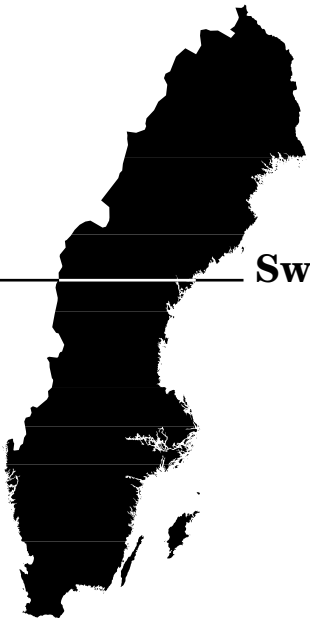
CIIP Country Surveys



Sweden

The Country Survey of Sweden 2004 was written with the help of Jan Lundberg and Sara Siri, Swedish Emergency Management Agency (SEMA) as well as Georg Fischer and Henrik Christiansson, Swedish Defence Research Agency (FOI).

Sweden

Critical Sectors

There is no official definition of CII or CIIP in Sweden. However, CIIP can be understood as the protection of essential electronic information services, such as IT systems, electronic communications, and radio and television services.[352] In a preparatory work to the *Commission on Vulnerability and Security*[353] (see below), the following critical information infrastructure sectors were suggested:

- Air control systems,
- Electric power systems,
- Financial systems,
- National command systems,
- Telecommunication systems.

Disruption of any of these systems would have immediate serious consequences for society.

Initiatives and Policy

CIIP-issues have been on the political agenda in Sweden for many decades. Measures to increase the robustness and security of critical national infrastructures have been implemented since World War II. The vulnerability problems associated with society's increasing dependence on IT and information infrastructures were identified early on as a matter of national security. In addition, management of IT-related vulnerabilities has been discussed since the early 1970s. The present Swedish CIIP policy is derived from these historical developments and from some more recent initiatives described below.

352 Information provided by a Swedish expert of SEMA, 2003.

353 The Swedish Commission on Vulnerability and Security. *Vulnerability and Security in a New Era – A Summary* (SOU 2001:41, Stockholm, 2001). http://forsvar.regeringen.se/propositionermm/sou/pdf/sou2001_41eng.pdf.

The Cabinet Office Working Group on Defensive Information Operations (AG-IO/IW)

On 12 December 1996, the government appointed within the cabinet a *Working Group on Defensive Information Operations*. In addition to the members from the cabinet office and ministries, the group also included representatives of relevant private companies and organizations. The working group's task was to monitor developing threats and risks in the area of information warfare and to spread information about these matters. In addition, the working group prepared a proposal on how to assign responsibilities and to formulate strategy guidelines for protection against information operations. The working group presented two main reports before it was disbanded. Some of its tasks have been transferred to the *Swedish Emergency Management Agency* (see below).

Commission on Vulnerability and Security

Following a decision on 23 June 1999, the Swedish government authorized the *Minister for Civil Defense* to appoint a *Special Investigator* to head a commission of inquiry, with a mandate to analyze and submit proposals for a more integrated approach to civil defense and emergency preparedness planning.[354] The findings and proposals of the *Commission on Vulnerability and Security*, as presented in May 2001, have been a most important step in the implementation of a new structure for a defense and emergency preparedness planning in Sweden.

The commission suggested several strategic measures for improving the general stability of critical technical infrastructure.[355] In its final report, the commission also proposed measures designed to specifically enhance information assurance and improve protection against information operations. The commission's view was that the central government must assume responsibility in these areas. At the same time, the commission emphasized that all managers and system owners are responsible for securing their own systems against computer intrusions and other types of IT-related threats. The role of the government should be to support these activities and to

354 Ibid.

355 Such as cross-sector activity, security standards, Computer Emergency Response Teams, a coordinating body for IT security, an information security technical support team, an intelligence and analysis unit, R&D, international cooperation, a system for the certification of IT products, and more. Ibid., pp. 41–60.

provide functions and facilities that exceed the financial capabilities of other sectors in society.

Committee on Information Assurance in the Swedish Society

The Swedish government on 11 July 2002 instituted the *Committee on Information Assurance in the Swedish Society*. The committee's brief was to present an assessment of information protection requirements in critical sectors of society, and to make a proposal on organizational matters of the Swedish signals protection service. In addition, the committee was asked to submit proposals regarding:

- The development of a national strategy for information assurance,
- The form and focus of future Swedish engagements in international cooperation on information assurance,
- The implementation of the *OECD Guidelines for the Security of Information Systems and Networks*.

The committee is also expected to monitor the implementation of information assurance measures within state agencies in accordance with the *Government Bill on Society's Security and Preparedness* (see below).[356] The committee will finish its work during 2005.

Committee on Joint Radio Communication for Public Safety and Security

At present, Sweden has no single radio communication infrastructure for public safety and security (PSS), i.e. emergency services. There are about two hundred different systems for radio communication within the domain of PSS in Sweden. In the light of this and other issues, the government instituted the *Committee on Joint Radio Communication for Public Safety and Security* on 10 June 2002. In September 2003, the government decided to allocate the necessary funding to finance a new radio system for PSS.

The aim of government policy on telecommunications is to give citizens and the Swedish authorities access to reliable and effective electronic communications. Everyone should have access to telecom services on equal terms. The communications systems should also be robust and accessible

356 Government bills 2001/02:158.

during situations of crisis and war.[357] Robust telecommunications are to be achieved through long-term and systematic preparatory efforts.

Government Bill on Society's Security and Preparedness

In March 2002, the government presented its bill on Swedish security and preparedness policy. The bill was, to a large extent, based on the findings and proposals of the *Commission on Vulnerability and Security* (see above).

The bill presented the government's framework for a new planning system to prepare for major societal crises and for activities related to a potential threat of war. Further, the bill gave an account on how the crisis management structure will be strengthened. All of this has implications for the assurance of critical infrastructures in general, and for critical information infrastructures in particular.

Based on the findings and proposals of the *Commission on Vulnerability and Security*, the government presented a new organizational structure for Swedish information assurance:

- Overall responsibility for information assurance and for policy intelligence and analysis in the public sector rests with the *Swedish Emergency Management Agency* (SEMA) (see below);
- A *Computer Emergency Response Team* operates at the *Swedish National Post and Telecom Agency*. The team monitors IT incidents, gathers statistics, and provides warnings to IT-system owners when necessary (see below);
- An *Information Security Technical Support Team* of experts and support staff with a high level of technological expertise operates at the *Swedish National Defense Radio Establishment* (see below);
- A system for security-oriented evaluation and certification of IT products and systems has been established at the *Swedish Defense Materiel Administration* (see below).

357 Government bills 2001/02:158 and 2002/03:110.

Organizational Overview

Public Agencies

The government agencies report to their respective ministries, but are formally subordinated only to collective cabinet decisions. The various agencies and organizations in charge of critical information infrastructure protection are presented below under the heading of the ministry they are affiliated with.

Ministry of Defense

The Swedish Emergency Management Agency (SEMA)

The *Swedish Emergency Management Agency* (SEMA) [358] was established on 1 July 2002 to coordinate work on the preparedness of society for major crises and war. When it was formed, SEMA took over some of the tasks of the *Swedish Agency for Civil Emergency Planning* and the *National Board of Psychological Defense*. SEMA presents proposals to the government on the allocation of resources, and then distributes funds to the authorities active in the emergency management area. This includes directing, coordinating, and evaluating measures taken.

SEMA analyzes the development of society, and the interdependency of critical societal functions. The agency further promotes interaction between the public and private sectors. The agency also coordinates and initiates research and development in the emergency management area and has overall governmental responsibility for information assurance in Sweden. The *Information Assurance Department* mainly manages the latter task, while the *Research and Analysis Department* handles the former task.

SEMA/The Information Assurance Department

The main activities of the Information Assurance Department include:

- The preparation of an annual overall assessment of information assurance in Sweden;
- Fostering and contributing to cooperation between governmental organizations, corporations, and other important actors within this area;

358 http://www.krisberedskapsmyndigheten.se/english/index.jsp.

- Gathering, analyzing, and disseminating open-source information related to information assurance;
- The development of preventive IT security recommendations (consistent with ISO/IEC 17799) to support the IT security activities of other organizations;
- Initiating research and development in the area and summarizing risk and vulnerability assessments of different important societal systems;
- Managing the Board of Information Assurance (see below).

SEMA/The Board of Information Assurance

The *Board of Information Assurance* was established to support SEMA's activities in the area of information assurance. This board will create a network of skilled experts from a variety of important organizations in the area. The board replaced the earlier *Cabinet Office Working Group on Information Operations.*[359] The board's primary assignment is to assist the senior management of SEMA by supplying:

- Information about trends in research and development in the area of information assurance;
- Suggestions and viewpoints concerning direction, prioritizing, and realization of SEMA's activities in the area of information assurance.

The Swedish Defense Materiel Administration (FMV) and the Certification Body for IT security (FMV CB)

The *Swedish Defense Materiel Administration* (FMV) [360] is the Swedish procurement agency for the armed forces. The FMV has been involved in the area of IT security evaluations since 1989, performing in-house evaluations of equipment intended for use by the armed forces.

In the summer of 2002, the FMV was tasked by the government with establishing a Swedish scheme for the evaluation and certification of IT

359 SEMA document 0160/2003: Account of Measures Taken in Assuming Responsibilities from the Working Group on Information Operations (Redovisning av åtgärder för att överta arbetsuppgifter från Ag IO 0160/2003).

360 http://www.fmv.se.

security products to be used within Swedish governmental organizations. The establishment of the *Certification Body* at the FMV[361] is planned for the period 2003–2004.[362]

FRA/The Information Security Technical Support Team

The *Information Security Technical Support Team* is associated with the *Swedish National Defense Radio Establishment* (FRA),[363] which is the Swedish signals intelligence organization. It is a civil agency directly subordinated to the *Ministry of Defense*. The *Information Security Technical Support Team* consists of twenty experts in the field of IT security. The team is specifically intended to support:

- National crisis management where IT security qualifications are required;
- Identification of individuals and organizations involved in IT-related threats against critical systems.

On request, the team supports the Swedish authorities, agencies, and state-owned corporations that are responsible for critical functions in Swedish society with IT-security expertise and services. The customized services consist of penetration tests, forensic computer investigations, source code analysis, audits, risk analyses etc. The team co-operates on a regular basis with the national and international IT security community.

The Swedish Armed Forces

The *Swedish Armed Forces*[364] must be able to quickly respond to different types of threats and risks. The Swedish parliament has therefore decided to develop the armed forces according to the concept of *Network-Based Defense*. This places a great demand on the information infrastructure in terms of availability and security. The armed forces are therefore heavily involved in research and development in areas such as IT security and information infrastructures.

361 http://www.fmv.se/cb/index.asp?K=016&L=UK.

362 Evaluations will be performed according to the international standard ISO/IEC 15408 Evaluation Criteria for IT Security, also known as Common Criteria (CC).

363 http://www.fra.se/english.shtml.

364 http://www.mil.se.

The *Swedish Military Intelligence and Security Service* handles operational IT security in the armed forces during peacetime. In addition, the *National Communications Security Group* (TSA) offers Swedish defense organizations and industries advice and inspections of cryptographic systems.

The National Center for IO/CIP Studies (CIOS)

The *National Center for IO/CIP Studies* (CIOS) is located at the *Swedish National Defense College.*[365] CIOS conducts research and policy development in the fields of IO and CIP. Research at CIOS is funded by the *Ministry of Defense* and the *Swedish Emergency Management Agency* (SEMA).

The Swedish Defense Research Agency (FOI)

The *Swedish Defense Research Agency* (FOI) [366] focuses on R&D in the field of applied natural sciences and political sciences, such as security policy analysis. At the Division of Defense Analysis, the *Critical Infrastructure Studies Unit* (CISU) research group is carrying out a long-term research program on CIP sponsored by SEMA, in cooperation with Systems Analysis and IT Security – another FOI department. This department has acquired a deep knowledge of commercial and military IT systems and applications.

Ministry of Industry, Employment, and Communications

The Swedish National Post and Telecom Agency (PTS)

The *Swedish National Post and Telecom Agency* (PTS) is a government authority that monitors all issues relating to Information Communication Technology (ICT) and postal services. One of its key tasks is to ensure the development of functioning postal and telecom markets. Within the PTS, the *Department of Network Security* is responsible for security issues concerning ICT.

The *Department of Network Security* is tasked with monitoring developments concerning security issues and implementing measures to reduce the threats to ICT from sabotage and terrorism. Emergency measures are planned in consultation with the ICT operators, the Swedish armed forces, and other agencies. As an example, critical nodes in the ICT structures are hardened, and all nodes that are crucial for running the *.se*-domain

365 http://www.fhs.se.
366 http://www.foi.se.

autonomously have been installed within Sweden's borders. The *Swedish IT Incident Center* (see Early Warning) is associated with this department.

Department of Justice

The Swedish National Police Board (NPB)

The *Swedish National Police Board* (NPB) [367] is the central administrative and supervising authority of the police service. The NPB administers the National Criminal Investigation Department and the Swedish Security Service. Within the NPB, the *IT Crime Squad* has expert knowledge in investigating IT crime. This group supports the local Swedish police departments in IT crime investigations, participates in the education of parts of the judicial system, and assembles and communicates information about IT crime. The *Internet Reconnaissance Unit* is linked to this squad.

Additionally, there is the *Swedish Security Service* (SÄPO). Its fundamental duty is to prevent and detect crimes against the security of the realm. SÄPO is engaged in four main fields: protective security (including personal protection), counter-espionage, counter-terrorism, and protection of the constitution. Whenever IT criminal activity touches upon these fields, the *Swedish Security Service* is involved.

The Government Office

The Swedish Agency for Public Management

The *Swedish Agency for Public Management*[368] conducts studies and evaluations at the request of the government and modernizes the public administration with the use of ICT. The agency helps to develop Swedish administrative policy and also ensures that electronic infrastructure in the public sector is open and secure.

The report "*The 24/7 Agency – Criteria for 24/7 Agencies in the Networked Public Administration*"[369] proposes a four-stage agency development plan towards enhancing accessibility and providing service round

367 http://www.polisen.se.
368 http://www.statskontoret.se.
369 http://www.statskontoret.se/pdf/200041.pdf.

the clock, seven days a week. The criteria recommended by the agency focus primarily on government agencies' capacity to provide interactive services for the public and businesses. In the area of IT security specifically, the agency has compiled a strategy for information assurance in society[370] and produced a publication on secure authentication.[371] At the time of writing, the agency was carrying out the project "*Information Security at Authorities*". It aims at supporting other authorities with methods and tools for implementing threat and risk analyses according to ISO 17799.

Public Private Partnerships

The Swedish Emergency Management Agency (SEMA)

The *Swedish Emergency Management Agency* (SEMA) promotes interaction between the public sector and the business sector, and works to ensure that the expertise of non-governmental organizations (NGOs) is taken into account in emergency management.

There are two advisory councils connected to SEMA: the *Private Sector Partnership Advisory Council* and the *Board of Information Assurance*. However, it has not yet been established how the CIIP public private partnership will be institutionalized.

The Industry Security Delegation (NSD)

The *Industry Security Delegation* (NSD)[372] is a delegation within the *Confederation of Swedish Enterprise* (Svenskt Näringsliv) whose objective is to increase cooperation between enterprises, organizations, and authorities, and to promote comprehensive views on vulnerability and security issues. The overall goal of this network structure is to enhance security and risk awareness among the general public and the business sector. The NSD arranges courses in information assurance as well as crisis and risk management to help its members improve security.

370 *Coherent strategy for information assurance in society* (Sammanhållen strategi för samhällets IT-säkerhet, rapport Statskontoret rapportserie, 1998, p. 18).

371 *Security related to electronic identification* (Säkerhet med elektronisk identifiering, rapport i Statskontorets rapportserie 1999, p. 30).

372 http://www.svensktnaringsliv.se/index.asp?pn=155246.

The Swedish Information Processing Society (DFS)

The *Swedish Information Processing Society* (DFS) [373] is an independent organization for IT professionals with 32'000 members. The DFS owns SBA brand of security products (the abbreviation stands for SårBarhetsAnalys, or "vulnerability assessment" in Swedish), which focus on risk analysis and information security. SBA is said to be a Swedish de facto standard.

Early Warning Approaches

PTS/The Swedish IT Incident Center (SITIC)

In May 2002 the Swedish government tasked the PTS with establishing the *Swedish IT Incident Center* (SITIC) [374]. The center was officially opened on 1 January 2003. SITIC supports national activities for the protection against IT-incidents by:

- Operating a system for information exchange on IT incidents between both public and private organizations and SITIC;
- Rapidly communicating information on new problems that can disrupt IT systems to the public;
- Providing information and advice on preventive measures;
- Compiling and publishing incident statistics as input to the continuing improvements of preventive measures.

373 http://www.dfs.se.
374 http://www.sitic.se.

Center for Security Studies, ETH Zurich
Volume 2, Zürich 2004.

The International CIIP Handbook 2004: An Inventory and Analysis of Protection Policies in Fourteen Countries

Myriam Dunn and Isabelle Wigert

edited by
Andreas Wenger and Jan Metzger