already under way with the goal of strengthening society's information and cyber security. The strategy also presents an account of what is to be protected and what threats and risks there are. The Government emphasises that information and cyber security is the responsibility of everyone in society.

The strategy covers six strategic priorities:

- Securing a systematic and comprehensive approach in cyber security efforts
- Enhancing network, product and system security
- Enhancing capability to prevent, detect and manage cyberattacks and other IT incidents
- Increasing the possibility of preventing and combating cybercrime
- Increasing knowledge and promoting expertise
- Enhancing international cooperation

The strategy encompasses the whole of society, that is to say authorities, municipalities and county councils, companies, other organisations and private individuals.

Securing a systematic and comprehensive approach in cyber security efforts	Enhancing network, product and system security	Enhancing capability to prevent, detect and manage cyberattacks and other IT incidents
Central government authorities, municipalities, county councils, companies and other organisations are to have knowledge of threats and risks, assume responsibility for their cyber security and conduct systematic cyber security efforts. There is to be a national model to support systematic cyber security efforts. Collaboration and cyber security information sharing is to be enhanced. There is to be appropriate super-vision to create conditions for increasing society's cyber security.	Electronic communications are to be effective, secure and robust and are to meet the needs of their users. Electronic communications in Sweden are to be available independent of functions outside the country's borders. The supervisory authority's need for being able to take adequate measures is to be met. Access to secure data encryption systems for IT and communications solutions are to meet society's needs. Security in industrial information and control systems is to increase.	The capability to prevent, detect and manage cyberattacks and other IT incidents in society is to be improved. Relevant stakeholders are to be able to take coordinated action to manage cyberattacks and other serious IT incidents. There is to be a developed cyber defence for the most securitysensitive activities in Sweden, with a strengthened military capability to meet and manage attacks from qualified opponents in cyberspace.
Increasing the possibility of preventing and combating cybercrime	**Increasing knowledge and promoting expertise**	**Enhancing international cooperation**
The law enforcement authorities shall have the preparedness and capability to combat cybercrime in an effective and appropriate manner. The work to prevent cybercrime shall be developed.	Knowledge in society as a whole regarding the most urgent vulnerabilities and needs for security measures is to increase. The knowledge of individual digital technology users regarding the most urgent vulnerabilities and needs for security measures is to increase. Higher education, research and development of high quality are to be conducted in the areas of cyber security and of IT and telecom security in Sweden. Both cross-sectoral and technical cyber security training is to be carried out regularly in order to enhance Sweden's capability to manage the consequences of serious IT incidents.	International cooperation on cyber security is to be enhanced, as part of the objective of a global, accessible, open and robust internet characterised by freedom and respect for human rights. Cyber security is to be promoted as part of the ambition to safeguard free flows in support of innovation, competitiveness and societal development.

Overview of the strategic priorities and associated objectives stated in the national cyber security strategy.

Action plan

In July 2018, the Swedish Government assigned the authorities with a specially appointed responsibility in cyber security, the Swedish Civil Contingencies Agency (MSB), the National Defence Radio Establishment (FRA), the Swedish Defence Materiel Administration (FMV), the Swedish Armed Forces, the Swedish Post and Telecom Authority (PTS), the Swedish Police Authority and the Swedish Security Service to formulate a comprehensive cyber security action plan for the years 2019–2022.

The authorities in this assignment have particular responsibilities in the cyber security area. They also have a well-established collaborative platform through the Cooperation Group for Information Security (SAMFI). The Government considers that in-depth collaboration between these authorities is a prerequisite for enhancing Sweden's capability to protect against cyberattacks and other serious IT incidents. The action plan contributes to providing the Government with a better platform for analysing if the authorities' planned measures are adequate to achieve the objectives in the national strategy and what other measures the Government needs to undertake. According to the Government, the comprehensive action plan should aim to bring about a coordination of the authorities' measures and activities.

The action plan constitutes a comprehensive account of what measures the authorities on their own initiative plan to undertake in the scope of their existing areas of responsibility to contribute to achieving the strategic priorities in the national strategy. The action plan does not constitute a governing document for the authorities.

Progress on the action plan shall be reported to the Government annually on 1 March. According to the government assignment, the MSB is the coordinator for this reporting. The assignment's final report is to be presented on 1 March 2023. This reporting does not replace the authorities' regular reporting to the Government.

The measures, and associated activities, are carried out within given financial allocations, either by one authority individually or in joint projects. The plan shall not be seen as a complete account of all of the measures that the authorities intend to carry out within their respective areas of responsibility.

Work of the authorities on the action plan

The work on the action plan began in early autumn 2018 and has primarily consisted of an inventory of measures already planned by the authorities. No further needs analysis was made for the 2019 report beyond what the Swedish Government had already established in the national cyber security strategy.

Preparation of the plan included joint workshops with the authorities involved where collaboration needs and opportunities were identified. The work on the action plan also included discussions and collaboration with various stakeholders in society. This included the National Board of Health and Welfare and supervisory authorities according to the Ordinance (2018:1175) on Information Security for Essential and Digital Services (the NIS ordinance) and other stakeholders relevant to Sweden's cyber security.

Actions

Actions

Chapter 2 presents planned and ongoing measures. Some measures can contribute to several strategic priorities or objectives in the national cyber security strategy. However, in the action plan, the measures are presented under the strategic priority and associated objective that the measure most clearly ties into. The measures under the respective objective are presented in no inherent priority order.

For every measure in the action plan, it is clarified which SAMFI authority or authorities are responsible for implementation. The responsible authority collaborates in several cases with other authorities or organisations.

Within the respective measures, collaboration with other actors can take place in various ways and for example, may serve the purpose of collecting comments or of documentation. Participation in collaboration always takes place based on available resources. The implementation of the various measures takes place consistently in consideration of the respective authority's area of responsibility. The ambition is for the work with the various measures to be characterised to the furthest possible extent by transparency between the SAMFI authorities.

Strategic priority 1. Securing a systematic and comprehensive approach in cyber security efforts

Objective 1.1. Central government authorities, municipalities, county councils, companies and other organisations are to have knowledge of threats and risks, assume responsibility for their cyber security and conduct systematic cyber security efforts.

1.1.1. Proactively supporting the most security-sensitive activities

Responsible authorities: Swedish Security Service, FRA and Swedish Armed Forces

Extensive and systematic proactive support for the most security-sensitive activities, such as advice, training, exercises, IT security analyses and inspections. The measure is being carried out in accordance with the reporting of the Government assignment on the development of the work to protect particularly security-sensitive activities (Fö2017/00535/SUND) and the reporting of the corresponding assignment issued to the Swedish Armed Forces in the authority's appropriation directions for 2018.

When: 2019–2025

1.1.2. Training of surveillance responsible authorities

Responsible authorities: Swedish Armed Forces and MSB

Training in information security and protected communication. This activity is linked to the Total Defence Exercise 2020 (TFÖ) and all surveillance responsible authorities and sectors concerned.[1] The measure is also carried out together with the Swedish Security Service and the Swedish Defence University.

When: 2019

1. Section 15 of the Ordinance (2015:1052) on Emergency Preparedness and Surveillance Responsible Authorities' Measures at Heightened Alert.

1.1.3. Training private actors regarding the Swedish Armed Forces' protective security requirements

Responsible authority: Swedish Armed Forces

The Swedish Armed Forces have begun signing contracts for preparedness agreements with business enterprises. This includes protective security agreements (PSA) and requirement specification as well as training in the protective security area so that they can be suppliers to the Swedish Armed Forces.

Some courses have been held. The Swedish Armed Forces provide training in parallel with establishing new agreements.

When: 2019–2021

1.1.4. Delivering aggregate information on threats and vulnerabilities

Responsible authorities: Swedish Security Service, FRA and Swedish Armed Forces

Systematically providing aggregated information on threats and vulnerabilities to decision makers at various levels, such as regulatory authorities. This makes it possible for information of a sensitive nature to be able be filtered and adapted to be useful in a broader scope of national cyber security effort. The measure is being carried out in accordance with the reporting of the Government assignment to the Swedish Security Service and the FRA on the development of the work to protect particularly security-sensitive activities (Fö2017/00535/SUND) and the reporting of the corresponding assignment issued to the Swedish Armed Forces in the authority's appropriation directions for 2018.

When: 2019 onwards

1.1.5. Preparing an action plan for authorities' participation in standardisation work in the scope of SIS TK318

Responsible authority: MSB

The MSB is to prepare and establish support for a three-year action plan for strategic and long-term work on standardisation regarding systematic and risk-based information security. The national engagement for national and international standardisation work including the ability to use the results from the standardisation work in the information and cyber security area needs to be strengthened. The action plan shall focus on the operating area of SIS TK318. The measure is being carried out together with the FMV/Swedish Certification Body for IT Security (CSEC) and relevant authorities and organisations.

When: 2019

1.1.6. Preparing supporting materials for the application of the new Protective Security Act

Responsible authorities: Swedish Security Service and Swedish Armed Forces

The Swedish Security Service and the Swedish Armed Forces are preparing new and updated guidelines and handbooks, training materials, etc. to support those who are to apply the new Protective Security Act and new regulations regarding protective security. The material is being prepared in coordination by both authorities for their respective supervisory area. The products will cover protective security in general and protective security analysis, information security, personnel security, physical security and protective security agreements. The work may in the long term be coordinated with the development of a national model to support systematic cyber security efforts.

When: 2019–2022

1.1.7. Organising an annual information security conference

Responsible authorities: MSB together with Swedish Armed Forces, FRA, Swedish Police Authority, FMV, PTS and Swedish Security Service.

Planning and holding an annual information security conference for municipalities, county councils, county administrative boards and authorities where the participants can exchange experiences and gain knowledge of the information security area.

The goal of the conference is to contribute to strengthening information security in the public sector by highlighting important issues and broadening knowledge of the area.

When: 2019–2022

1.1.8. Revision and supplementation of the MSB's regulations for government authorities

Responsible authority: MSB

Implementing a review of and supplementing the MSB's regulations and general guidelines regarding government authorities' information security (MSBFS 2016:1) and government authorities' reporting of IT incidents (MSBFS 2016:2). The objective is to clarify requirements on security measures and, where appropriate, harmonise with corresponding requirements for suppliers of critical services covered by the NIS regulations.

When: 2019

1.1.9. Developing and administering national terminology

Responsible authority: MSB

A process for development and administration of national terminology shall be developed. The term bank shall contain terminology for the specialised area of information and cyber security. The work shall include a mapping of various technical solutions for the provision of terms. The process for development and administration should take place in a broad consultation with relevant private and public actors. In the long term, the work may be coordinated with the development of a national model to support systematic cyber security efforts.

When: 2019

1.1.10. Investigating the possibility of greater control regarding the information security for municipalities and county councils

Responsible authority: MSB

The MSB will conduct an investigation of the need to introduce legal requirements of systematic and riskbased information security for municipalities and county councils. The legal requirements shall supplement already existing NIS regulations. The investigation should, besides requirements of systematic and risk-based information security, also analyse needs to introduce requirements on incident reporting and inspections. The investigation shall be able to answer what governance is needed to improve the information security in municipalities and county councils and is being carried out with the support of reference groups, including municipalities, county councils and county administrative boards.

The measure is being carried out with relevant stakeholders.

When: 2019–2020

1.1.11. Developing the MSB's implementation guide for systematic information security

Responsible authority: MSB

The MSB is developing the implementation guide for systematic information security with relevant stakeholders in the following prioritised areas: methods for classifying information in relation to security measures, risk analysis, incident management, continuity, including total defence aspects, and the organisation's governance and management.

The work may in the long term be coordinated with the development of a national model to support systematic cyber security efforts.

When: 2019–2020

1.1.12. Preparing a concept for basic security measures for information security

Responsible authority: MSB

Preparing a concept for basic security measures that shall be applicable to all kinds of organisations. The concept shall also include requirements on risk analysis.

The security measures are of particular importance for the organisations operating critical infrastructure.

The work may in the long term be coordinated with the development of a national model to support systematic cyber security efforts.

When: 2019–2020

1.1.13. Establishing and administer a reference list for IT security products

Responsible authorities: MSB in collaboration with FMV

The MSB will establish and administer a reference list of recommended protection profiles and IT security products that are third-party reviewed according to the international standard Common Criteria, ISO 15408. In addition, there will be a list of recommended encryption functions. The list will serve as a support to organisations when procuring IT security products to be used in public administration and in critical infrastructure in Sweden.

When: 2019 onwards

Objective 1.2. There is to be a national model to support systematic cyber security efforts.

1.2.1. Carrying out a preliminary study on a national model to support systematic cyber security efforts

Responsible authorities: MSB, Swedish Armed Forces, FRA, Swedish Police Authority, FMV, PTS and Swedish Security Service

The SAMFI authorities and other relevant actors will carry out a preliminary study on how a national model to support systematic cyber security efforts can be developed in concrete terms. The study shall describe the purpose of a national model and implement a stakeholder analysis. It shall also describe how work on such a model can be conducted so that all stakeholders can participate and contribute at an adequate level, how decisions are made, what parts a model should have and the order in which the parts can be developed. The preliminary study shall identify needs for and prepare any new measures in the follow-up

of the comprehensive action plan, which will be reported no later than 1 March 2020. The MSB has a coordinating role in this work.

When: 2019

Objective 1.3. Collaboration and cyber security information sharing is to be enhanced.

1.3.1. Spreading knowledge and experience on the work with information evaluation to other authorities and organisations

Responsible authority: Swedish Armed Forces

The Swedish Armed Forces intends to support other authorities and organisations with evaluation and classification of data volumes in technical systems. This shall aim to improve methods and approaches for evaluation of information and shall be carried out through knowledge and experience exchange. The activities will be based on requests from other authorities and organisations.

When: 2019–2022

1.3.2. Increasing the knowledge of information security in the Swedish Armed Forces' supervisory area for protective security

Responsible authority: Swedish Armed Forces

Information distribution regarding information security such as Swedish Armed Forces' requirements on approved security functions (KSF) and approved IT security products, through e.g. meetings with protective security managers at authorities that the Swedish Armed Forces have supervision over.

When: 2019–2022

1.3.3. Establishing collaboration possibilities for NIS actors

Responsible authority: MSB

This measure aims to establish a concept for the MSB, the NIS supervisory authorities and the National Board of Health and Welfare to reach out to suppliers of critical and digital services and to create better conditions for affected suppliers to exchange experiences with others in the respective sector. The MSB intends to provide information and support regarding systematic information security, inform about incident reporting and the work with connections to the EU. The supervisory authorities and National Board of Health and Welfare can provide information on supervision and other issues linked to the respective sector. The work with the measure includes preparing proposals on how such a concept can be formulated with external support and how financing shall be resolved. The measure is being carried out together with the NIS supervisory authorities and the National Board of Health and Welfare.

When: 2019 onwards

1.3.4. Deepening the cooperation between the FRA, the Swedish Security Service, the Swedish Armed Forces and the MSB

Responsible authorities: FRA, Swedish Security Service, Swedish Armed Forces and MSB

The FRA, the Swedish Security Service, the Swedish Armed Forces, and the MSB intend to deepen their cooperation in the cyber security area. This includes capa-

bility needs, organisational aspects and public-private partnership in the respective authority's area of responsibility. Since year-end, a working group has been exploring these issues. The authorities intend to present their findings, including suggested activities, to the Swedish Government in 2019.

When: 2019

1.3.5. Developing security requirements for specific IT products

Responsible authorities: FMV in collaboration with MSB

The FMV/CSEC shall collaborate with the MSB to participate in European[1] and international[2] working groups with the aim of drafting detailed requirements on IT security and evaluation methodology for specific types of IT products of interest to Sweden, such as USB memory sticks and database processors.

When: 2019 onwards

1.3.6. Expanding the collaboration with other authorities, international partners and civil companies in the defence sector regarding situational awareness and incident management capability

Responsible authority: Swedish Armed Forces

The Swedish Armed Forces intends to expand collaboration with other authorities, international partners and civil companies in the defence sector. The aim is to improve the situational awareness and the capability to manage incidents at authorities and companies in the defence sector that provide services and material to the Swedish Armed Forces. The measure is also aimed at international partners that the Swedish Armed Forces have cooperation agreements with.

When: 2019

Objective 1.4. There is to be appropriate supervision to create conditions for increasing society's cyber security.

1.4.1. Continued development of regulations for protective security

Responsible authorities: Swedish Security Service and the Swedish Armed Forces

The Swedish Security Service and Swedish Armed Forces will further develop regulations on protective security for their respective supervisory area, due to the report from the commission on certain protective security issues, Supplementing the new Protective Security Act (SOU 2018:82).

When: 2019–2022

1.4.2. Supporting and coordinating development of the NIS regulation regarding security measures

Responsible authority: MSB

Within the framework of existing NIS cooperation, a working group will be established to share experiences and support the NIS supervisory authorities and the National Board of Health and Welfare in their work on regulations on security measures.

When: 2019–2020

1. http://www.sogis.org
2. http://www.commoncriteriaportal.org

1.4.3. Preparing support for and developing coordinated supervision within NIS

Responsible authority: MSB

Within the framework of existing NIS cooperation, a working group will be established to provide support and create conditions for effective and equal supervision. The coordination aims to create common guidelines and the possibility to harmonise assessments in supervision in various sectors.

When: 2019

Strategic priority 2. Enhancing network, product and system security

Objective 2.1. Electronic communications are to be effective, secure and robust and are to meet the needs of their users.

2.1.1. Preparing support for acquiring robust electronic communications

Responsible authority: PTS

The PTS is preparing support for acquiring robust electronic communications. The robustness in electronic communications is affected by several factors. One factor is the users' acquisition of communications networks and communications services. There is a need for support to companies, authorities and other organisations that in various ways are dependent on robust electronic communications in their activities, regarding how they can acquire robust electronic communication. The support shall simplify matters for activities to evaluate their own needs for secure electronic communications, convert these needs to requirements prior to an acquisition and support to follow up the requirements during the contract period.

When: 2019–2020

2.1.2. Implementing a project to reduce dependence on central functions in electronic communications networks and services

Responsible authority: PTS

The PTS is implementing a project to reduce dependence on central functions in electronic communications networks and services The project begins with an analysis done together with operators to assess the possibility of reducing dependence on central functions. Findings from the analysis are then applied in a pilot project where the possibility of implementing regional autonomous networks is tested in a geographically delimited part of the country. The measure begins with the final report from the Särimner project.

When: 2019–2022

2.1.3. Investigating the possibility of increasing traceability in trusted services

Responsible authority: PTS

The PTS is investigating the possibility of increasing traceability in trusted services There is a need to investigate the possibility of greater traceability between underlying equipment for the generation of encryption keys and the services provided on the inner market. The aim is to increase confidence in the system by adding greater protection for individual countries and trusting parties in a transaction based on a qualified certificate.

PTS will work for supplemental rules being developed in the EU in areas where a deficient harmonisation on the inner market for qualified trusted services leads to a reduced trust for the services.

When: 2019 onwards

2.1.4. Development and acquisition of IT security projects

Responsible authorities: Swedish Armed Forces and FMV

Development, acquisition, and security of general IT security products primarily for the Swedish Armed Forces needs but with possible further use by other authorities that can benefit from the review being done. For example, meny suppliers to authorities should be able to and want to use reviewed and approved products when they handle the authorities' security-sensitive assets.

When: 2019 onwards

2.1.5. Establishing new secure and robust communications for actors with special protective security needs

Responsible authority: Swedish Armed Forces

The Swedish Armed Forces are further developing the possibility of secure and robust communications for actors in the defence sector and actors in total defence with special protective security needs.

When: 2019–2022

2.1.6. Establishing new secure and robust communications services for actors in public order, security, health and defence

Responsible authority: MSB

The MSB is providing new secure and robust communications services for actors in total defence and developing the ability to share sensitive and security classified information. The measure means realising services such as encrypted videoconferencing to the level of Restricted in Swedish Government Secure Intranet (SGSI), encryption in Rakel, the Swedish national digital communications system used by the emergency services and others in the fields of civil protection, public safety and security, emergency medical services and healthcare, and establishment of a supplemental data services in Rakel. These services can be utilised by these actors, after suitability assessment, if they themselves have no other technical means to share sensitive and security classified information.

When: 2019–2022

2.1.7. Establishing a federation service for SGSI affiliated actors

Responsible authority: MSB

The MSB shall together with relevant actors establish and administer a federation service in the Swedish Government Secure Intranet (SGSI). By establishing and administering a federation service a central function is created between the SGSI-connected authorities. With a central federation service possibilities are provided, by using encryption, to increase protection of information when it is to be shared between various actors, which increases the ability for more secure information sharing.

When: 2019

2.1.8. Monitoring and contributing to the development of secure communication for other organisations

Responsible authority: Swedish Armed Forces

The Swedish Armed Forces will contribute experience regarding realisation of secure system solutions in the strategic development efforts of e.g. network infrastructures, communication solutions, etc. within the scope of total defence.

When: 2019–2022

Objective 2.2. Electronic communications in Sweden are to be available independent of functions outside the country's borders.

2.2.1. Investigating electronic communications independence of functions abroad

Responsible authority: PTS

The PTS is investigating what it conceptually means with "electronic communications independence of functions abroad", and the degree to which electronic communications functions today independent of functions abroad.

The investigation will analyse the extent to which operators of special significance to the public sector can provide electronic communications services independent of functions abroad and map any dependencies that currently make this impossible. The investigation can form the basis of changes in the PTS regulations on peace-time planning for total defence needs of telecommunications (PTSFS 1995:1).

When: 2019–2020

Objective 2.3. The supervisory authority's need for being able to take adequate measures is to be met.

2.3.1. Investigating the possibility to decide on specific security measures for actors in the electronic communications sector

Responsible authority: PTS

The PTS is investigating the possibility of deciding on measures that aim to order operators to quickly undertake security measures to counter specific vulnerabilities in their networks or services.

When: 2019–2022

2.3.2. Investigating the possibility of making traceable time and frequency available to actors outside the electronic communications sector

Responsible authority: PTS

The PTS is investigating the possibility of making traceable time and frequency available to actors outside the electronic communications sector, Since 2015, the PTS maintains a national system for production and distribution of traceable time and frequency in the electronic communications sector. The purpose of the system is to contribute robustness and redundancy and reduce the dependence on GNSS (Global Navigation Satellite System) for time and frequency synchronisation within the sector. Actors from other sectors, including the financial sector and energy sector, have in various contexts expressed interest in a PTP connection to the service.

For society, provisioning to more actors would be positive from a preparedness perspective. For actors outside the electronic communication sector to be able to connect, certain other investigations must be done, however.

When: 2019–2020

Objective 2.4. Access to secure data encryption systems for IT and communications solutions are to meet society's needs.

2.4.1. Drafting a specified proposal on a national strategy and action plan for secure encryption functions

Responsible authorities: FRA, Swedish Armed Forces and MSB

Based on the Information Security Commission in NISU 2014 appendix 4 (SOU 2015:23), a proposal is being drafted on a national strategy and action plan for handling and transferring information in the electronic communication network and IT systems using encryption also for the information that does not fall under the mandate of the Communication Security Service. The strategy shall comprise overall objectives for society's information security related to cryptography, and how Sweden shall maintain security and integrity in critical IT infrastructure using cryptographic functions.

The result shall constitute a report with specified proposals on national strategy and action plan for cryptographic functions after consultation with the Swedish Armed Forces, the FRA, and the MSB. The proposal shall contain a cost accounting and be able to be used as basis for a concrete assignment decision for relevant authorities.

When: 2019

2.4.2. Continued development of communication security systems

Responsible authorities: Swedish Armed Forces and FMV

The Swedish Armed Forces is setting requirements on new and further developed communication security systems procured by the FMV. The Swedish Armed Forces is carrying out reviews and approval of the products delivered.

When: 2019 onwards

2.4.3. Preparing a process for handling communication security

Responsible authorities: Swedish Armed Forces in cooperation with FMV, FRA and MSB

The authorities with responsibility for various parts of communication security will develop and update processes that can handle decisions on allocation and distribution of communication security material to the actors covered by the new Protective Security Act. The processes will ensure that the appropriate actors gain access to communication security. The new Protective Security Act will mean that additional actors, both authorities and individuals, will be covered by requirements on the use of encryption systems approved by the Swedish Armed Forces to protect security classified information (communication security).

When: 2019

2.4.4. Introducing encrypted mobile speech and text message function at the Restricted level

Responsible authority: Swedish Armed Forces

The Swedish Armed Forces will introduce encrypted mobile speech and text message function at the Restricted level There is a major and growing need to exchange protective security classified messages within the Swedish Armed Forces and total defence. The phone shall support collaboration needs for authority management, senior managers and their primary contacts internally and externally. The phone is also intended for function experts and operational needs. The phone supports a wide range of applications that make it possible to replace a regular business mobile phone. Agreement on the use and handling in total defence is being drafted by the Swedish Armed Forces together with the MSB.

When: 2019

2.4.5. Introducing secure speech at the level Secret in total defence

Responsible authorities: Swedish Armed Forces in cooperation with FMV, FRA and MSB

The Swedish Armed Forces in cooperation with the FMV, the FRA, and the MSB shall introduce secure speech at the Secret level in total defence. The need for secure speech in total defence is extensive and increasing. The current system will be phased out. A new system therefore needs to be implemented. This consists of an encrypted mobile telephone with a key server for easier key management.

When: 2020

2.4.6. Developing and introducing message encryption at the level Secret in total defence

Responsible authorities: Swedish Armed Forces in cooperation with the FMV, the FRA, and the MSB

The Swedish Armed Forces in cooperation with FMV, FRA and MSB shall introduce message encryption at the level Secret to total defence actors. There is an extensive and increasing need in total defence to be able to exchange security classified messages between actors that do not have access to interconnected systems for information of that classification. The systems used today (Kryfax and Krypto-PC) will be phased out. Therefore a new system to meet the need will be developed and implemented.

When: 2019 – 2022

Objective 2.5. Security in industrial information and control systems is to increase

2.5.1. Providing expertise and awareness materials on IT security in the build-up of new intelligent transportation systems

Responsible authority: MSB

Working on awareness-raising efforts and strengthening the prevention work for IT security during the build-up of the new intelligent transport systems. The work is being carried out together with FOI and other responsible bodies.

When: 2019–2021

2.5.2. Promoting the use of protected satellite services for time, speed and position for critical infrastructure

Responsible authority: MSB

The MSB will promote the use of protected satellite services for time, frequency and position for critical infrastructure. Time, frequency and position are critical factors for many functions in our society. An outage of GNSS (Global Navigation Satellite System, such as GPS) means that many systems and services can no longer function normally. Examples of systems that can be affected by disruptions in services that provide time, frequency, and position are control systems for water treatment, technical systems used in agriculture, operation of electricity networks, and communication systems.

Emergency response vehicles from the police, fire brigade and ambulance services receive faster and more exact information from GNSS on destination and route. Besides vehicles, GNSS is today an important aid for aircraft, trains and ships. Commercial traffic has long used satellite navigation as an aid to find recipients of cargo and to monitor where vehicles are.

In the future, GNSS will also be important for wireless applications in smart cities such as self-driving vehicles. There is currently a clear threat against GNSS in the form of scrambling and spoofing. Galileo PRS is a European GNSS services intended for authorised users who are in need of a high robustness against scrambling and spoofing and high availability. There are therefore major advantages to work for critical functions in society that today use various GNSS services and are in continued need of mobile solutions to move to the encrypted service Galileo PRS. Fixed installations that have critical dependencies on exact time and or frequency, should be coordinated with the PTS service for correct and traceable time and frequency.

When: 2019–2022

2.5.3. Implementing a national initiative on improved security in cyber-physical systems

Responsible authority: MSB

The MSB shall together with relevant stakeholders implement a national initiative that includes technical, preventive, capability improving, and coordinated activities to improve the security of industrial information and control systems and Internet of Things (IoT). These activities shall result in the development and provision of training, guides, technical tools, strengthening existing collaboration structures, and provide support for skills provisioning. The overall objective is to strengthen society's collective ability to prevent and handle both shortages and inaccuracies as well as IT attacks on such functions in society that are dependent on industrial information and control system (ICS).

When: 2019–2020

Strategic priority 3. Enhancing capability to prevent, detect and manage cyberattacks and other IT incidents

Objective 3.1. The capability to prevent, detect and manage cyberattacks and other IT incidents in society is to be improved

3.1.1. Increasing incident management capability for qualified threat actors

Responsible authorities: Swedish Security Service, FRA and the Swedish Armed Forces

The Swedish Security Service, the FRA, and the Swedish Security Service are developing the capability to discover cyberattacks and attempted attacks by qualified adversaries and support the most security-sensitive activities with incident management in such attacks and attempted attacks. The measure is being carried out in accordance with the reporting of the Government assignment on the work to protect particularly security-sensitive activities (Fö2017/00535/SUND). The Swedish Armed Forces are carrying out similar measures in accordance with the reporting of assignments issued to the Swedish Armed Forces in the authority's appropriation directions for 2018.

When: 2019–2025

3.1.2. Providing awareness raising material on reducing disruption sensitivity when using wireless communication in industrial information and control systems in critical infrastructure

Responsible authority: MSB

The MSB is providing awareness raising material on reducing disruption sensitivity when using wireless communication in industrial information and control systems in critical infrastructure. With the digital transformation and technical development, society is becoming increasingly dependent on various wireless communication technologies. This can for example concern governance and control of various industrial information and control systems over WiFi. In the use of wireless communication, there is an electromagnetic threat dimension in addition to traditional IT threats. The measure aims to work to increase knowledge of electromagnetic threats and the importance of reducing disruption sensitivity in industrial information and control systems and increasing the ability to detect disruptive incidents.

When: 2019–2022

3.1.3. Establishing a sensor system for NIS operators

Responsible authority: MSB

Through CERT-SE, the MSB will offer operators of essential and digital services (NIS operators) the possibility of connecting to a sensor system. The sensor system provides connected actors an expanded capability to discover and protect themselves from serious IT attacks. Through improved situational awareness and information sharing, the sensor system also contributes to a greater ability in society to prevent and handle IT attacks. The system shall constitute a complement to commercial products and be designed with a high level of security and integrity protection.

When: 2019–2022

3.1.4. Continued development of a national Cyber Range

Responsible authority: MSB

The MSB is, with relevant stakeholders, continuing to develop a national Cyber Range (practice environment). To secure Swedish critical information infrastructure and critical IT systems, practically oriented exercises are needed. The measure aims to develop a national Cyber Range for education, training and practice in information and cyber security within ICS.

When: 2019–2020

3.1.5. Creating conditions for cooperation within the framework of the MSB's CSIRT activities

Responsible authority: MSB

The measure aims to facilitate collaboration and when necessary coordination of measures within the scope of the CSIRT activities (Computer Security Incident Response Team) and the MSB/CERT-SE's tasks to support society in the work of preventing and handling IT incidents. In this work, both the needs of access to workplaces and protected meeting spaces are met.

When: 2019–2020

Objective 3.2. Relevant stakeholders are to be able to take coordinated action to manage cyberattacks and other serious IT incidents

3.2.1. Investigating the possibility of sharing operational information and incident information securely between SAMFI authorities

Responsible authorities: MSB, FRA, Swedish Security Service, Swedish Armed Forces, PTS, FMV and Swedish Police Authority

The SAMFI authorities shall investigate the possibility of sharing information in a secure way to facilitate the collaboration between relevant authorities. An example could be information on IT related threats to improve the respective authority's incident management and security requirements.

When: 2019–2020

3.2.2. Working within NSIT to increase the capability to counter complex and serious IT threats

Responsible authorities: Swedish Security Service, Swedish Armed Forces and FRA

National Cooperative Council against Serious IT Threats (NSIT) is a collaboration between the Swedish Security Service, the Swedish Armed Forces, and the FRA. NSIT analyses and assesses threats and vulnerabilities regarding serious or qualified cyberattacks against our most security-sensitive national interests. NSIT develops the collaboration and implements activities aiming to impede a qualified attacker from accessing or damaging sensitive civil or military resources.

When: 2019 onwards

3.2.3. Establishing a collaborative forum for various authorities' incident management functions

Responsible authority: MSB together with the Swedish Police Authority

The MSB together with the Swedish Police Authority will establish a cooperation forum for information exchange on statistics and current events related to incident management.

When: 2019 onwards

Objective 3.3. There is to be a developed cyber defence for the most security-sensitive activities in Sweden, with a strengthened military capability to meet and manage attacks from qualified opponents in cyberspace

3.3.1. Supplying military strategic situation reports on the status in the Swedish Armed Forces' information and command support system, threats and risks

Responsible authority: Swedish Armed Forces

The Swedish Armed Forces delivers a military strategy situational awareness weekly and presents it to its supreme commander and the highest chain of command. The report can when necessary be used for the entire defence sector, for example in the scope of NSIT.

When: 2019–2022

3.3.2. Providing TDV to the most security-sensitive activities

Responsible authorities: FRA in cooperation with Swedish Security Service and the Swedish Armed Forces

In collaboration with the Swedish Security Service and the Swedish Armed Forces, the FRA conducts continued development of the technical detection and warning system (TDV) and its deployment at the most security-sensitive activities. The measure is being carried out in accordance with the reporting of the Government assignment on the work to protect particularly security-sensitive activities (Fö2017/00535/SUND) and the appropriation directions for the 2019 budget year for the FRA.

When: 2019 onwards

3.3.3. Strengthening the ability to conduct defensive and offensive operations against a qualified opponent in cyberspace

Responsible authorities: Swedish Armed Forces with support from FRA

The Swedish Armed Forces with support from the FRA are strengthening the ability to conduct defensive and offensive operations against a qualified opponent in cyberspace

The assignment has been set in the appropriation directions to the Swedish Armed Forces and the FRA. Proposals on measures have been discussed with the Ministry of Defence in budget request 19.

When: 2019–2022

3.3.4. Developing a military Cyber Range

Responsible authority: Swedish Armed Forces

The Swedish Armed Forces has begun the establishment of a military Cyber Range to strengthen the Armed Forces possibilities to conduct training, education and exercises in cyber defence. In addition to this, possibilities are also being created to be able to evaluate both capability and technology in cyber space.

When: 2019–2020

Strategic priority 4. Increasing the possibility of preventing and combating cybercrime

Objective 4.1. The law enforcement authorities shall have the preparedness and capability to combat cybercrime in an effective and appropriate manner

4.1.1. Strengthening cooperation in incident reporting on criminal activities

Responsible authorities: Swedish Police Authority together with MSB

The Swedish Police Authority will, together with the MSB, establish a process for cooperation on incident reporting to increase prosecutions and strengthen the possibility of crime prevention.

When: 2019

4.1.2. Establishing regional cybercrime centres

Responsible authority: Swedish Police Authority

The Swedish Police Authority is establishing regional cybercrime centres in the seven police regions to increase the capability to investigate and prevent IT-related crime and increase the quality of the crime prevention work.

When: 2019–2022

4.1.3. Increasing cooperation with other law enforcement authorities

Responsible authority: Swedish Police Authority

The Swedish Police Authority will increase the cooperation with other law enforcement authorities through regular meetings and joint participation in courses to increase the ability to fight IT-related crime.

When: 2019–2022

Objective 4.2. The work to prevent cybercrime shall be developed

4.2.1. Using European Community resources for crime prevention campaigns

Responsible authorities: Swedish Police Authority together with MSB

The Swedish Police Authority will, together with the MSB, increase cooperation with Europol on crime prevention activities by using the resources that that Europol and ENISA offer, for example during European Cyber Security Month (ECSM).

When: 2019–2022

4.2.2. Cooperating with the financial and transaction markets

Responsible authority Swedish Police Authority

The Swedish Police Authority participates in cooperation with the financial and transaction markets for more secure payment methods to reduce IT-related crime over the transaction systems.

When: 2019–2022

Strategic priority 5. Increasing knowledge and promoting expertise

Objective 5.1. Knowledge in society as a whole regarding the most urgent vulnerabilities and needs for security measures is to increase

5.1.1. Establishing strategic approaches for monitoring and evaluating society's ability in the cyber security area

Responsible authority: MSB

The MSB is establishing processes and structures to maintain a current picture of society's ability in cyber security. This includes long-term planning for implementation of mapping and regular follow-up of implementation at actors of importance to critical functions and ability regarding strategic and operational intelligence. The measure is being carried out with authorities who exercise supervision and implement mappings and studies with bearing on the cyber security area.

When: 2019–2020

5.1.2. Further develop hardware analysis capability

Responsible authority: FRA

The FRA is further developing the capability to analyse hardware-related threats and vulnerabilities. This is accomplished through the build-up of a hardware lab and reinforcement of skills and staff in the field.

When: 2019 onwards

Objective 5.2. The knowledge of individual digital technology users regarding the most urgent vulnerabilities and needs for security measures is to increase

5.2.1. Implementing a targeted information campaign to raise security awareness

Responsible authority: Swedish Armed Forces

The Swedish Armed Forces is implementing a targeted information campaign primarily directed at those active in all parts of the Armed Forces and secondarily addressing other defence authorities. The campaign is a new way to reach out to the target group. It is intended to contain both interest-evoking films and more indepth information. The objective of the campaign is to raise security awareness among individual employees by pointing out risky behaviours, possible consequences of inadequate security and how to reduce these risks. The campaign may be followed up with more campaigns of a similar type.

When: 2019–2022

Objective 5.3. Higher education, research and development of high quality are to be conducted in the areas of cyber security and of IT and telecom security in Sweden.

5.3.1. Developing conditions for competence provisioning

Responsible authorities: FRA, Swedish Security Service and Swedish Armed Forces

The FRA, the Swedish Security Service, and the Swedish Armed Forces need to develop conditions for competence provisioning to achieve the goal in the reporting of the Government assignment to the Swedish Security Service and the FRA on the development of the work to protect particularly security-sensitive activities

(Fö2017/00535/SUND) and reporting of the corresponding assignment issued to the Swedish Armed Forces in the authority's appropriation directions for 2018. In the long term, the work should involve more organisations (such as the SAMFI authorities) and work for national competence provisioning in the cyber security area.

When: 2019–2025

5.3.2. Establishing a model for competence development

Responsible authorities: Swedish Armed Forces together with FRA and the Swedish Security Service

The Swedish Armed Forces together with the FRA and the Swedish Security Service are establishing a cohesive model for competence development and the flows within the Swedish Armed Forces and between the Swedish Armed Forces and the FRA and the Swedish Security Service. The measure is also being carried out with other actors in the area, both nationally and internationally.

When: 2019–2022

5.3.3. Advancing research and technical development in the cyber defence area

Responsible authority: Swedish Armed Forces

The Swedish Armed Forces are strengthening and conducting further development of research and technical development in the cyber defence area. The aim is to increase the knowledge of and ensure access to methods and technology on the cutting edge of research. The results shall be able to convert to applications that contribute to the ability to conduct operations in cyberspace. The Swedish Defence Research Agency (FOI), the Swedish Defence University (FHS), etc. support the research.

When: 2019 onwards

5.3.4. Establishing adapted selection and recruitment in the cyber direction

Responsible authorities: Swedish Armed Forces together with FRA

The Swedish Armed Forces and the FRA are developing a concept for military service training and a structure for further education in the cyber defence area and implementing and inventory of competence requirements. An example of the measure is cyber soldier training. The measure is also being carried out with other actors in the area, both nationally and internationally.

When: 2019–2022

5.3.5. Implementing a preliminary study on skills provisioning in the information security and cyber security area in society

Responsible authority: MSB

The MSB intends to analyse the possibilities of supporting the development of skills provisioning in the information security and cyber security area. The MSB will also submit proposals on measures in the form of governance and support that this would presuppose in various kinds of courses, such as professional courses, further education, university and upper secondary school.

The work should be coordinated with activities already under way that are being carried out by other actors. The measure is being carried out together with relevant stakeholders in society.

When: 2019–2020

Objective 5.4. Both cross-sectoral and technical cyber security training is to be carried out regularly in order to enhance Sweden's capability to manage the consequences of serious IT incidents

5.4.1. Carrying out subcomponents in TFO 2020

Responsible authorities: Swedish Armed Forces together with MSB

The Swedish Armed Forces are planning, implementing and evaluating subcomponents in the Total Defence Exercise 2020 (TFÖ 2020) together with the MSB. The various activities in the exercise include exercise components to be able to transfer security classified information

When: 2019–2020

5.4.2. Carrying out NISÖ 2021

Responsible authority: MSB

The MSB is carrying out the National Information Security Exercise 2021 (NISÖ) in collaboration with the Swedish Armed Forces, the Swedish Security Service, the PTS and the Swedish Police Authority. The previous exercise took place in 2018. The purpose of the exercise is to give private and public actors the possibility to exercise together. This is to strengthen society's collective ability to handle IT related disruptions in society where the actors quickly need to coordinate to be able to take relevant steps.

When: 2019–2021

5.4.3. Carrying out recurring joint exercises with cyber security authorities on the handling of IT incidents

Responsible authority: MSB

The MSB is carrying out recurring joint exercises with cyber security authorities on the handling of IT incidents. The purpose is to develop the joint ability to handle IT incidents.

When: 2019–2020

5.4.4. Carrying out annual information and cyber security exercise SAFE Cyber

Responsible authorities: Swedish Armed Forces in cooperation with FRA, MSB and Swedish Security Service

The Swedish Armed Forces is, in cooperation with the FRA, the MSB, and the Swedish Security Service, carrying out an annual information and cyber security exercise called SAFE Cyber. The exercise comprises collaboration with the purpose of securing important functions in the event of computer and network operations targeting Sweden. Focus of the exercise is IT security including risk and incident management, threat assessment, situational awareness, reporting, management, coordination and decision-making. The exercise is directed at staff from authorities responsible for cyber defence of Sweden and authorities and companies responsible for systems and services with connections to the Swedish Armed Forces. Structure and theme for the annual exercises vary and are adapted to external developments.

When: 2019–2022

Strategic priority 6. Enhancing international cooperation

Objective 6.1. International cooperation on cyber security is to be enhanced, as part of the objective of a global, accessible, open and robust internet characterised by freedom and respect for human rights

6.1.1. Working for international harmonisation of rules and requirements for information security

Responsible authority: Swedish Armed Forces

The Swedish Armed Forces is working for international harmonisation of rules and requirements for information security. This is done through collaboration to share and develop knowledge in various areas and to harmonise regulations and information security measures. The work is conducted in e.g. ITTF (Implementation Tempest Task-Force), various groups in the crypto field and, among others, in the Federated Mission Networking (FMN) community. FMN is a concept to create shared networks to support multinational missions. The security cooperation within this framework is therefore of major significance to the protection of Sweden's contribution to such missions.

When: 2019–2022

6.1.2. Establishing a resource at Europol

Responsible authority: Swedish Police Authority

The Swedish Police Authority is positioning a resource to be placed at the Joint Cybercrime Action Taskforce (J-CAT) at Europol in The Hague to facilitate the cooperation with other countries and authorities to investigate crime.

When: 2019

6.1.3. Developing and improving standards and methodology for requirements and control of cyber security in IT products

Responsible authority: FMV

The FMV/CSEC will contribute in Swedish and international standardisation bodies and forums to develop and improve standards to set requirements and evaluate IT security and cryptography.

When: 2019 onwards

Objective 6.2. Cyber security is to be promoted as part of the ambition to safe-guard free flows in support of innovation, competitiveness and societal development

6.2.1. Participating in international cooperation forums for industrial security

Responsible authority: FMV

The FMV already participates actively in the international cooperation forum Multinational Industrial Security Working Group (MISWG). Within MISWG, there is a number of working groups in various areas. By participating in MISWG Ad Hoc Working Group (AHWG) 7 on Cyber Security, knowledge is gained on how other countries' industrial security authorities work with requirement specification of cyber security towards domestic industry. The knowledge will contribute to the build-up of the Swedish Designated Security Authority (DSA) and provide input that contributes to the work on a national model to support systematic cyber security efforts.

When: 2019

6.2.2. Continuing to participate in the cooperation group and CSIRT network in the scope of the NIS Directive's implementation and application

Responsible authority: MSB

The MSB will continue to participate in the cooperation group and CSIRT network in the scope of the NIS Directive's implementation and application. As a national contact point and national CSIRT, the MSB is participating in the EU cooperation to harmonise the implementation of the NIS Directive in general in the NIS Cooperation Group, and cooperate regarding incident management in CSIRT's Network.

When: 2019 onwards

Follow-up and continued work

Follow-up and continued work

To realise the Swedish Government's goals in the cyber security area, strategic priorities formulated in the national cyber security strategy have been converted to concrete measures. Progress on implementing the measures will be followed up. In upcoming reports of the comprehensive information and cyber security action plan, the authorities also intend to jointly analyse what other measures are required to fulfil objectives of the strategy based on needs in society.

The continued work on the action plan will be started as soon as possible after the 2019 report has been submitted to the Government. The work will be conducted within the scope of the joint working group established by the SAMFI authorities to carry out the assignment. By beginning the work early on, the chances increase of resource allocation, coordination and joint planning.

In 2019, a method for administration and follow-up will be developed. The aim is to create conditions to follow up the implementation of the measures described in the action plan. The method should comprise the working processes needed for follow-up, analysis and formulation of supplemental activities to ensure expected results.

Follow-up will take place in cooperation with relevant actors. This includes the Agency for Digital Government, the Swedish Data Protection Agency, the National Board of Health and Welfare and supervisory authorities in the scope of the NIS regulation, the Swedish Association of Local Authorities and Regions (SKL), companies and other organisations.

Concluding words

Concluding words

Work on the 2019 report on a comprehensive cyber security action plan for the years 2019–2022 has constituted a collaboration platform that according to the authorities contributed to greater coordination of measures and activities. Even if planning and resource allocation of the measures now included in the action plan had largely already been done when work on the action plan begun, coordination of the upcoming implementation of certain measures and activities was able to take place. This applies to coordination in the form of expanded information exchange between authorities that implement measures with adjacent purposes, structures and target groups. For a few of the measures, more extensive coordination was possible. The authorities have for example agreed on adding a measure to jointly conduct a preliminary study of a national model to support systematic cyber security efforts . The authorities assess that the conditions for further coordination of measures and activities in the years 2020–2022 will improve as the implementation of the action plan continues.

Even if a needs analysis has not been included in this year's action plan, needs for certain future measures have been identified. In some cases, these needs included in this year's report. However, there are a number of extensive areas that the authorities deemed to be of major significance to strengthening cyber security in society, but were not fully handled within the measures in the 2019 edition of the action plan. The reasons for this may be insufficient resources or mandates. In some cases, the work was deemed to be facilitated if it takes place in the scope of a Government assignment.

Swedish Civil Contingencies Agency (MSB)
SE-651 81 Karlstad Tel +46 (0)771-240 240 www.msb.se
Publ.no. MSB1393 - May 2019 ISBN: 978-91-7383-944-0