Comprehensive Information and Cyber Security Action Plan for the years 2019–2022

Report, March 2020

MSB Swedish Civil Contingencies Agency
FRA
FMV
FÖRSVARSMAKTEN
PTS
Polisen
Säkerhetspolisen

Comprehensive Information and Cyber Security Action Plan for the years 2019−2022 – Report 2020

Cover photo: Shutterstock
Printing: DanagårdLiTHO
Layout: Advant

Order No.: MSB1597 – June 2020
ISBN: 978-91-7927-049-0

Swedish edition: MSB1478 – March 2020

Innehåll

Summary 6

Introduction 8

National strategy 10

Work of the public authorities on the Action Plan 11

New developments presented in the Report, March 2020 13

External Collaboration 14

Following-up 16

Strategic priority 1. Securing a systematic and comprehensive approach in cyber security efforts 17

Strategic priority 2. Enhancing network, product and system security 18

Strategic priority 3. Enhancing capability to prevent, detect and manage cyberattacks and other IT incidents 19

Strategic priority 4. Increasing the possibility of preventing and combating cybercrime 19

Strategic priority 5. Increasing knowledge and promoting expertise 20

Strategic priority 6. Enhancing international cooperation 21

Measures 22

Strategic priority 1. Securing a systematic and comprehensive approach in cyber security efforts 24

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. 24

Objective 1.2. There is to be a national model to support systematic cyber security efforts. 28

Objective 1.3. Collaboration and cyber security information sharing is to be enhanced. 28

Objective 1.4. There is to be appropriate supervision to create conditions for increasing the society's cyber security. 30

Strategic priority 2. Enhancing network, product and system security 31

Objective 2.1. Electronic communications are to be effective, secure and robust and are to meet the needs of their users. 31

Objective 2.2. Electronic communications in Sweden are to be available independent of functions outside the country's borders. 33

Objective 2.3. The supervisory authority's need for being able to take adequate measures is to be met. 33

Objective 2.4. Access to secure data encryption systems for IT and communications solutions are to meet the society's needs. 34

Objective 2.5. Security in industrial information and control systems is to increase. 36

Strategic priority 3. Enhancing capability to prevent, detect and manage cyberattacks and other IT incidents 37

Objective 3.1. The capability to prevent, detect and manage cyberattacks and other IT incidents in the society is to be improved. 37

Objective 3.2. Relevant stakeholders are to be able to take coordinated measure to manage cyberattacks and other serious IT incidents. 38

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 counter and manage attacks from "professional" opponents in cyberspace. 39

Strategic priority 4. Increasing the possibility of preventing and combating cybercrime 40

Objective 4.1. The law enforcement authorities are to have the preparedness and capability to combat cybercrime in an effective and appropriate manner. 40

Objective 4.2. The efforts to prevent cybercrime is to be further developed. 40

Strategic priority 5. Increasing knowledge and promoting expertise 41

Objective 5.1. Knowledge in the society as a whole regarding the most urgent vulnerabilities and needs for security measures is to increase. 41

Objective 5.2. The knowledge of individual digital technology users regarding the most urgent vulnerabilities and needs for security measures is to increase. 42

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. 43

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. 44

Strategic priority 6. Enhancing international cooperation 46

Objective 6.1. International cooperation on cyber security is to be enhanced, within the framework of the objective of a global, accessible, open and robust internet characterised by freedom and respect for human rights. 46

Objective 6.2. Cyber security is to be promoted as part of the ambition to safeguard free flows in support of innovation, competitiveness and societal development. 47

Concluding words 48

Appendix 1: List of measures 50

Current measures 51

Measures implemented 57

Written-off measures 59

Appendix 2: Assignment regarding a Comprehensive Information and Cyber Security Action Plan for the years 2019–2022 62

Summary

Summary

The Comprehensive Information and 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 National Post and Telecom Agency (PTS), the Swedish Police Authority and the Swedish Security Service individually, together or in collaboration with other parties intend to undertake to increase information and cyber security in the society. A number of measures have been concluded, some have been updated, and some new ones have been added, as discussed in the 2020 Report. Selected results of the measures implemented are described in the chapter "Follow-up".

The measures in the Action Plan are within the scope of the areas of responsibility and assigned tasks that the public authorities have. However, the Action Plan should not be regarded as a complete account of all of the measures that the various public authorities intend to carry out within their respective activities in the information and cyber security area.

All measures in the Action Plan connect to one or more of the six strategic priorities that the Government has decided in the national cyber security strategy (official letter 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 public authority is responsible for the respective measure, who contributes in the work and what the measure covers.

Introduction

Introduction

In July 2018, the Swedish Government assigned the public authorities with a particular responsibility in the field of information and cyber security, MSB, FRA, FMV, Swedish Armed Forces, PTS, the Swedish Police and Swedish Security Service the task of developing and preparing a Comprehensive Information and Cyber Security Action Plan for the years 2019-2022.

The public authorities in this assignment have key areas of responsibility and tasks in promoting information and cyber security in the society. They also have a well-established collaborative culture via the interagency Cooperation Group for Information Security (SAMFI). The Government considers that an in-depth collaboration between these public 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 a better platform to be able to analyse 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 public authorities' measures and activities.

The Action Plan constitutes a collective account of what measures the authorities plan to undertake on their own initiative in the scope of their existing areas of responsibility and assigned tasks, to contribute to achieving the strategic priorities in the national strategy. The Action Plan does not constitute a steering document for the public authorities' activities.

The work with the measures in the Action Plan shall be reported to the Government annually on 1 March. According to the Government assignment, 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 public authorities' ordinary reporting to the Swedish Government.

The measures are conducted within the given financial limits, either by a single public authority individually or in the context of joint projects. Ongoing work relating to information and cyber security is reported where it is deemed to be relevant. Therefore the plan should not be seen as a complete account of all of the measures that the various public authorities intend to carry out within their respective areas of activity.

National strategy

In the national strategy for social information and cyber security (official letter 2016/17:213) the Government of Sweden expresses comprehensive prioritisations intended to constitute a platform for Sweden's continued development work within the field of information and cyber security. The main aims of the strategy are to help to create the long-term conditions for all stakeholders in the society to work effectively on cyber security, and raise the level of awareness and knowledge throughout the society. The strategy also aims to support the efforts already underway with the goal of strengthening the 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 strategy covers six strategic priorities:

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

The strategy encompasses the whole of the society, that is to say central government authorities, municipalities and regions, companies, non-governmental organisations, and private individuals.

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

Securing a systematic and comprehensive approach in cyber security efforts

- Central government authorities, municipalities, regions, companies and other non-governmental 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 supervision to create conditions for increasing the society's cyber security.

Enhancing network, product and system 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 the society's needs.
- Security in industrial information and control systems is to increase.

Enhancing capability to prevent, detect and manage cyberattacks and other IT incidents

- The capability to prevent, detect, and manage cyberattacks and other IT incidents in the 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 security-sensitive activities in Sweden, with a strengthened military capability to respond to and manage attacks from experienced "professional" opponents in cyberspace.

Increasing the possibility of preventing and combating cybercrime

- The law enforcement authorities are to have the preparedness and capability to combat cybercrime in an effective and appropriate manner.
- The work to prevent cybercrime is to be further developed.

Increasing knowledge and promoting expertise

- Knowledge in the 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 conducted regularly in order to enhance Sweden's capability to manage the consequences of serious IT incidents.

Enhancing international cooperation

- 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.

Work of the public authorities on the Action Plan

The work on the 2020 Action Plan began in spring 2019, and has been carried out in the joint working group which the authorities in the SAMFI interagency group established in preparation of the work on the prior year's reporting on the Action Plan. Compared with the prior year, the group has had an increased focus on following-up the work concerning the measures in the Action Plan. In line with and as part of this, the public authorities have also made efforts to further clarify existing measures regarding content and anticipated impact. This year's Action Plan presents the follow-up of the work conducted collectively and at an overall level in connection with the respective strategic priorities. The method can be further developed to support an in-depth analysis of the impact of the measures on security in the society-at-large.

Increased interaction and collaboration between both private parties and governmental entities has also been an integral part of the work with the Action Plan. The purpose was both to anchor and develop the Action Plan along with identifying the need for new measures. This collaboration is regarded as having been of great value and is explained in some detail in the chapter "External Collaboration." For the purpose of further developing the public authorities' capacity to both identify and manage the needs of the society, in the work on the 2020 Report the authorities in the interagency group SAMFI have focused on two measures in particular. The development of a national cyber security centre and the establishment of a national model for systematic information security efforts are two examples of platforms for such collaboration and these create improved possibilities to respond to the long-term needs of the stakeholders. The work on both of these measures involves all authorities in the SAMFI interagency group and aims to ensure that the knowledge as well as skills and expertise of these public authorities are used in a more integrated manner to support both private public parties and governmental entities.

New developments presented in the Report, March 2020

This year's Report of the Action Plan contains several new elements and items:

- A new chapter that describes, in clearer terms, the external collaborative efforts in the work on the 2020 Report of the Action Plan.
- A new follow-up chapter that summarises selected results of the work on the Action Plan's measures in 2019.
- A number of new measures that in part constitute a continuation of certain completed measures and in part respond to new needs that have been identified.
- Updated appendices where measures are sorted and grouped in new ways to facilitate traceability over time and for greater transparency.

External Collaboration

External Collaboration

The Swedish Government's mandate to the authorities in the SAMFI interagency group underlines the need for external cooperation in order to allow coordination of the governmental authorities' measures and activities in the Action Plan. The Agency for Digital Government (DIGG), the Swedish Data Protection Authority, the supervisory authorities of the NIS Directive including the National Board of Health and Welfare are designated for collaboration in the assigned task. Interaction with other parties helps to identify needs and reinforces the implementation of measures in the Action Plan. In the work on the 2020 Action Plan, the external collaboration has been expanded.

On three occasions, broad external collaboration was conducted with the aim of identifying needs for updates or additions and to strengthen possibilities for collaboration in the implementation of measures in the Action Plan. Some 50 representatives from industry and professional organisations, standardisation bodies, universities and central government authorities, county administrative boards, companies, along with regions and municipalities participated.

At the collaboration meetings, stakeholders not only pointed to different needs for support and direction, but also formulated a series of concrete proposals for new measures. The amount of views and proposals is an indication of a high level of commitment to the Action Plan.

A number of needs raised, such as coordination of support and requirements, increased support in the assessment of threats and risks and the prevention of cyber incidents, require even closer collaboration between the authorities in the SAMFI interagency group.

The perspective of Total Defence was seen as natural in the Action Plan and can be further clarified, as well as research and development and the role of trade and industry.

Further resource enhancement at the authorities in the SAMFI interagency group may be necessary in the coming years in order to fully respond to the needs expressed in external collaboration.

Prior to future reports, external collaboration meetings are planned to be held on several occasions and with a broader range of issues being raised. The possibility for all stakeholders in the society to contribute to the picture of needs within this area and in-depth interaction in the implementation of the Action Plan's measures is of great importance for the work with the Action Plan.

Follow-up

Follow-up

Prior to the 2020 presentation of the Action Plan, the authorities in the SAMFI interagency group have conducted a joint review of the work in 2019, summarising the selected results of the work on the Action Plan's measures in 2019. The follow-up presents what has already been achieved to respond to the Government's six strategic priorities. Most often, the intended goals and anticipated results of the measures within each respective strategic priority are described.

The follow-up is presented in order to be able to give a clear picture of what has been achieved from year-to-year. In updates of the action plan for the coming years, the public authorities intend to continue this joint review and follow-up.

The follow-up concerns only the work on the Action Plan's measures and not the other efforts of the public authorities in this area.

A number of measures have been updated in the 2020 report. This concerns changes in contents or schedule.

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

Over the past year, the public authorities have implemented a range of different measures that paved the way for a more systematic and unified approach to information and cybersecurity work among key stakeholders in the society. By means of targeted training, the establishment of new collaboration forums, new security regulations and the provision of guidance, efforts have been made to increase the security of the management of information – from the most sensitive to the wider range of information that is handled daily by the various parties in society. In preparation of the 2020 Total Defence Exercise (TFÖ 2020), MSB and the Swedish Armed Forces conducted a much in demand training programme in information security and protected communications for the public authorities responsible for surveillance and monitoring, which is to have facilitated the establishment of the preconditions for a more secure implementation of the exercise.

The SAMFI conference "Information Security for the Public Sector" was organised for the tenth year in a row. The number slots available for attendees was expanded from 600 to 750 to respond to the high demand.

By means of working with standards for both IT products and terminology, and for their increased application, the preconditions for both increased efficiency and strengthened information security throughout the society have been established.

In collaboration with FMV, MSB has established a reference list of recommended protection profiles. This is meant as a support to governmental entities in the procurement of information technology security products and will assist in increasing the basic IT security protection in Swedish government administration and activities important for the community-at-large. Parties who, in their systematic information security efforts, choose products from the reference list may have confidence in the actual functionality of the IT security products and that they meet the established requirements. The management of the reference list will be included in MSB's ongoing work for the further development of support in cybersecurity.

The authorities in the SAMFI interagency group jointly carry out a feasibility study on a national model for systematic information security efforts and identify in this work the key elements of such a model. The national model aims, among other things, to facilitate the establishment of the preconditions for a concerted, coordinated, and effective effort concerning the society's information security and to raise the minimum level of information security.

Within the framework of the efforts for the protection of activities that have a special need for protection or are particularly security-sensitive, the Swedish Security Service and FRA have begun to develop a common situational awareness concerning protection values, threats, and vulnerabilities.

The enhanced collaboration between FRA, the Swedish Security Service, the Swedish Armed Forces and MSB that took place during 2019 is a starting point for the Swedish Government's assigned task to establish a national cybersecurity centre. In 2019, the joint collaboration has been formalised in an agreement. The public authorities have also submitted a joint report to the Swedish Government concerning its assignment as a basis for the establishment of a cybersecurity centre. The work has been conducted in close cooperation with the Swedish Police Authority, FMV and PTS.

Strategic priority 2. Enhancing network, product and system security

In 2019, several measures have been implemented which collectively have provided several key parties, in the public sector in particular, the possibility of further securing communication of particularly security-sensitive information internally and among themselves. The supplemental "Confidential" service has been launched in Rakel (not approved for Classified Information with a protective security classification).

The Swedish Armed Forces and FMV have, via the establishment of requirements for new and further development of existing signal protection systems, facilitated the establishment of better preconditions for access to needs-adapted signal protection systems that maintain an adequate level of security with regard to cryptological developments. This is expected to result in better possibilities for adequate protection of the communication of information in electronic format.

In cooperation with a Swedish telecommunications carriers, during the year FRA conducted testing operations to ensure that older analogue cryptofax and cryptotelephony systems work in today’s IP-based telecommunications networks.

PTS has analysed the possibilities to increase traceability in trusted services, such as electronic signatures and stamps. The analysis has been discussed with European supervisory authorities. The issue will be raised by several regulatory authorities in the context of the ongoing review of the eIDAS Regulation. The anticipated results of the measures, in the long term, is increased protection for transactions based on qualified certificates.

In order to increase the security of networks, together with telecommunications carriers, PTS has highlighted the characteristics that are to be sought from a regional perspective in order to increase resilience and sustainability in publicly available electronic communications networks.

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

During 2019, the Swedish Security Service, FRA and the Swedish Armed Forces has increased via collaboration their own capabilities to prevent, detect, and manage cyber-attacks from professional threat actors. FRA has, in cooperation with the Swedish Security Service, made the Technical Detection and Warning System (TDV) available to more of the most security-sensitive activities. By means of this measure, the capability to prevent, detect, and manage cyber-attacks against our most security-sensitive activities has been strengthened. The Swedish Armed Forces, with support from FRA, has developed their capability to conduct both defensive and offensive operations against a professional opponent in the cyber environment.

MSB, together with the Swedish Armed Forces and the Swedish Defence Research Agency (FOI), has continued the development of a National Cyber Range (NCR) as a part of a common strategy for NCR. The work leads to a modern and flexible platform for exercises, educational programmes and training, and research, as well as tests. The developed NCR will be inaugurated in 2020.

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

The Swedish Police Authority and MSB have established a process for collaboration surrounding incident reporting. The streamlined sharing of information between public authorities leads to faster management and increased quality – both in the proactive sharing of information to stakeholders in the society and with incidents that have occurred. MSB works to ensure that anyone impacted by a cyber-related criminal act will report the incident to the police themselves. In certain investigations, MSB/CERT-SE provides support to the Swedish Police Authority. This collaboration can shorten the investigation time as well as learning and skills development can take place in both public authorities to the benefit of the society-at-large and law enforcement specifically.

Via the Swedish Police Authority's establishment of regional cybercrime centres in all seven police regions, improved possibilities for an increased inflow of IT-related questions from investigators has been established, and with this, a strengthened development of important skills. For the purpose of increasing the level of quality in criminal investigations where digital evidence is an important part of the investigation work, the Public Prosecutor's Office and the Swedish Police Authority have jointly conducted courses.

By means of the "Tänk säkert" information campaign, in 2019 MSB and the Swedish Police Authority have reached out with important information concerning how individuals and small business owners can establish more secure online behaviour. The campaign was national in scope and had a major impact partly due to the high level of engagement of some 50 external parties from both the private and public sectors. In a subsequent follow-up survey, a large proportion of the respondents who saw the campaign commented that it had provoked an interest, raised awareness, and increased their knowledge. The Swedish Armed Forces campaign (reported under priority 5) has further disseminated knowledge among those who work with sensitive data, primarily in the defence sector, about how and why information needs to be protected.

By working togehter with the financial and transaction markets, the Swedish Police Authority, via working together with the financial and transaction markets, has i.a. contributed to banks being able to impose requirements on the need for a person and computer to be in the identical physical location for certain banking matters. This ensures a higher level of security in the payment system.

Strategic priority 5. Increasing knowledge and promoting expertise

During the year, the FRA has increased knowledge and expertise in analysing hardware-related threats and vulnerabilities. This analytical capacity has already been put to use within the framework of FRA's activities providing support in the field of cybersecurity. The Swedish Armed Forces has focused on research in areas such as artificial intelligence, surveillance functions and innovation to facilitate the establishment of the possibility of applied solutions for strengthened cybersecurity in both the Swedish Armed Forces and the rest of the society.

The Swedish Armed Forces has also conducted an internal information campaign that is expected to give a higher level of security awareness among employees about the management of information and thus contribute to that particularly security-sensitive information is exposed to a lesser extent than previously. The campaign was targeted primarily at employees of the Swedish Armed Forces, but has also been used by other stakeholders in the society.

FRA, the Swedish Security Service, and the Swedish Armed Forces has an on-going continuous cooperation relating to assuring the supply of skills and expertise. Among other things, the public authorities have jointly conducted recruitment promotion activities on labour market days. In order to further provide skills and expertise to the cyber defence, the Swedish Armed Forces has commenced the work to establish an obligation for training, which in the long term will not only benefit the Swedish Defence Forces, but also other public authorities such as the FRA. Enrolment of national service conscripts for enlistment to cyber army training has commenced.

The Swedish Armed Forces conduct research and technology development in the areas of cyber defence and information security (FoT Cyber) aimed at strengthening cyber defence and developing capabilities to be able to conduct all types of computer and network operations in the cyber environment, as well as the capability to develop and maintain the necessary information and cyber security in the Swedish Armed Forces' technical method support system. The activities are conducted primarily at FMV, FOI, FHS and KTH. The activities are characterised by close cooperation between the parties and designated national and international partners.

In order to interest young people in cybersecurity and give insight into FRA's other activities, upper secondary school students have been afforded the opportunity to spend a week during the summer with the public authority. FRA has also established a podcast on cyber defence.

In 2019, a number of exercises have been conducted. The Swedish Armed Forces has conducted the SAFE Cyber 2019 exercise, which was targeted at public authorities responsible for cybersecurity in Sweden, as well as for public authorities and companies responsible for systems and services linked to the Swedish Armed Forces. The purpose and goal of the exercise was, among other things, to practice risk management and decision-making, practice dealing with incidents as well as collaboration.

Strategic priority 6. Enhancing international cooperation

Via strengthened international collaboration in 2019, the Defence Materiel Administration (FMV) has contributed to developing a framework for support to address cybersecurity threats, vulnerabilities, and develop countermeasures – something that can be used by security experts in both government and trade and industry. The work is the result of a cooperative effort within the Multinational Industrial Security Working Group (MISWG) on national cybersecurity strategies, national Industrial Security policies, and best practices in this context. Given that several of the countries participating in MISWG already have similar national models, a harmonisation can be achieved.

MSB's participation in the cooperation group and the national Computer Security Incident Response Team (CSIRT) Network within the framework of the NIS Directive has established a strategic cooperation and information exchange between Member States in the field of cybersecurity. The collaboration also creates added value in areas such as monitoring emerging technologies.

The Swedish Police Authority's Europol Resource was established in early 2019. This has increased the inflow of cases to the Swedish Police Authority and contributed to assisting other countries with information from Sweden in their ongoing cases. In summary, the measure has provided better possibilities to combat transnational cyber-related crimes.

Measures

Measures

The planned and ongoing measures are presented in this chapter. Some measures contribute to the work in 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 not presented in any order of priority. So as to preserve the traceability in the Action Plan, ongoing measures retain their original numbering despite the fact that some measures have concluded in 2019 and are no longer included in this chapter. The measures that have been concluded are set out in Appendix 1.

For every measure in the Action Plan, it is clarified which public authority or authorities in the SAMFI interagency group are responsible for the implementation. The responsible public authority collaborates in several cases with other public authorities or organisations.

Within the respective measures, collaboration with other parties can take place in various ways and for example be intended for the collection of comments or 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 public 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 authorities in the SAMFI interagency group.

In order to increase readability, new and updated measures in the chapter have been indicated with highlighting. The same marking is found in Appendix 1.

🏢 means the responsible public authority.

🕒 means the period of implementation of the measure.

# means the unique number of the measure in the Action Plan.

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.

Proactively supporting the most security-sensitive activities

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.

🏢 **Swedish Security Service, FRA and the Swedish Armed Forces**

🕒 **2019–2025**

#️⃣ **1.1.1.**

Training private parties regarding the Swedish Armed Forces' protective security requirements

The Swedish Armed Forces has begun signing contracts for preparedness agreements with trade and industry. This includes protective security agreements (PSA) and requirement specification as well as training in the protective security area so that they can be a supplier to the Swedish Armed Forces.

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

🏢 **Swedish Armed Forces**

🕒 **2019–2021**

#️⃣ **1.1.3.**

Delivering aggregate documentation on threats and vulnerabilities

Updated

Systematically serving aggregate information on threats and vulnerabilities to decision makers at various levels, such as prescribing public authorities. This makes it possible for information of a sensitive nature to be able to be adapted to be useful in a broader 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 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.

🏢 **Swedish Security Service, FRA and the Swedish Armed Forces**

🕒 **2019–2025**

#️⃣ **1.1.4.**

Preparing an Action Plan for public authorities' participation in standardisation work in the scope of SIS TK318 Updated

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 efforts. The national engagement for national and international work on standardisation including the ability to use the results from the standardisation work in the field of information and cyber security area needs to be strengthened. The Action Plan is to focus on the involvement of the public authorities and the operating area that SIS TK318 works within. The measure is being carried out together with FMV/Swedish Certification Body for IT Security (CSEC) and relevant public authorities and organisations.

MSB
2020–2021
1.1.5.

Preparing supporting materials for the application of the new Swedish Protective Security Act Updated

The Swedish Security Service and the Swedish Armed Forces are preparing new and updated guides and handbooks, training materials, etc. to support those who are to apply the new Swedish Protective Security Act and new regulations regarding protective security. The material is being prepared in coordination by both of the public authorities for their respective supervisory area. The products will comprise both protective security in general and protective security analysis, information security, personnel security, physical security and protective security agreements.

Swedish Security Service and the Swedish Armed Forces
2019–2021
1.1.6.

Arrange an annual information security conference Updated

Planning and arranging an annual information security conference for municipalities, regions, and central government authorities where the participants exchange experience and gain knowledge in the information security area.

The goal of the conference is to contribute to strengthening the public sector's information security by highlighting important issues within the area. MSB is leading the work for the conference.

MSB, FRA, FMW, Swedish Armed Forces, PTS, the Swedish Police Authority and the Swedish Security Service
2019–2022
1.1.7.

Revision and supplementation of MSB's regulations for government authorities Updated

Review and supplement 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 efforts means that the regulations requiring central government authorities to carry out systematic and risk-based information security efforts are reviewed and supplemented with new regulations on fundamental requirements for cybersecurity measures and related guidance. The regulations relating to reporting of IT incidents are also reviewed and clarified, for the purpose of facilitating the public authorities' cyber incident reporting. Where appropriate, the requirements of the regulations will be harmonised with the corresponding requirements of the NIS Directive. The review contributes to an increased systematic approach to information security efforts by the public authorities and to more consistent assessments.

🏢 **MSB**
🕒 **2019–2020**
1.1.8.

Developing and administering national terminology Updated

A process for development and administration of national terminology is to be developed. The term bank is to contain terminology for the specialised area of information and cyber security. The work is to 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. The term bank is to be publicly available and free of charge.

🏢 **MSB**
🕒 **2020–2021**
1.1.9.

Developing MSB's implementation guide for systematic information security efforts Updated

MSB is developing the method support for systematic information security efforts with relevant parties in the following prioritised areas: methods for classify information with ties to security measures, risk analysis, incident management, continuity, including aspects of Total Defence, and the organisation's governance and management.

🏢 **MSB**
🕒 **2020**
1.1.11.

Guidance for basic IT security measures Updated

Develop guidance on basic IT security measures that can be used by all types of organisations. Based on this basic level, an organisation can, via a risk assessment and analysis of the legal requirements and operational needs, determine whether the information technology security measures that have been implemented are sufficiently adequate or need to be further strengthened . The security measures are of particular importance for the organisations whose activities are of significance to the functioning of the society.

🏢 **MSB**
🕒 **2019–2020**
1.1.12.

Support stakeholders' efforts to develop robust physical conditions for operations and management New measure

MSB is to develop an overall strategic direction for the Command Center with the aim of prioritising measures that strengthen the capability of private parties to manage and work in interaction with others in everyday life and in the event of increased readiness.

Based on this focus, MSB supports parties with robustness-enhancing measures for regular activities and management, as well as with planning, construction, and development of alternative and protected Command Centers. This includes supporting the development of management systems and ensuring access to secure and robust communications as a basis for management capabilities.

MSB
2020–2022
1.1.14.

Conduct an annual conference on secure communications New measure

MSB will hold an annual conference for the user circle of Rakel, SGSI and Web-based Information System (WIS) where participants gain information and exchange experiences, thereby gaining increased knowledge about secure communications. The goal of the conference is to strengthen the parties' capability for effective and secure collaboration.

MSB
2020–2023
1.1.15.

Develop a structure for monitoring the systematic information security efforts in the public administration New measure

MSB is to develop a structure for monitoring the systematic information security efforts in the public administration. The follow-up structure will be an important component of the efforts to ensure a systematic and comprehensive approach in the work with information and cyber security. The measure follows a task assigned by the Swedish Government (Ju2019/03058/SSK, Ju2019/02421/SSK) to be conducted in ongoing dialogue with the Swedish Association of Local Authorities and Regions (SKR) in the parts that affect municipalities and regions and, if necessary, in cooperation with the Agency for Digital Government (DIGG) and other relevant authorities.

MSB
2019–2021
1.1.16.

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

Conduct a feasibility study regarding the establishment of a national model for systematic information security Updated

The authorities in the SAMFI interagency group will conduct a feasibility study on how a national model for systematic information security can be developed in concrete terms. The feasibility study is to describe the purpose of a national model and carry out a stakeholder analysis. The feasibility study will also describe how work with 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 contain, and the order in which the parts can be developed. The feasibility study is to identify the need for and develop proposals for possible new measures in the follow-up to the National Action Plan. MSB has a coordinating role in the work.

MSB, FRA, FMW, Swedish Armed Forces, PTS, the Swedish Police Authority and the Swedish Security Service

2019–2020

1.2.1.

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

Spread knowledge and experience on the work with information evaluation to other public authorities and organisations

The Swedish Armed Forces intends to support other public 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 is to be carried out via knowledge and experience exchange. Activities based on requests from other public authorities and organisations.

Swedish Armed Forces

2019–2022

1.3.1.

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

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

Swedish Armed Forces

2019–2022

1.3.2.

Establishing possibilities for opportunities for collaboration for NIS actors Updated

MSB, NIS-supervisory authorities and the National Board of Health and Welfare are establishing a national meeting arena for providers of operators of essential services and digital services. The purpose of this is to raise the awareness of the NIS Directive and to facilitate the establishment of the preconditions for NIS suppliers to exchange experiences with others within their sector. MSB will provide information and support concerning systematic information security efforts, incident reporting and the work with a link to the EU. The NIS-supervisory authorities and National Board of Health and Welfare will provide information on supervision and other issues linked to the respective sector.

MSB
2019–2022
1.3.3.

Developing security requirements for specific IT products

FMV/CSEC is to collaborate with MSB to participate in European and international 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.

FMV in collaboration with MSB
2019 onwards
1.3.5.

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

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

Swedish Armed Forces
2019–2022
1.3.6.

Preparatory project for the establishment of a National Cyber Security Centre New measure

FRA, The Swedish Armed Forces, MSB, the Swedish Security Service, Swedish Police Authority, FMV and PTS are preparing to establish a National Cyber Security Centre. The efforts take the form of a joint establishment project. The Cyber Security Centre will strengthen Sweden's overall ability to prevent, detect and manage antagonistic Cyber Security threats against Sweden. The Centre will also provide developed and coordinated support to various actors in the private and public sectors on how to protect themselves against cyber attacks. The activities of the Centre will be developed gradually in the coming years.

MSB, FRA, FMW, Swedish Armed Forces, PTS, the Swedish Police Authority and the Swedish Security Service
2020
1.3.7.

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

Continued development of regulations for protective security

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

🏢 **Swedish Security Service and the Swedish Armed Forces**
🕓 **2019–2022**
1.4.1.

Support and coordinate development of NIS Regulations regarding security measures Updated

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. The efforts can contribute to greater clarity for parties subjected to the NIS Directive by means of coordinated planning and design.

🏢 **MSB**
🕓 **2019–2020**
1.4.2.

Further develop support for coordinated supervision within NIS New measure

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.

🏢 **MSB**
🕓 **2020–2022**
1.4.4.

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.

Implementing project to reduce dependence on central functions in electronic communication networks and services

PTS is implementing a project to reduce dependence on central functions in electronic communication networks and services. The project is beginning with an analysis done together with telecommunications companies to assess the possibility of reducing dependence on central functions. Experiences from the analysis are 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.

🏢 **PTS**
🕒 **2019–2022**
# **2.1.2.**

Development and acquisition of IT security products Updated

Development and acquisition and security review of general IT security products primarily for Swedish Armed Forces needs but with possible further use by other public authorities that can benefit from the review being done.

🏢 **Swedish Armed Forces and FMV**
🕒 **2019 onwards**
# **2.1.4.**

Establishing new secure and robust communications for parties with special protective security needs

Swedish Armed Forces are further developing the possibility of secure and robust communication for parties in the defence sector and parties in Total Defence with special protective security needs.

🏢 **Swedish Armed Forces**
🕒 **2019–2022**
# **2.1.5.**

Establishing new secure and robust communications services for parties in general order, security, health and defence Updated

MSB is providing new secure and robust communications services for parties in Total Defence and developing the ability to share sensitive and security Classified Information. The measure involves, among other things, the implementation of services such as encrypted videoconferencing for the RESTRICTED security classification in SGSI, enhanced protection for communications in Rakel via the introduction of additional encryption (not approved for Classified Information with a protective security classification), and the establishment of additional data services to Rakel.

MSB
2019–2022
2.1.6.

Establishing a federation service for SGSI affiliated parties Updated

MSB is, together with relevant parties, to 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 public authorities. With a central federation service, possibilities are provided, using encryption, to increase the protection of the information when it is to be shared between various parties, which increases the ability for more secure information sharing.

MSB
2020
2.1.7.

Following and contributing to the development of secure communication for other organisations

The Swedish Armed Forces will contribute with experience regarding realisation of secure system solutions in the strategic work with further development of e.g. Net infrastructures, communication solutions, etc. within the framework for Total Defence.

Swedish Armed Forces
2019–2022
2.1.8.

Establish WIS over SGSI New measure

MSB is to develop, establish, and manage a solution that enables information sharing using Web-based information systems (WIS) over SGSI. This ensures protected and Internet-independent sharing of information between parties who use WIS and are connected to SGSI.

MSB
2020–2021
2.1.9.

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

Investigating electronic communication independence of functions abroad

PTS is investigating what it conceptually means with "electronic communication independence of functions abroad," in the degree to which electronic communication 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 communication 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 peacetime planning for Total Defence needs of telecommunications (PTSFS 1995:1).

🏢 **PTS**

🕒 **2019–2020**

#2.2.1.

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

Investigating the possibility to decide on specific security measures at parties in the electronic communication sector

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.

🏢 **PTS**

🕒 **2019–2022**

#2.3.1.

Investigating the possibility of making traceable time and frequency available to parties outside the electronic communication sector

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

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

🏢 **PTS**

🕒 **2019–2020**

#2.3.2.

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

Develop a proposed national strategy and action plan for secure encryption Updated

Based on the Information Security Commission in NISU 2014, Appendix 4 (SOU 2015:23), with support from FRA, the Swedish Armed Forces and MSB, a proposal is being drafted for a national strategy and action plan for managing and transmitting information in electronic communication networks and IT systems using encryption including information that does not fall under the mandate of the communications security service. The strategy is to comprise overall objectives for the society's information security efforts related to cryptography, and how Sweden is to maintain security and integrity in critical IT infrastructure using cryptographic functions.

The results shall constitute a report with specified proposals on a national strategy and Action Plan for cryptographic functions after consultation with the Swedish Armed Forces, FRA and MSB. The proposal is to contain a cost accounting and be able to form the basis for a concrete assignment decision for relevant public authorities.

FMV with support from FRA, Swedish Armed Forces and MSB

2020

2.4.1.

Continued development of communications security systems

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

Swedish Armed Forces and FMV

2019 onwards

2.4.2.

Management of process and equipment for information protected by national security act Updated

The public authorities with responsibility for various parts of communications security will develop and update processes that can handle decisions on allocation and distribution of communications security material to the parties covered by the new Swedish Protective Security Act. The processes will ensure that the right parties gain access to communications security. The new Swedish Protective Security Act will mean that further parties, both public authorities and individuals, will be covered by requirements on the use of encryption systems that are approved by the Swedish Armed Forces to protect Classified Information with a classification level (communications security).

Swedish Armed Forces in cooperation with FMV, FRA and MSB

2019–2020

2.4.3.

Introducing encrypted mobile speech and text message function for Classified Information with the classification level RESTRICTED Updated

The Swedish Armed Forces will establish encrypted mobile speech and text message function for Classified Information with the classification level RESTRICTED. There is a high demand and growing need to exchange classified messages within the Swedish Armed Forces and Total Defence. The telephone is to 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. With the telephone there is a wide range of applications that make it possible to replace a regular business mobile phone.

Agreement on the usage and handling in Total Defence is being drafted by the Swedish Armed Forces together with MSB.

The system should be further developed for a broader use in Total Defence.

Swedish Armed Forces
2019 onwards
2.4.4.

Establish secure speech for the classification level SECRET in Total Defence Updated

The Swedish Armed Forces, in cooperation with FMV, FRA and MSB, will establish secure speech for the classification level SECRET in the Total Defence. There is a high and growing demand for secure speech in Total Defence. The current systems are old and do not support today's communication standards, which is why there is a significant need for a modern replacement. This consists of an encrypted mobile telephone with key server for simpler key management.

Swedish Armed Forces in cooperation with FMV, FRA and MSB
2020–2022
2.4.5.

Develop and implement secure communications cryptographics for Classified Information with the classification level SECRET in Total Defence

The Swedish Armed Forces, in cooperation with FMV, FRA and MSB, is to establish message encryption for Classified Information with the classification level SECRET in Total Defence. There is a great and growing need in Total Defence to be able to exchange classified messages between parties that do not have access to interconnected systems for Classified Information. The systems used today (kryfax and krypto-PC) will be phased out. Therefore, a new system to meet the need is being developed and implemented.

Swedish Armed Forces in cooperation with FMV, FRA and MSB
2019–2022
2.4.6.

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

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

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.

MSB
2019–2021
2.5.1.

Promoting the usage of protected satellite services for time, speed and position for critical infrastructure Updated

Time, pace and position are critical factors for a wide range of functions in our society. In the event of a failure of the Global Navigation Satellite System, many systems and services will no longer be able to function normally. At the same time, there is a clear threat to GNSS in the form of both interference with the signal and more intelligent attacks such as misdirection. Therefore MSB is to promote the use of the publicly regulated Galileo Public Regulated Service (PRS) for the benefit of critical societal functions in need of mobile solutions for time, pace and position. For fixed installations that are critically dependent on exact time and or frequency, the work should be coordinated with the PTS service for correct traceable time and frequency.

MSB
2019–2022
2.5.2.

Implementing a national initiative on greater security in cyber-physical systems

MSB is to together with relevant parties implement a national initiative that includes technical, preventive, capability improving and coordinated activities to increase the security of industrial information and control systems and the Internet of Things (IoT). These activities is to result in the development and provision of training, guides, technical tools, strong exiting collaboration structures, and provide support for skills provisioning. The overall objective is to reinforce the society's collective capability to prevent and deal with both deficiencies as well as improper behaviour such as IT attacks in such society functionality that are dependent on industrial control systems (ICS).

MSB
2019–2020
2.5.3.

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 the society is to be improved.

Increasing incident management capability relating to professional threat actors

The Swedish Security Service, FRA and the Swedish Armed Forces are developing the capability to discover cyberattacks and attempted attacks by professional threat actors and support the most sensitive operations 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.

Swedish Security Service, FRA and the Swedish Armed Forces

2019–2025

3.1.1.

Providing awareness raising materials on reducing disruption sensitivity in the use of wireless communication in industrial information and control systems used in critical functions

MSB is providing awareness raising materials on reducing disruption sensitivity in the use of wireless communication in industrial information and control systems used in critical functions. With the extensive digitalisation and technical development, the 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 Wi-Fi. 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.

MSB

2019–2022

3.1.2.

Establishing a sensor system for NIS suppliers

MSB will offer via CERT-SE suppliers of services that are critical to the society and digital functions (NIS suppliers) the possibility of connecting to a sensor system. The sensor system provides connected parties an expanded capability to discover and protect themselves from serious IT attacks. Via improved situational awareness and information sharing, the sensor system also contributes to a greater ability in the society to prevent and repel IT attacks. The system is to constitute a complement to commercial products and be designed with a high level of security and integrity protection.

- 🏢 **MSB**
- 🕒 **2019–2022**
- #️⃣ **3.1.3.**

Continued development of a national Cyber Range

MSB, together with the Swedish Armed Forces and the Swedish Defence Research Agency (FOI), continues to develop a national Cyber Range (exercise 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 exercises in information and cyber security within ICS.

- 🏢 **MSB**
- 🕒 **2019–2020**
- #️⃣ **3.1.4.**

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

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

National collaboration for protection against serious IT threats (NSIT) is a collaboration between the Swedish Security Service, Swedish Armed Forces and FRA. NSIT analyses and assesses threats and vulnerabilities regarding serious or “professional” 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.

- 🏢 **Swedish Security Service, Swedish Armed Forces and FRA**
- 🕒 **2019 onwards**
- #️⃣ **3.2.2.**

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 counter and manage attacks from "professional" opponents in cyberspace.

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

The Swedish Armed Forces delivers a military strategy situation report weekly and presents it to its senior management. The situation report can when necessary be used for the entire defence sector, for example in the scope of NSIT.

Swedish Armed Forces

2019–2022

3.3.1.

Provide TDV to the most security-sensitive operations Updated

In collaboration with the Swedish Security Service, FRA conducts continued development of a Technical Detection and Warning System (TDV) plus 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 FRA.

FRA in cooperation with the Swedish Security Service

2019 onwards

3.3.2.

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

The Swedish Armed Forces is strengthening the ability to conduct defensive and offensive operations against a qualified opponent in cyberspace. FRA provides support to the Swedish Armed Forces to conduct active operations in the cyber environment for an enhanced cyber defence.

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

The Swedish Armed Forces with support from FRA

2019–2022

3.3.3.

Developing a military Cyber Range

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

Swedish Armed Forces

2019–2020

3.3.4.

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

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

Establishing regional cybercrime centres

The Swedish Police Authority is building up regional cybercrime centres in their seven regions to increase the capability to investigate and prevent IT-related crime and raise the quality of the crime prevention work in the area.

Swedish Police Authority
2019–2022
4.1.2.

Cooperating with law enforcement authorities

The Swedish Police Authority deepens the collaboration with other law enforcement authorities via regular meetings and joint participation in courses to i.a. increase the ability to fight IT-related crime.

Swedish Police Authority
2019–2022
4.1.3.

Objective 4.2. The efforts to prevent cybercrime is to be further developed.

Using European resources for crime prevention campaigns Updated

The Swedish Police Authority is expanding the cooperation with Europol on crime prevention efforts by increasing the use of the materials and the activities that Europol offers, including during European Cyber Security Month (ECSM).

Swedish Police Authority
2020–2022
4.2.1.

Participating in cooperation with the financial and transaction markets

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

Swedish Police Authority
2019–2022
4.2.2.

Building up a European cybercrime prevention network New measure

In order to slow down the increase in cybercrime, the Swedish Police Authority will participate in the construction of a European crime prevention network (EUCPN) concerning cybercrime.

Swedish Police Authority
2020–2022
4.2.3.

Nordic prevention efforts concerning cybercrime New measure

The Swedish Police Authority initiates prevention efforts within the Nordic countries regarding cybercrime. The collaboration involves becoming aware of each other's information campaigns and an exchange of experience relating to ways to combat cybercrime.

Swedish Police Authority
2020
4.2.4.

Strategic priority 5. Increasing knowledge and promoting expertise

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

Establishing strategic approaches for monitoring and valuation of the society's ability in the cyber security area

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

MSB
2019–2020
5.1.1.

Further developing analysis capacity of hardware

FRA is further developing the capability to analyse hardware-related threats and vulnerabilities. The capability development takes place via the build-up of a hardware lab and skills and staff reinforcement in the area.

FRA
2019 onwards
5.1.2.

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

Implement a targeted information campaign to raise security awareness Updated

In May 2019, the Swedish Armed Forces launched a communication campaign targeted primarily at those active in all parts of the Swedish Armed Forces and secondarily to other public authorities, primarily defence authorities. Other external target audiences (e.g. municipalities and individuals) have also been reached by the campaign. The structure of the campaign differs from previous campaigns with a similar purpose and is thus a new way of reaching out to the target groups.

A key part has been working with short information videos that have been disseminated via social media, as well as using the Swedish Armed Forces website, where in-depth information can be found. 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 ran in 2019, and will continue also in 2020, when it will be supplemented with other security aspects.

Swedish Armed Forces
2019 onwards
5.2.1.

Implement targeted training activities in the field of information security to the public sector New measure

MSB is to implement targeted training activities in the field of information security to the public sector and also, where necessary, develop support for smaller public authorities.

The measure is part of a task assigned by the Government (Ju2019/03057/SSK) which is to be conducted in cooperation with the Agency for Digital Government (DIGG) and the Swedish Association of Local Authorities and Regions (SKR) and, if necessary, the county administrative boards.

MSB
2019–2021
5.2.2.

The national "Tänk säkert" campaign New measure

Conduct a national campaign to get individuals and companies to take measures to protect their most important information. The campaign will take place during the European Cyber Security Month (ECSM) in October, which seeks to raise awareness about cyber security threats.

MSB together with the Swedish Police Authority
2020
5.2.3.

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.

Developing the preconditions for assuring the supply of skills and expertise

FRA, Swedish Security Service and the Swedish Armed Forces need to develop the preconditions for assuring the supply of skills and expertise to achieve the goal in the reporting of the Government assignment to the Swedish Security Service and FRA on the development of the efforts 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. In the long term, the efforts should involve more operations (such as the authorities in the SAMFI interagency group) and efforts for assuring the supply nationally of skills and expertise in the cyber security area.

FRA, Swedish Security Service and the Swedish Armed Forces
2019–2025
5.3.1.

Establishing a model for skills development

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

The Swedish Armed Forces together with FRA and the Swedish Security Service
2019–2022
5.3.2.

Strengthening and further development of research and technical development in the cyber defence area Updated

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 are to be able to be converted to applications that contribute to the ability to conduct operations in cyberspace. The Swedish Defence Research Agency (FOI), the Swedish Defence University (FHS), the Royal Institute of Technology (KTH) and others support the research.

Swedish Armed Forces
2019 onwards
5.3.3.

Establishing adapted selection and recruitment in the cyber direction Updated

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

Swedish Armed Forces and FRA
2019–2022
5.3.4.

Implementing a preliminary study on assuring the supply of skills and expertise in the cyber security area for the society

MSB intends to analyse the possibilities of supporting the development of the supply of skills and expertise in the cyber security area. 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, continuing professional development, as well as at universities and other institutions of higher education, and upper secondary schools.

MSB
2020
5.3.5.

Funding research to respond to the challenges of the future in the field of information and cybersecurity New measure

MSB funds research into information and cybersecurity challenges arising from digitalisation and solutions to respond to them. MSB monitors the development of the society and develops its methods for designing new calls based on the unique information flows that the Agency has. The research spans technical, social sciences, organisational and strategic issues. Via collaboration with international partners, resources can be gathered and focused in order to achieve critical mass and synergies. In 2020-2021, support will commence for research into the future of autonomous and automated cybersecurity.

MSB
2020–2022
5.3.6.

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.

Implementing subcomponents in TFO 2020

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

The Swedish Armed Forces together with MSB
2019–2020
5.4.1.

Implementing NISÖ 2021

MSB is implementing the National Information Security Exercise 2021 (NISÖ) in collaboration with the Swedish Armed Forces, the Swedish Security Service, PTS and the Swedish Police Authority. The previous exercise was done in 2018. The purpose of the exercise is to give private parties and governmental entities the possibility to engage in the exercise together. The exercise aimed at strengthening the society's collective capability to deal with IT-related disruptions with a broad impact where the parties quickly need to coordinate in order to be able to take relevant measures.

MSB
2019–2021
5.4.2.

Implementing recurring joint exercises with cyber security public authorities on the managing of IT incidents Updated

MSB is implementing recurring joint exercises with Swedish and European cyber security authorities on the managing of IT incidents. The purpose is to develop the joint ability to handle IT incidents.

MSB
2020–2021
5.4.3.

Implementing annual information and cyber security exercise SAFE Cyber

The Swedish Armed Forces is implementing in cooperation with FRA, MSB and the Swedish Security Service an annual information and cyber security exercise called SAFE Cyber. The exercise comprises collaboration with the purpose of ensuring important functions in the event to computer and network operations targeting Sweden. Focus of the exercise is IT security including risk and incident management, threat assessment, situation report, reporting, management, coordination and decision-making. The exercise is targeted towards 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.

Swedish Armed Forces in cooperation with FRA, MSB and the Swedish Security Service
2019–2022
5.4.4.

Strategic priority 6. Enhancing international cooperation

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

Working for international harmonisation of rules and requirements for information security

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

Swedish Armed Forces
2019–2022
6.1.1.

Developing and improving standards for requirements and evaluation of cyber security in IT products

FMV/CSEC will contribute to Swedish and international standardisation bodies and forums to develop and improve standards for the requirements and evaluation of IT security and cryptography.

FMV
2019 onwards
6.1.3.

Europol Resource New measure

The Swedish Police Authority has a resource at the Joint Cybercrime Action Taskforce (J-CAT) at Europol in the Hague for the purpose of strengthening the collaboration with other countries and public authorities in the efforts to investigate cybercrime.

Swedish Police Authority
2020–2022
6.1.4.

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

Participating in international cooperation forums for industrial security

Updated

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. Via participating in the MISWG Ad Hoc Working Group (AHWG) 7 on Cyber Security, knowledge is gained regarding how other countries' industrial security authorities work vis-à-vis industry with requirement specifications in the Cyber Security field. This knowledge will contribute to the build-up of the FMV as a national industrial security authority, Designated Security Authority (DSA), plus provide input that contributes to the efforts to produce a national model to support systematic information security efforts.

FMV
2019–2020
6.2.1.

Monitor and contribute to the development of the NIS Directive

Updated

The requirements of the NIS Directive assist to increase the level of cyber security in a wide range of important public services. As the national point of contact for the NIS Directive and national CSIRT Unit, MSB participates in the NIS Cooperation Group and the CSIRTs Network for the purpose of monitoring and contributing to the development of the NIS Directive in the EU.

MSB
2019 and until further notice
6.2.2.

Concluding words

Concluding words

The efforts relating to the 2020 report on a Comprehensive Information and Cyber Security Action Plan for the years 2019-2022 has contributed to increased coordination of the governmental authorities measures and activities. The public authorities have built upon the experiences with working on the prior year's Action Plan and have taken how the plan was used by stakeholders in the society was into account. The efforts relating to the development of the Action Plan's measures in terms of clarity and follow-up will continue next year as well.

The establishment of a national cyber security centre and a national model for systematic information security efforts is expected to not only develop the information and cyber security of the society. As collaborative platforms, they can gather and coordinate efforts on many of the measures, which may affect the design of next year's Action Plan.

A number of additional measures have been suggested by private parties and governmental entities within the framework of the collaboration that has taken place for efforts to implement the Action Plan. In some cases, these needs have been addressed in this year's report or are deemed to be able to be taken into care in the framework of efforts on the Cybersecurity Centre and national model. Others are deemed, due to limited resources or mandates, not to be fully addressed within the framework of the efforts to implement the Action Plan.

The work on next year's report of the Action Plan will commence as soon as feasible after the 2020 Report has been submitted to the Government. The work will continue to be conducted in the scope of the joint working group established by the authorities in the SAMFI interagency group. By beginning the work early on and with external collaboration, the possibilities for allocation of resources, coordination and joint planning increase.

Appendix 1:

List of measures

List of measures

Current measures

The appendix provides a clear list of all the measures of the Action Plan. The measures concluded can be found in the section "Measures implemented" below. Measures that are no longer relevant to implement can be found under the section "Written-off measures" below.

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

#	Measure	Responsible public authority	Status	Page
1.1.1.	Proactively supporting the most security-sensitive activities	Swedish Security Service, FRA and the Swedish Armed Forces		24
1.1.3.	Training private parties regarding the Swedish Armed Forces' protective security requirements	Swedish Armed Forces		24
1.1.4.	Delivering aggregate documentation on threats and vulnerabilities	Swedish Security Service, FRA and the Swedish Armed Forces	Updated	24
1.1.5.	Preparing an Action Plan for public authorities' participation in standardisation work in the scope of SIS TK318	MSB	Updated	25
1.1.6.	Preparing supporting materials for the application of the new Swedish Protective Security Act	Swedish Security Service and the Swedish Armed Forces	Updated	25
1.1.7.	Arrange an annual information security conference	MSB, FRA, FMV, Swedish Armed Forces, PTS, the Swedish Police Authority and the Swedish Security Service	Updated	25
1.1.8.	Revision and supplementation of MSB's regulations for government authorities	MSB	Updated	25
1.1.9.	Developing and administering national terminology	MSB	Updated	26
1.1.11.	Developing MSB's method support for systematic information security efforts	MSB	Updated	26

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

#	Measure	Responsible public authority	Status	Page
1.1.12.	Design guidance for basic IT security measures	MSB	Updated	26
1.1.14.	Support stakeholders' efforts to develop robust physical preconditions for activities and management	MSB	New measure	27
1.1.15.	Conduct an annual conference on the topic of secure communications	MSB	New measure	27
1.1.16.	Develop a structure for monitoring the systematic information security efforts in the public administration	MSB	New measure	27
1.2.1.	Conduct a feasibility study regarding the establishment of a national model for systematic information security	MSB, FRA, FMV, Swedish Armed Forces, PTS, the Swedish Police Authority and the Swedish Security Service	Updated	27
1.3.1.	Spread knowledge and experience on the efforts with information evaluation to other public authorities and organisations	Swedish Armed Forces		28
1.3.2.	Increasing the knowledge of information security in the Swedish Armed Forces' supervisory area for protective security	Swedish Armed Forces		28
1.3.3.	Establishing possibilities for collaboration for NIS parties	MSB	Updated	28
1.3.5.	Developing security requirements for specific IT products	FMV in collaboration with MSB		29
1.3.6.	Expanding the collaboration with other public authorities, international partners and civil companies in the defence sector regarding situation reports and incident management capability.	Swedish Armed Forces		29
1.3.7.	Preparatory project for the establishment of a National Cyber Security Centre	MSB, FRA, FMV, Swedish Armed Forces, PTS, the Swedish Police Authority and the Swedish Security Service	New measure	29
1.4.1.	Continued development of regulations for protective security	Swedish Security Service and the Swedish Armed Forces		29
1.4.2.	Support and coordinate development of NIS Regulations regarding security measures	MSB	Updated	30
1.4.4.	Further develop support for coordinated supervision within NIS	MSB	New measure	30

Strategic priorities 2. Enhancing network, product and system security

#	Measure	Responsible public authority	Status	Page
2.1.2.	Implementing project to reduce dependence on central functions in electronic communication networks and services	PTS		30
2.1.4.	Development and acquisition of IT security projects	Swedish Armed Forces and FMV	Updated	30
2.1.5.	Establishing new secure and robust communications for parties with special protective security needs	Swedish Armed Forces		31
2.1.6.	Establishing new secure and robust communications services for parties in general order, security, health and defence	MSB	Updated	31
2.1.7.	Establishing a federation service for SGSI affiliated parties	MSB	Updated	31
2.1.8.	Following and contributing to the development of secure communication for other organisations	Swedish Armed Forces		31
2.1.9.	Establish WIS over SGSI	MSB	New measure	32
2.2.1.	Investigating electronic communication independence of functions abroad	PTS		32
2.3.1.	Investigating the possibility to decide on specific security measures at parties in the electronic communication sector	PTS		32
2.3.2.	Investigating the possibility of making traceable time and frequency available to parties outside the electronic communication sector	PTS		32
2.4.1.	Develop a proposed national strategy and action plan for secure encryption	FMV with support from FRA, the Swedish Armed Forces and MSB	Updated	33
2.4.2.	Continued development of communication security systems	Swedish Armed Forces and FMV		33
2.4.3.	Management of process and equipment for information protected by national security act	Swedish Armed Forces in cooperation with FMV, FRA and MSB	Updated	34
2.4.4.	Introducing encrypted mobile speech and text message function for Classified Information with the classification level RESTRICTED	Swedish Armed Forces	Updated	34
2.4.5.	Establish secure speech for the classification level SECRET in Total Defence	Swedish Armed Forces in cooperation with FMV, FRA and MSB	Updated	34

Strategic priorities 2. Enhancing network, product and system security

#	Measure	Responsible public authority	Status	Page
2.4.6.	Develop and implement secure communications cryptographics for Classified Information with the classification level SECRET in Total Defence	Swedish Armed Forces in cooperation with FMV, FRA and MSB		35
2.5.1.	Providing expertise and awareness materials on IT security in the build-up of new intelligent transportation systems	MSB		35
2.5.2.	Promoting the usage of protected satellite services for time, speed and position for critical societal functions	MSB	Updated	35
2.5.3.	Implementing a national initiative on greater security in cyber-physical systems	MSB		35

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

#	Measure	Responsible public authority	Status	Page
3.1.1.	Increasing incident management capability relating to professional threat actors	Swedish Security Service, FRA and the Swedish Armed Forces		36
3.1.2.	Providing awareness raising materials on reducing disruption sensitivity in the use of wireless communication in industrial information and control systems used in critical functions	MSB		36
3.1.3.	Establishing a sensor system for NIS suppliers	MSB		37
3.1.4.	Continued development of national Cyber Range	MSB		37
3.2.2.	Working within NSIT to increase the capability to counter complex and serious IT threats	Swedish Security Service, FRA and the Swedish Armed Forces		37
3.3.1.	Supplying military strategic situation reports on the status in the Swedish Armed Forces' information and command support system, threats and risks	Swedish Armed Forces		38
3.3.2.	Provide TDV to the most security-sensitive operations	FRA in cooperation with the Swedish Security Service	Updated	38
3.3.3.	Strengthening the capability to conduct defensive and offensive operations against a qualified opponent in cyberspace	The Swedish Armed Forces with support from FRA	Updated	38
3.3.4.	Developing a military Cyber Range	Swedish Armed Forces		38

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

#	Measure	Responsible public authority	Status	Page
4.1.2.	Establishing regional cybercrime centres	Swedish Police Authority		39
4.1.3.	Cooperating with law enforcement authorities	Swedish Police Authority		39
4.2.1.	Using European resources for crime prevention campaigns	Swedish Police Authority	Updated	39
4.2.2.	Participating in cooperation with the financial and transaction markets	Swedish Police Authority		39
4.2.3.	Building the European cybercrime prevention network	Swedish Police Authority	New measure	40
4.2.4.	Nordic prevention efforts on cybercrime	Swedish Police Authority	New measure	40

Strategic priorities 5. Increasing knowledge and promoting expertise

#	Measure	Responsible public authority	Status	Page
5.1.1.	Establishing strategic approaches for monitoring and valuation of the society's capability in the cyber security area.	MSB		40
5.1.2.	Further developing analysis capacity of hardware	FRA		40
5.2.1.	Implement a targeted information campaign to raise security awareness	Swedish Armed Forces	Updated	41
5.2.2.	Implement targeted training activities in the field of information security to the public sector	MSB	New measure	41
5.2.3.	The national "Think ahead about Security" campaign	MSB together with the Swedish Police Authority	New measure	41
5.3.1.	Developing the preconditions for assuring the supply of skills and expertise	FRA, Swedish Security Service and Swedish Armed Forces		42
5.3.2.	Establishing a model for skills development	The Swedish Armed Forces together with FRA and the Swedish Security Service		42
5.3.3.	Strengthening and further development of research and technical development in the cyber defence area	Swedish Armed Forces	Updated	42
5.3.4.	Establishing adapted selection and recruitment in the cyber direction	Swedish Armed Forces and FMV	Updated	43

Strategic priorities 5. Increasing knowledge and promoting expertise

#	Measure	Responsible public authority	Status	Page
5.3.5.	Implementing a preliminary study on assuring the supply of skills and expertise in the cyber security area for the society	MSB	Updated	43
5.3.6.	Funding research to respond to the challenges of the future in the field of information and cybersecurity	MSB	New measure	43
5.4.1.	Implementing subcomponents in TFO 2020	The Swedish Armed Forces together with MSB		44
5.4.2.	Implementing NISÖ 2021	MSB		44
5.4.3.	Implementing recurring joint exercises with cyber security public authorities on the managing of IT incidents	MSB	Updated	44
5.4.4.	Implementing annual information and cyber security exercise SAFE Cyber	Swedish Armed Forces in cooperation with FRA, MSB and the Swedish Security Service		44

Strategic priorities 6. Enhancing international cooperation

#	Measure	Responsible public authority	Status	Page
6.1.1.	Working for international harmonisation of rules and requirements for information security	Swedish Armed Forces		45
6.1.3.	Developing and improving standards for requirements and evaluation of cyber security in IT products	FMV		45
6.1.4.	Europol Resource	Swedish Police Authority	New measure	45
6.2.1.	Participating in international cooperation forums for industrial security	FMV	Updated	46
6.2.2.	Monitor and contribute to the development of the NIS Directive	MSB	Updated	46

Measures implemented

#	Measure	Responsible public authority	Clear
1.1.2.	**Train authorities responsible for surveillance** Training and information security and protected communication The activity is linked to the 2020 Total Defence Exercise (TFÖ 2020) and all public authorities responsible for surveillance and monitoring plus relevant sectors are involved. The measure is also carried out together with the Swedish Security Service and the Swedish Defence College.	Swedish Armed Forces and MSB	2019
1.1.13.	**Establish and administer a reference list for IT security products** MSB will establish and administer a reference list over 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 list of recommended encryption functions. The list will serve as a support to organisations in the purchase of IT-security products used in Swedish government administration and in critical operations in Sweden.	MSB in collaboration with FMV	2019
1.3.4.	**Deepening the cooperation between FRA, the Swedish Security Service, the Swedish Armed Forces and MSB** FRA, Swedish Security Service, Swedish Armed Forces and MSB intend to deepen their cooperation in the information and cyber security area. This includes capability needs, organisational aspects and public-private cooperation in the respective public authority's area of responsibility. Since beginning of the year, a special working group has been working with these issues. The public authorities intend to return to the Government in 2019 with suggested activities.	FRA, Swedish Security Service, Swedish Armed Forces and MSB	2019
1.4.3.	**Preparing support for and developing coordinated supervision within NIS** 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.	MSB	2019

#	Measure	Responsible public authority	Clear
2.1.3.	**Investigating the possibility of increasing traceability in trusted services** 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.	PTS	2019
4.1.1.	**Strengthening cooperation in incident reporting on criminal activities** The Swedish Police Authority is establishing together with MSB a process for cooperation on incident reporting to increase prosecutions and strengthen the possibility of crime prevention.	The Police Authority together with MSB	2019
6.1.2.	**Establishing a resource at Europol** The Swedish Police Authority is hiring 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 public authorities in the work to investigate crime.	Swedish Police Authority	2019

Written-off measures

#	Measure	Responsible public authority	Written-off
1.1.10.	**Investigating the possibility of greater control regarding the information security efforts for municipalities and county councils** MSB will conduct an investigation of the need to establish legal requirements to conduct systematic and risk-based information security efforts for municipalities and regions. The legal requirements are to supplement already existing NIS regulations. The investigation should, besides requirements of systematic and risk-based information security efforts, also analyse needs to introduce requirements on incident reporting and inspections. The investigation is to be able to answer what control is needed to improve the information security efforts 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 parties. MSB is awaiting the implementation of the Government commission to develop a structure for monitoring the systematic information security efforts in the public administration (Ju2019/03058/SSK, Ju2019/02421/SSK) in order to assess the continued need for governing of municipalities and regions.	MSB	2019
2.1.1.	**Preparing support for acquiring robust electronic communication** PTS is preparing support for acquiring robust electronic communication The robustness in the electronic communication is affected by several factors. One factor is the users' acquisition of communication networks and communications services. There is a need for support to companies, public authorities and other organisations that in various ways are dependent on robust electronic communications in their operations, regarding how they can acquire robust electronic communication. The support is to simplify matters for operations to evaluate their own needs for secure electronic communication, convert these needs to requirements prior to an acquisition and support to follow up the requirements during the contract period. The measure is part of the efforts related to the future National Cybersecurity Centre.	PTS	2019

#	Measure	Responsible public authority	Written-off
3.1.5.	**Creating conditions for cooperation within the framework of MSB's CSIRT activities** 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 MSB/CERT-SE's tasks to support the society in the efforts with preventing and managing IT incidents. In this work, both of the needs of access to workplaces and protected meeting spaces are met. The measure is part of the efforts related to the future National Cybersecurity Centre.	MSB	2019
3.2.1.	**Investigating the possibility of sharing operational information and incident information securely between the authorities in the SAMFI interagency group** The authorities in the SAMFI interagency group are to investigate the possibility of sharing information in a secure way to facilitate the collaboration between relevant public authorities. This can for example cover information on IT-related threats to improve the respective public authority's incident management and security requirement specification. The measure is part of the efforts related to the future National Cybersecurity Centre.	MSB, FRA, Swedish Security Service, Swedish Armed Forces, PTS, FMV and Swedish Police Authority	2019
3.2.3.	**Establishing a collaborative forum for various public authorities' incident management functions** MSB together with the Swedish Police Authority establishes a cooperation forum for information exchange on statistics and current events in public authorities' incident management functions. The measure amounts to regular line activities within the framework of the cooperation agreement between the two public authorities.	MSB together with the Swedish Police Authority	2019

Appendix 2:

Assignment regarding a Comprehensive Information and Cyber Security Action Plan for the years 2019–2022

Regeringen

Regeringsbeslut **I:9**

2018-07-12
Ju2018/03737/SSK

Justitiedepartementet

Uppdrag om en samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022

Regeringens beslut

Regeringen uppdrar åt Myndigheten för samhällsskydd och beredskap, Försvarets radioanstalt, Försvarets materielverk, Försvarsmakten, Post- och telestyrelsen, Polismyndigheten och Säkerhetspolisen att ta fram en samlad handlingsplan för dessa myndigheters arbete utifrån målen i Nationell strategi för samhällets informations- och cybersäkerhet (skr. 2016/17:213). Handlingsplanen ska omfatta åren 2019–2022. Myndigheten för samhällsskydd och beredskap ska vara sammanhållande för arbetet med handlingsplanen.

Av handlingsplanen ska framgå planerade åtgärder som myndigheterna enskilt eller i samverkan med andra aktörer avser att vidta för att höja informations- och cybersäkerheten i samhället. Den samlade handlingsplanen bör syfta till att bidra till att det sker en samordning avseende myndigheternas åtgärder och aktiviteter.

I framtagandet av handlingsplanen ska myndigheterna särskilt samverka med den eller de myndigheter som utövar tillsyn med stöd av den kommande lagen om informationssäkerhet för samhällsviktiga och digitala tjänster samt Datainspektionen och Myndigheten för digital förvaltning (från den 1 september 2018). Myndigheterna bör även på ett systematiskt sätt inhämta idéer och råd och i övrigt samverka med andra relevanta statliga myndigheter, kommuner, landsting, Sveriges Kommuner och Landsting, företag och andra organisationer som kan bidra i arbetet. Handlingsplanen kan även omfatta planerade åtgärder inom ramen för internationella samarbeten.

Myndigheten för samhällsskydd och beredskap ska vara sammanhållande för en redovisning av den samlade handlingsplanen senast den 1 mars 2019 till Regeringskansliet (Justitiedepartementet, Försvarsdepartementet och Näringsdepartementet).

Myndigheten för samhällsskydd och beredskap ska även vara sammanhållande för en årlig redovisning av dessa myndigheters arbete med att genomföra handlingsplanen. Den första redovisningen ska lämnas den 1 mars 2020 till Regeringskansliet (Justitiedepartementet, Försvarsdepartementet och Näringsdepartementet) och därefter den 1 mars varje år fram till att uppdraget slutredovisas den 1 mars 2023. I samband med de årliga redovisningarna bör myndigheterna vid behov uppdatera handlingsplanen så att den ger en rättvisande bild av myndigheternas huvudsakliga aktiviteter.

En utgångspunkt för uppdragets genomförande är att de aktiviteter och åtgärder som myndigheterna redovisar i handlingsplanen ska rymmas inom givna ekonomiska ramar.

Skälen för regeringens beslut

Regeringen har vidtagit en rad åtgärder för att stärka informations- och cybersäkerheten i samhället. I det fortsatta arbetet ser regeringen ett behov av en samlad redovisning av vilka åtgärder de sju myndigheterna på eget initiativ planerar att vidta för att höja informations- och cybersäkerheten i samhället inom ramen för sina befintliga ansvarsområden de kommande åren. Med en samlad handlingsplan kommer regeringens styrning av de sju myndigheterna för att genomföra strategin bli mer ändamålsenlig. Uppdraget bidrar till att ge regeringen ett bättre underlag för att kunna analysera om myndigheternas planerade åtgärder är tillräckliga för att nå målsättningarna i strategin och vilka ytterligare åtgärder regeringen behöver vidta.

Utöver detta uppdrag om en samlad handlingsplan avser regeringen att återkomma med specifika uppdrag som myndigheterna ska utföra i samverkan. Ett prioriterat uppdrag är ett uppdrag om framtagandet av en nationell modell för systematiskt informationssäkerhetsarbete som utgör en av målsättningarna i den nationella strategin för samhällets informations- och cybersäkerhet. Den nationella modellen syftar till att utgöra en gemensam plattform för det systematiska informationssäkerhetsarbetet genom att samordna och samla regelverk, metoder, verktyg, utbildningar med mera på ett lättillgängligt sätt.

Regeringens strategi ger uttryck för regeringens övergripande prioriteringar och målsättningar och syftar till att utgöra en plattform för Sveriges fortsatta utvecklingsarbete. Ingen aktör kan ensam lösa utmaningarna på detta område. När flera aktörer arbetar mot samma mål är det särskilt viktigt med samverkan och en gemensam riktning. Tillsammans med strategin bidrar den samlade handlingsplanen till en sådan riktning och risken minskar för till exempel överlappande arbete eller att centrala behov inte tillgodoses.

Försvarsberedningen har i sin rapport Motståndskraft, Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025 (Ds 2017:66) betonat vikten av ett kontinuerligt och systematiskt arbete med informations- och cybersäkerhet för en trovärdig totalförsvarsförmåga. För att öka förmågan inom totalförsvaret är det enligt Försvarsberedningen centralt att bygga vidare på arbetet inom krisberedskapen och de strukturer för samhällets informations- och cybersäkerhet som redan är etablerade.

Myndigheterna i detta uppdrag har centrala ansvarsområden i arbetet för en god informations-och cybersäkerhet i samhället. De har också en etablerad samverkansstruktur genom Samverkansgruppen för informationssäkerhet (SAMFI). Regeringen anser att en fördjupad samverkan mellan dessa myndigheter är en förutsättning för att stärka vår förmåga att skydda oss mot cyberattacker och andra allvarliga it-incidenter.

För ett effektivt genomförande av strategin krävs att myndigheterna i detta uppdrag i så stor utsträckning som möjligt samordnar sitt arbete. Myndigheterna ska därför i sin egen planering och prioritering av verksamheten när så är relevant för myndigheten beakta arbetet med handlingsplanen för att ta tillvara effektivitets- och kvalitetsnyttor i arbetet med hela samhällets informations- och cybersäkerhet. I uppdraget ingår även att löpande hålla regeringen informerad om hur arbetet med handlingsplanen fortskrider.

Avgränsningar i uppdraget

Löpande arbete med informations- och cybersäkerhet i den egna organisationen ska i enlighet med ansvarsprincipen bedrivas kontinuerligt och självständigt. Den typen av åtgärder ska inte ingå i handlingsplanen.

Varje myndighet ska även bedöma om, och i så fall i vilken omfattning, planerade åtgärder ska delges inom ramen för den samlade handlingsplanen med anledning av att informationen bedöms hemlig eller omfattas av sekretess.

På regeringens vägnar

Morgan Johansson

Emelie Juter

Likalydande original till

Myndigheten för samhällsskydd och beredskap
Försvarets radioanstalt
Försvarets materielverk
Försvarsmakten
Post- och telestyrelsen
Polismyndigheten
Säkerhetspolisen

Kopia till

Datainspektionen
Transportstyrelsen
Statens energimyndighet
Finansinspektionen
Inspektionen för vård och omsorg
Livsmedelsverket
Sveriges Kommuner och Landsting
Vetenskapsrådet
Arbetsmarknadsdepartementet/A
Finansdepartementet/BA, DF, SFÖ, K, FPM
Försvarsdepartementet/SUND, MFI, MFU
Justitiedepartementet/L4, L6, KRIM, Å, PO, KH
Kulturdepartementet/MF
Miljödepartementet/STM
Näringsdepartementet/D, IFK, FÖF, SUBT, BT, TIF, SUN
Socialdepartementet/FS, SF
Utbildningsdepartementet/F
Utrikesdepartementet/ES, HI, SÄK

A joint collaboration between:

MSB Swedish Civil Contingencies Agency

FRA

FMV

FÖRSVARSMAKTEN

PTS

Polisen

Säkerhetspolisen

651 81 Karlstad Tel. 0771-240 240 **www.msb.se**
Order No. MSB1597 – June 2020 ISBN 978-91-7927-049-0