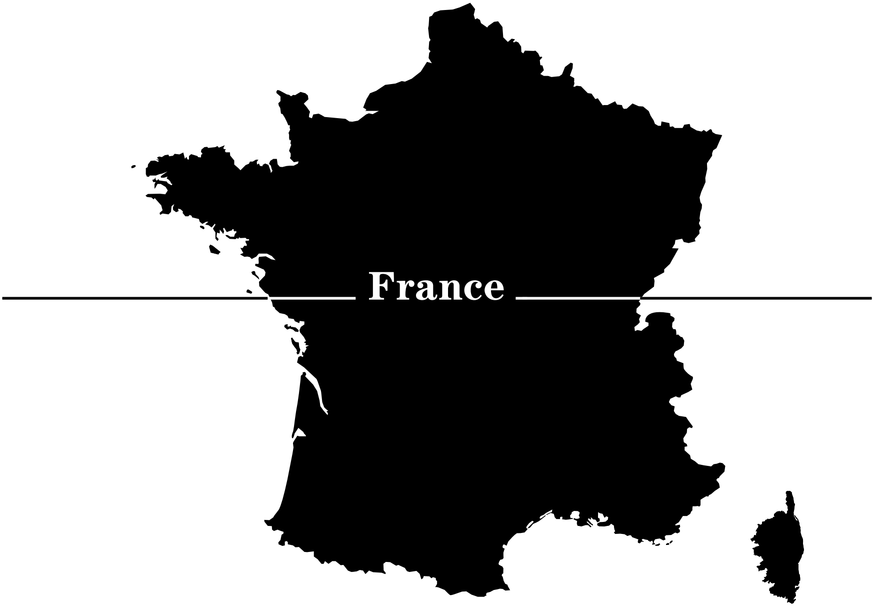
CIIP Country Surveys



France

France

Critical Sectors

All infrastructures that are vital to the maintenance of primary social and economic processes are considered critical sectors in France. These critical sectors are the following:[134]

- Banking and Finance,
- Chemical and Biotechnological Industries,
- Energy and Electricity,
- Nuclear Power Stations,
- Public Health,
- Public Safety and Order,
- Telecommunication,
- Transport Systems,
- Water Supply.

Initiatives and Policy

Government Action Program for an Information Society (PAGSI)

In August 1997, the prime minister of France designated the information and communication society as a priority for government action. The objective was to build an information society for all, to prevent a digital divide, and to help France catch up with other countries in terms of Internet usage. Making government services available online has been the main goal of the formation of the *Government Action Program for an Information Society* (PAGSI)[135] in January 1998 (adopted at the meeting of the *Inter-ministerial Committee for Information Society* (CISSI)). In addition to the improvement of general public services, standardization, and training for civil servants, PAGSI supports projects in the fields of education, culture, electronic com-

[134] Haut Comité Francais pour la Défense Civile. *Livre Blanc HCFDC: 20 ans, 20 constats et propositions*. 2003, p. 18. See also: Preparation for Y2K in France, sensitive sectors: http://www.urgence2000.gouv.fr/y2k/1.htm.

[135] http://www.internet.gouv.fr/francais/textesref/essentiel-archives.htm.

merce, and research and innovation, and establishes appropriate regulations for the safer use of information technologies and networks. Two of the main priorities of the PAGSI action plan are managing the *Security of Information Systems* (SSI) (see below) and combating cyber-threats.[136]

Expression of the Needs and Identification of Security Objects (EBIOS)

In 1997, the *Directorate for the Security of Information Systems* (DCSSI) developed and published the first version of the guide *Expression of the Needs and Identification of Security Objects* (EBIOS).[137] It outlines a method for risk analysis concerning the security of information systems (for more details, see Part II).

Preparation for Y2K in France

The *Y2K French National Agency* was set up in 1998. Y2K Senior Officers were appointed in each ministry. The Agency, commissioned by the minister for economy, finance, and industry and by the secretary of state for industry, stimulated awareness of the Y2K issue in France, especially within the government services and small and medium enterprises (SMEs). The website "urgence2000" was established as an important information source for actors interested in the topic. The government's task was to make sure that the main infrastructures would be still functioning at the transition to the year 2000.[138] However, it does not seem that the Y2K experience was subsequently taken into consideration when dealing with information security policies.[139]

[136] Service d'Information du Gouvernement. *Four years of Government measures to promote the information society* (August 2001). http://archives.internet.gouv.fr/francais//textesref/agsi4years.pdf.

[137] Premier Ministre, Service Central de la Sécurité des Systèmes d'Information. *Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS)*. Technical Guide – English Version, Version 1.02. February 1997.

[138] http://www.urgence2000.gouv.fr/y2k/1.htm.

[139] Dependability Development Support Initiative (DDSI) – Dependability Overview: *National Dependability Policy Environments*, p. 106, (September 2002).

Organizational Overview

In France, the *Secretary-General of National Defense (SGDN)*, a service attached to the Prime Minister's Office, bears complete responsibility for organizing CIP.

Furthermore, within the Ministry of Defense, the *Direction for Security of Information Systems*, (DCSSI), the *Inter-Ministerial Commission for the Security of Information Systems* (CISSI), and the *Advisory Office* are the key organizations responsible for CIP/CIIP, whereas in the Ministry of Interior, the *Central Office for the Fight Against Hi-Tech Crime* plays a comparative lead role.

Public Agencies

Secretary-General for National Defense (SGDN)

The *Secretary-General for National Defense* (SGDN) deals with national and international security affairs. The SGDN is directly subordinated to the French prime minister. The organization was first called into action for Y2K, when a specific network of contacts among different bodies from the public and private sectors became involved under the coordination of the SGDN.

The SGDN promotes and co-ordinates the activities between ministries involved in CIIP. This includes responsibility for the security of information systems (since 1996) and chairing the *Inter-Ministerial Commission for the Security of Information Systems* (CISSI),[140] as well as responsibility for the protection of classified and sensitive military information. The SGDN deals with the impact of the scientific and technical revolution on defense and security policy, focusing on securitization of information and communication technology relating to military as well as civil matters. In this area, the SGDN works closely together with DCSSI.[141]

Since its establishment, SGDN has been refined. One visible aspect is *Piranet*, an equivalent to *VigiPirate*, which involves all security forces (police and army) when the situation requires it, and decisions are taken at the prime minister's level; it deals directly with cyber crime, especially (but not exclusively) with attacks targeted at Critical Infrastructure.[142]

[140] Commission interministérielle pour la Sécurité des Systèmes d'Information (CISSI).

[141] http://www.premier-ministre.gouv.fr/fr/p.cfm?ref=6467&txt=1#contenu.

[142] http://www.ssi.gouv.fr/fr/actualites/afnor-dcssi-270303/pdf/AFNOR270303.pdf.

Central Directorate for Security of Information Systems (DCSSI)[143]

The *Central Directorate for the Security of Information Systems* (DCSSI), which is linked to the *Secretary-General for National Defense* (SGDN), was created in 2000. The DCSSI administers the *Security of Information Systems* (SSI) website and co-ordinates its activities. The SSI website comprises information on the *Computer Emergency Response Team* (CERTA),[144] information on regulation, certification, authorization, electronic signature, and cryptography, and provides technical advice.[145] The DCSSI advises the French government, and it supports the national regulation authority and public services in the field of security of information systems. It builds up scientific and technical expertise in this field, evaluates threats, and issues alerts. It also has a training center for administration staff. Furthermore, it is responsible for the co-ordination of activities between the different government administrations.[146]

Advisory Office

A core operational part of the *Central Directorate for the Security of Information Systems* (DCSSI) is the *Advisory Office* (le bureau conseil), which assists the administration in CIIP matters. If it is in the overall interest of France's security, the *Advisory Office* also advises and collaborates with the private sector. In addition, the *Advisory Office* publishes methodological and technical guides to clarify concepts presented in the *Information Technology Security Evaluation Criteria* (ITSEC)[147] (see Part II for more details).

Central Office for the Fight Against Hi-Tech Crime

In May 2000, the *Central Office for the Fight against Cyber-Crime*[148] was launched by the Ministry of Interior and co-operates with Interpol. It deals with unauthorized intrusions and crime in the field of information and communication technologies and supports the legal investigations in this

[143] Direction Centrale de la Sécurité des Systèmes d'Information. (DCSSI): http://www.ssi.gouv.fr/fr/dcssi/index.html.

[144] Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques informatiques: http://www.ssi.gouv.fr/fr/index.html.

[145] http://www.ssi.gouv.fr/fr/index.html.

[146] http://www.ssi.gouv.fr/fr/dcssi/index.html.

[147] http://www.ssi.gouv.fr/fr/dcssi/conseil.html.

[148] http://www.interieur.gouv.fr/rubriques/c/c3_police_nationale/c3312_oclctic/missions.

field. The Central Office has been granted nation-wide jurisdiction in this matter and works closely together with the national police as well as the private sector. It provides assistance to all agencies responsible for fighting computer crime such as the police, gendarmerie, and sensitizes the actors at stake.[149]

Public Private Partnerships

The Strategic Advisory Board on Information Technologies (CSTI)

The *Strategic Advisory Board on Information Technologies* (CSTI)[150] was created in July 2000 by a government committee meeting on information society. It is chaired by the French prime minister. The CSTI is composed of leading entrepreneurs from industry and research and development. It is responsible for recommendations to government concerning CIIP topics and the French contribution to the *6th European Framework Research and Development Program*. The CSTI, in particular, has the duty

- to communicate opinions and recommendations to the government on the studies and documents commissioned,
- to maintain a permanent dialog with representatives of industry and to improve co-ordination between private and public researchers (and the industry),
- to define national priorities and to select areas where more action is required,
- to provide general monitoring and warning services in the area of CIIP.

French Dependability Institute (ISDF)

The *French Dependability Institute* (ISDF) provides a forum for the private sector to discuss CIIP issues across a variety of industries. It is strongly supported by the *Department of Industry* as well as representatives from the automotive, military, and space industries and from professional organizations. ISDF fosters connections on information exchange with the industry and aims at becoming the official representative of France in international organizations in the field of CIIP.[151]

[149] http://www.interieur.gouv.fr/rubriques/c/c3_police_nationale/c3312_oclctic/missions.

[150] Conseil Stratégique des Technologies de l'Information: http://www.csti.pm.gouv.fr.

[151] DDSI – Dependability Overview: *National Dependability Policy Environments*, p. 108.

Every year since 1990, ISDF has launched a set of projects in connection with the activities of its members. These projects reflect current issues in the field of securing information systems such as reliability, availability, maintainability, safety, and security. As there are about twenty-five technical working groups at ISDF, gathered into seven colleges (management; methods and tools; maintainability; human factor; safety; education and standards; software and systems dependability), the propositions embrace the whole spectrum of safety and dependability topics.[152]

Early Warning Approaches

Computer Emergency Response Teams (CERTs) in France

In France, there are three different Computer Emergency Response Teams (CERTs) addressing three different constituencies: CERT-RENATER, CERTA, and CERT-IST.

CERT-RENATER has existed since 1993 and especially addresses research centers and academic institutions. CERT-RENATER gathers and provides information about information security and is dedicated to the membership of GIP RENATER, the *National Network of Telecommunications for Technology, Education, and Research*.[153]

The *Central Direction for the Security of Information Systems* (DCSSI) has hosted a Computer Emergency Response Team called CERTA[154] since 2000. CERTA deals in particular with the French administration services. As a center of expertise, it evaluates CIIP threats and gives advice, issues warnings, and provides information on how to prevent, respond to, and handle an attack against information systems.

CERT-IST (*CERT-Industry, Services, and Tertiary*) was launched in 1999 by Alcatel (a telecom company), CNES (the French Space Agency), France Telecom, and the TotalFinaElf energy group. It serves France's private sector as a contact point for security incident response. CERT-IST provides alerts and means of protection against computer attacks aimed at French enterprises. It also helps the association members with incident handling.[155]

[152] http://www.bull.com/fr/isdf/pgena.htm.

[153] http://www.renater.fr/.

[154] http://www.certa.ssi.gouv.fr/.

[155] http://www.cert-ist.com.

CERT-IST interacts with the French national security organizations SGDN and DCSSI, in conjunction with CERT- RENATER and CERTA.[156]

CLUSIF (Club de la Sécurité des Systèmes d'Information Français)

The *Club de la Sécurité des Systèmes d'Information Français* (CLUSIF) was created in 1984 and is a non-profit organization of over 600 members representing 300 corporations or administrative organizations. CLUSIF fosters the sharing of information and experiences between its members, keeps users informed about new IT security material, and provides IT security information and whitepapers. Furthermore, it is involved in CIIP activities related to education, raising awareness, and security threat analysis.[157]

The *Secretary-General of National Defense* (SGDN) is also an early warning actor, to the extent that the office coordinates the ministerial officials called High Functionaries of Defense (Hautes fonctionnaires de Défense).[158]

[156] DDSI – Dependability Overview: *National Dependability Policy Environments*, p. 107.

[157] https://www.clusif.asso.fr/en/clusif/present/.

[158] Présentation des nouvelles orientations de l'Etat en sécurité des systèmes d'information. Séminaire DCSSI-AFNOR, 27 March 2003. http://www.ssi.gouv.fr/fr/actualites/afnor-dcssi-270303/pdf/AFNOR270303.pdf.

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