CIIP Country Surveys

Italy

The Country Survey of Italy 2004 was written with the help of Roberto Setola, Working Group for Critical Information Infrastructure Protection; Giovanna Dondossola, CESI, and Sandro Bologna, Italian National Agency for New Technologies, Energy and the Environment (ENEA).

Italy

Critical Sectors

The main premise underlying Italy's CIIP policy is that the welfare of most countries depends increasingly on information and communication technology (ICT) systems.[228] ICT plays an important role in a number of critical sectors of Italian society.[229] There is no official definition of critical sectors in Italy, but the following sectors are taken into consideration:[230]

- Banking and Finance,
- Civil Defense,
- (Tele-) Communication,
- E-Governance,
- Energy,
- Gas,
- Public Administration,
- Public Health,
- Transport Systems on Air and on Land,
- Water.

Initiatives and Policy

The subject of CIIP was officially discussed for the first time in a meeting held at the *Ministry of Foreign Affairs*, organized by the *Directorate-General for Economical Cooperation* of the same ministry in March 2000. It was a preparatory meeting to identify potential areas of scientific and technological cooperation between Italy and the US. A second important occasion to foster awareness of the problem was a *Workshop on Critical Information Infrastructure Protection* jointly organized between the *Italian Prime Minister's Office* and the US embassy in Rome in May 2002.

228 Gruppo di Lavoro sulla Protezione delle Infrastrutture Critiche Informatizzate. *Protezione delle Infrastrutture Critiche Informatizzate – La realtà Italiana* (ottobre 2003).

229 Ministero per l'innovazione e le tecnologie. *Le politiche governative in tema sicurezza*. http://securit.cineca.it/eventi/atti_290503/cilli.pdf.

230 Information provided by the Italian experts involved.

A follow-up *Working Group on Critical Information Infrastructure Protection* was set up at the *Ministry for Innovation and Technologies* in March 2003. All ministries involved in the management of critical infrastructures are represented inside the group, together with many Italian infrastructure operators and owners as well as some research institutes. The main goal of this Working Group was to help the Italian government to come to a better understanding of the problems associated with CIIP, particularly accidental and deliberate faults, and to provide a basis for the identification of organizational requirements and initiatives that could increase the robustness of critical infrastructures.

Critical Information Infrastructure Protection

The *Working Group on Critical Information Infrastructure Protection* in October 2003 released the document *Protezione delle Infrastrutture Critiche Informatizzate – La realtà Italiana* (Critical Information Infrastructures Protection: The Case of Italy) offering a synthesis of its efforts. The document describes many elements of the Italian infrastructures, emphasizes their interdependencies and suggests CIIP policy strategies. In particular, the Working Group suggests that full responsibility for the correct implementation of a survivability policy should remain with the individual owners and operators of critical infrastructure, while the government should be responsible for the definition of an overall policy to minimize interdependencies and cascading failures. The document also suggests:

- The establishment of a *National Interest Group on Critical Infrastructure* (GdIN – Gruppo di Interesse Nazionale) that would survey the requirements of different owners and operators.
- The definition of a national research and development agenda in the area of Critical Infrastructure Protection.
- The realization of an Interdependencies Simulation and Analysis Center (SAI – Centro Virtuale di Simulazione e Analisi delle Interdipendenze).[231]

Action Plan for E-Government

The Italian government intends to reform the public administration to meet user needs, to provide modern services, and create public value. The necessary steps are outlined in detail in the e-Government Action Plan of June

231 Information provided by expert.

2000 .[232] One crucial step is the establishment of a model for e-Government. It must be based on a modern infrastructure that will ensure the efficient and secure provision of a number of basic functions. To achieve this goal, the *Ministry for Innovation and Technologies* has developed the following strategic reference points for e-Government:

- Service Provision,
- Digital Identification,
- Access Channels,
- Service Provision Agencies,
- Interoperability and Cooperation,
- Communication and Infrastructure.

The Government's Guidelines for the Development of the Information Society

On 28 May 2002, the *Committee of Ministers for the Information Society* welcomed the *Government Guidelines for the Development of the Information Society* published by the Ministry of Innovation and Technologies.[233] It is stated the Italian government's commitment to making Italy a leader in the digital age, stressed its dedication to modernizing the country through widespread use of new ICT in both the public and private sectors, and vowed to boost the country's competitiveness by accelerating e-Business and e-Government.[234] The *Government Guidelines* also deal with network security and introduce a national plan for ICT security and privacy. The aim of this security model is to increase network security; in particular, it aims to create trust and to convince consumers and businesses to use the Internet, especially in their dealings with government. The national plan is based on the following principal actions:

- The introduction of an *ICT Security Directive* (to define the basic minimum of security that all government departments must achieve);
- The establishment of a *National Technical Committee for ICT Security* (to co-ordinate all activities);

232 http://www.innovazione.gov.it/eng/egovernment/index.shtml.

233 Minister for Innovation and Technologies. *The Government's Guidelines for the Development of the Information Society.* (June 2002). http://www.innovazione.gov.it/eng/documenti/linee_guida_eng.pdf.

234 Ibid., p. 19f. http://www.innovazione.gov.it/eng/documenti/linee_guida_eng.pdf.

- The establishment of an organizational model for ICT security (to include guidelines, recommendations, standards, and certification procedures);
- The introduction of a *National Plan for ICT Security* (to specify the activities, areas of responsibility, and deadlines for the introduction of necessary standards and methods for security certification in government);
- The final certification of ICT security for the public administration within five years.[235]

Organizational Overview

Besides the *Working Group on Critical Information Infrastructures Protection*, the main Italian government bodies dealing with CIIP are the *Ministry of Innovation and Technologies*, the *Ministry of Communication*, and the *Ministry of the Interior* –(*Postal and Communications Police*).

Public Agencies

Ministry for Innovation and Technologies

The *Ministry for Innovation and Technologies*[236] is charged with promoting specific action plans and programs for the deployment of information technologies in order to improve governmental online services for citizens and business. A *Committee of Ministers for the Information Society* was set up in 2001 to support the development and use of information and communication technologies in public administration, as well in Italian society as a whole. The first meeting of this committee was on 19 September 2001. The following areas were chosen for priority action:

- Communications (it was decided to set up a joint Ministry of Communications and Ministry for Innovation and Technologies Task Force on Broadband Communication);
- Education and training;
- Small and medium-sized enterprises and legislative change.[237]

235 Ibid., pp. 65–66. http://www.innovazione.gov.it/eng/documenti/linee_guida_eng.pdf.
236 http://www.innovazione.gov.it/eng/index.shtml.
237 http://www.innovazione.gov.it/eng/intervento/pol_soc_eng.shtml.

National Technical Committee on Computer and Telecommunications Security within the Public Administration

On 16 October 2002, the *Ministry for Innovation and Technologies* and the *Ministry of Communication* created the *National Technical Committee for ICT Security in the Public Administration*. The establishment of this new committee followed from the Directive on ICT Security for the Public Administration, which enacts EU recommendations with the important initial aim of achieving compliance with a set of minimum-security standards. The Technical Committee can therefore be seen as the operative arm of the new national IT security policy.[238]

The *National Technical Committee for ICT Security in the Public Administration* was constituted in July 2002 with support from the *Ministry for Innovation and Technologies* and the *Ministry for Communications*[239].

The committee aims to attain a satisfactory security level in information systems and digital communications, in compliance with international standards, in order to guarantee the integrity and reliability of the information. It prepares strategy proposals concerning computer and telecommunications security for the public administration; in particular, it develops:

- The Emergency National Plan for the security of information and communication technologies in the public administration. The committee annually verifies its state of advance, and proposes corrective measures if required;
- The ICT security national organizational model for the public administration. The committee monitors its level of activation and application.

Furthermore, the committee formulates proposals for regulating the certification and security assessment, as well as certification criteria and guidelines for ICT security certification in the public administration, on the basis of national, sectoral, and international norms of reference.

Finally, the committee elaborates guidelines for agreements with the Department of Public Administration for training public employees in ICT security. Among the other proposals, the group is to set up the Computer Emergency Response Team (CERT) for the Public Central Administration (CERT-PA). It will have a central "Early-Warning System" operating around the clock.

238 http://www.innovazione.gov.it/eng/comunicati/2002_10_11.shtml.

239 Minister for Innovation and Technologies. *The Government's guidelines for the development of the Information Society.* http://www.innovazione.gov.it/eng/documenti/linee_guida_eng.pdf.

National Center for Informatics in the Public Administration (CNIPA)

The *Authority for IT in the Public Administration* (AIPA), founded in 1993, was transformed into the *National Center for Informatics in the Public Administration* (CNIPA) in 2003.[240] CNIPA belongs to the *Ministry of Innovation and Technologies*, and its head is nominated by the *Council of Ministries*. It addresses central and local administration, especially the elements responsible for IT systems in the public administration.[241] CNIPA's main task is to promote modern information technologies in the Italian public administration, to establish standards and methods, to deal with security issues, and to make recommendations and technical regulations in the field of IT for public administration.[242] CNIPA published a comprehensive guide on the protection of personal data in 2001.[243]

Ministry of Communication

The *Ministry of Communication* supervises postal and telecommunications services, acting personally as a regulator, as well as practicing a policy of coordination, supervision, and control – tasks that were previously in the purview of the *Ministry of Post and Telecommunications*.[244] It is involved in the definition of the security polices for communication and the Internet.

Permanent Working Group on Network Security and Communications Protection

The *Permanent Working Group on Network Security and Communications Protection* was constituted in 1998. It was composed of representatives of the Ministries of Communication, Internal Affairs, and Justice. Within the group, the "Subgroup Internet" deals with investigative and judicial matters related to the Internet. This subgroup is preparing a list of data that Internet Service Providers will have to supply to the police if so ordered by a judge. A similar list already exists for telephone companies. A coordination center was recently constituted to coordinate crime-fighting with other governmental institutions.[245]

240 http://www.cnipa.gov.it.
241 http://www.cnipa.gov.it.
242 http://www.cnipa.gov.it.
243 http://www.innovazione.gov.it/ita/intervento/normativa/allegati/dl_030630.pdf.
244 http://www.comunicazioni.it/en/index.php?Mn1=5.
245 Information provided by the Italian experts involved.

The Postal and Communications Police

In 1992, the *Ministry of the Interior* issued a directive assigning to the state police specific responsibilities for IT and telecommunications security that are in fact carried out by the *Postal and Communications Police*. The *Postal and Communications Police* is a flexible organization with a staff of around 2000 highly trained officers, subdivided in a central service and placed at the peak of a structure involving 19 regional departments and 76 territorial sections. The *Postal and Communications Police* reviews communications regulations, studies new technical investigative strategies to fight computer crime, and coordinates operations and investigations for other offices. This police force also collaborates with other institutions – in particular with the Ministry of Communication and the Privacy Authority – and with private operators who deal with communications. As the Italian contact point for G8 country computer crime offices, it is available at all times. This particular organizational aspect guarantees a quick, qualified, and efficient response[246] in the event of a threat or computer attack originating nationally or internationally.

From a technical and operational point of view, the *Postal and Communication Police Service* will host and manage an emergency center at both the national and regional levels, in order to better deal with computer crimes against critical infrastructure and conduct preventive monitoring activities. The center will be a focal point for the evaluation of threats, thus providing adequate countermeasures to face such situations.

Establishment of a National Certification Body for the Information Technologies

The Ministry for Innovation and Technologies and the Ministry of Communication plan to establish the *Istituto superiore delle comunicazioni e delle tecnologie dell'informazione* (ISCTI) as the national body for security certification in IT. It will be responsible for certifying IT systems' compliance with ITSEC, SO/IEC IS-15408 (Common Criteria) or ISO standards.

246 http://www.poliziadistato.it/pds/english/specialist.htm.

Public Private Partnerships

Italian Association for Security in Informatics: CLUSIT

The *Italian Association for Security in Informatics* (CLUSIT) [247] is a non-profit organization founded in 2000. It is based at the *Department of Informatics and Communications* (DICO) at the University of Milan.[248] CLUSIT addresses individuals and organizations involved or interested in information security in order to promote awareness, continuous education, and information-sharing. The specific duties of CLUSIT are:

- To raise awareness concerning computer security among companies, the public administration, and citizens;
- To participate in and contribute to the development of laws, practical codes, and computer security at national and international level;
- To help define certifications for computer security professionals;
- To promote the adoption of methodologies and technologies to contribute to the improvement of the security level of the information infrastructure at all levels.[249]

National Interest Group on Critical Infrastructure: GdIN – Gruppo di Interesse Nazionale

The *Working Group on Critical Information Infrastructure Protection* has strongly encouraged the constitution of a forum, to be formed on a voluntary basis, of the owners and operators of critical infrastructure. This forum will serve as a meeting-point to exchange best practices, and report to the government institutions on needs and problems.

247 Associazione Italiana per la Sicurezza Informatica: http://www.clusit.it/homee.htm.
248 http://www.dico.unimi.it.
249 http://www.clusit.it/indexe.htm.

Early Warning Approaches

CERT-IT

The *Italian Computer Emergency Response Team* (CERT-IT) is the main body in charge of early warning at the technical level in Italy.[250] CERT-IT was founded in 1994 as a non-profit organization. It is mainly supported by the *Department of Informatics and Communications* (DICO) at the University of Milan.[251] CERT-IT is a member of the Forum of Incident Response and Security Teams (FIRST). Its main goal is to contribute to the development of security in the computer world. It promotes research and development activities in security systems, provides information about computer security, and has an expertise team for handling computer incidents.[252] CERT-IT has also developed an electronic forum in order to disseminate all information related to vulnerabilities in a timely and widespread fashion.[253]

Other CERT-IT activities in Italy include the GARR-CERT and the MoD CERT (Ministry of Defense). A CERT-PA is planned by the *National Technical Committee on Computer and Telecommunications Security* within the public administration. Its task will be to support the public central administrations.

Incident Response Italy: IRItaly

Incident Response Italy (IRItaly)[254] is a project of the Department of Information Technologies at the University of Milan-Crema that was presented on 10 June 2003 at the *First Italian Forum on Incident Response in the Information Security.* Its main aim is to inform the Italian scientific community, small and medium-size private organizations, and private and public actors on incident response issues.

250 http://securit.cineca.it/eventi/atti_290503/cilli.pdf.
251 http://www.dico.unimi.it/.
252 http://idea.sec.dsi.unimi.it/index.html.
253 Dependability Development Support Initiative (DDSI) – *Dependability Overview: National Dependability Policy Environments* (2002), p. 159.
254 www.iritaly.org.

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