CIIP Country Survey

United Kingdom

The Country Survey of the United Kingdom 2004 was written with the help of Stephen Cummings, Ted Barry, and John Park, National Infrastructure Security Coordination Centre (NISCC).

United Kingdom

Critical Sectors

In the United Kingdom, the *Critical National Infrastructure* (CNI) comprises those parts of the infrastructure for which "the continuity is so important to national life that loss, significant interruption, or degradation of service would have life-threatening, serious economic or other grave social consequences for the community or would be of immediate concern to the Government."[409] Many of the critical services that are essential to the well being of the UK depend on IT and are provided by both the public and private sectors. The term 'national' has been adopted to indicate infrastructures that are critical to the UK's national interest.[410]

The ten sectors and 39 sub-sectors that comprise the CNI reflect the government's current classification of what is critical to UK interests considering vulnerabilities to physical and electronic attack and from the perspective of civil contingency planning. This comprehensive list is therefore jointly used by all UK agencies involved in CIP, CIIP, or emergency management:[411]

- Communications (Data Communications, Fixed Voice Communications, Mail, Public Information, Wireless Communications),
- Emergency Services (Ambulance, Fire and Rescue, Marine, Police),
- Energy (Electricity, Natural Gas, Petroleum),
- Finance (Asset Management, Financial Facilities, Investment Banking, Markets, Retail Banking),
- Food (Produce, Import, Process, Distribute, Retail),
- Government and Public Services (Central Government, Regional Government, Local Government, Parliaments and Legislatures, Justice, National Security),
- Hazards and Public Safety (Chemical, Biological, Radiological and Nuclear (CBRN) Terrorism; Crowds and Mass Events),
- Health (Health Care, Public Health),
- Transport (Air, Marine, Rail, Road),
- Water (Mains Water, Sewage).

[409] http://www.niscc.gov.uk/cni/index.htm.

[410] Information provided by an NISCC expert in 2003.

[411] Ibid.

A *UK Government Strategy for Information Assurance* has been developed. The *Central Sponsor for Information Assurance* (CSIA), a unit within the *UK Cabinet Office*, is implementing this strategy in partnership with other organizations across the public sector. A public document relating to the main points of the strategy is to be launched early in 2004.

Initiatives and Policy

CIIP Policy Guidelines

The British government aims at protecting the CNI from two kinds of threat: terrorist attacks against installations and equipment on the one hand and electronic attacks against computer or communications systems on the other hand.[412]

The government has produced a *Government Information Assurance Strategy*, which complements counter-terrorism strategies, national security considerations, and measures against high-tech crime. The aim of the strategy is to provide ongoing assurance to the government that the risks to information systems underpinning key public interests are appropriately managed. Most importantly, the strategy recognizes that within an increasingly interdependent and interconnected information infrastructure, the government must concern itself with the confidentiality, availability, and integrity of *all* information systems. The *Central Sponsor for Information Assurance* (CSIA) is the coordinating body for the strategy, working alongside other key government bodies.

e-commerce@its.best.uk

The UK approach to the information society was laid out in 1998 by the *Department of Trade and Industry's Competitiveness White Paper* that noted the major role played by ICT in facilitating growth.[413] In September 1999, the *Performance and Innovation Unit* (now the *Cabinet Office's Strategy Unit*[414]) issued "*e-commerce@its.best.uk*", a report outlining the

[412] http://www.mi5.gov.uk/major_areas_work/major_areas_work_5_4.htm.

[413] Department of Trade and Industry. *UK Digital Content: An Action Plan for Growth* (1998). http://www.dti.gov.uk/comp/competitive/wh_int1.htm.

[414] http://www.strategy.gov.uk/about/about.shtml.

organizational and policy framework for achieving these goals.[415] The report's recommendations have been implemented under a national strategy known as *UK Online*, which gives access to government information and services online. UK Online aims to give every citizen Internet access by 2005.[416]

UK Online Strategy

The *UK Online Strategy* is overseen by the e-Minister and the e-Envoy, who report directly to the prime minister. The e-Envoy is responsible for ensuring that all government services are available electronically by 2005 and supports government plans to develop the UK as a world leader for electronic business.[417] The *UK Online Action Plan* includes 113 detailed recommendations covering 26 commitments to ensure that the UK is at the forefront of the knowledge economy revolution.[418]

Progress Report on Electronic Security

The e-Minister and the e-Envoy delivered their progress report on electronic security to the prime minister on 3 March 2003.[419] The key developments highlighted in the report were:

- A new information security element of the *UK Online for Business Website* was launched, with a view to offering basic security advice;[420]
- The *National Hi-Tech Crime Unit* (NHTCU) has developed a confidentiality charter to address the concerns of business, which has traditionally been reluctant to report IT incidents;
- The Office of the e-Envoy/CSIA has published a complete set of security frameworks describing measures that organizations should take to secure their electronic service delivery systems against assessed risks;
- The *Office of the e-Envoy/CSIA* has also published advice on the selection of biometrics products, which are of increasing interest;

[415] Performance and Innovation Unit Report: "*e-commerce@its.best.uk*" (September 1999). http://www.cabinet-office.gov.uk/innovation/1999/ecomm.shtml.

[416] http://www.ukonline.gov.uk/Home/Homepage/fs/en.

[417] http://www.e-envoy.gov.uk/oee/oee.nsf/sections/about-oee/$file/aboutus.htm.

[418] http://www.e-envoy.gov.uk/oee/oee.nsf/sections/ukonline-top/$file/ukstrategy.htm.

[419] *Monthly Report from the e-Minister and e-Envoy* (3 March 2003). http://www.e-envoy.gov.uk/oee/OeE.nsf/sections/reports-pmreports-2003/$file/3march03.htm.

[420] http://www.ukonlineforbusiness.gov.uk/informationsecurity.

- The *Office of the e-Envoy* has published guidelines for the registration of individuals and organizations with governmental electronic services, and a skeleton *Information Security Policy Document* that public-sector organizations can use to develop their own security policies;
- The *Central Sponsor for Information Assurance* (CSIA) is supporting the *National Infrastructure Security Co-ordination Centre* (NISCC) in establishing the first *Warning*, *Advice and Reporting Point* (WARP) in partnership with *London Connects*, the agency responsible for delivering electronic government (e-Government) in London.

Standard for Information Security Management

The *Cabinet Office's Security Division* promotes good practice in information security within government departments and across governmental systems. This includes the development of ISO/IEC 17799, which began as the British Standard BS 7799, one of the most popular codes of practice relating to information technology and information security management.[421] It deals with external, internal, accidental, and malicious threat sources, and aims at ensuring the confidentiality, integrity, and availability of information. The code deals with:

- Security policy and organization;
- Information security infrastructure;
- Information classification;
- Secure areas;
- Responding to security incidents and malfunctions;
- Network management and access control.[422]

[421] http://www.cabinet-office.gov.uk/cabsec/Previous%20years/1998/sd/index.htm.

[422] http://www.bsi-global.com/Portfolio+of+Products+and+Services/IT+Information/Info+Security/Overview/Topics.xalter.

Organizational Overview

In the UK, the main responsibility for CIIP lies with the home secretary.[423] However, a number of other departments play a role in the protection of the various CNI sectors and contribute resource and expertise to the British CIIP effort. These contributions are coordinated by an interdepartmental center that reports to the Home Office – the *National Infrastructure Security Co-ordination Centre* (NISCC). Policy is formulated and developed at a working level through a dialog between several government departments and bodies: the NISCC; the *Central Sponsor for Information Assurance* (CSIA); the *Civil Contingencies Secretariat* (CCS); the *Cabinet Office Security Policy Division*; and the *Home Office* itself. The various roles and responsibilities of these governmental bodies are described below.

While the NISCC has the lead in coordinating CIIP efforts within government and with the private sector, other responsibility is placed with a number of bodies:

- CIIP is a subset of CIP: the provision of physical protective security advice to the CNI is the responsibility of the *Security Service* and the *Police*;
- CIIP (focusing on just the CNI) is also a subset of the wider information assurance strategy dealing with all aspects of the information society. Responsibility for this lies with the *Central Sponsor for Information Assurance*;
- The coordination of the government's contingency and emergency response effort (regardless of the cause of the disruption) is the responsibility of the *Civil Contingencies Secretariat* (CCS) within the Cabinet Office.

Public Agencies

National Infrastructure Security Co-ordination Centre (NISCC)

The protection of the CNI from electronic attack has been the responsibility of the *National Infrastructure Security Co-ordination Centre* (NISCC) since 20 December 1999. The latter is an interdepartmental center that coordinates and develops existing work within government departments and agencies as well as CNI organizations in the private sector. The NISCC operates under a director, who is a member of a management board chaired

[423] http://www.homeoffice.gov.uk/terrorism/govprotect/infrastructure/index.html.

by the Home Office. The other members of the board are from the *Cabinet Office*, the *Communications-Electronics Security Group* (CESG – the government's technical authority on information security), the *Security Service*, the *Ministry of Defence*, the *Police*, and the *Department of Trade and Industry* (DTI).

The NISCC aims to establish partnerships with CI providers. It has various duties towards its CNI partners across the UK:

- Promoting dialog with owners of CI systems to identify the most critical systems;
- Issuing alerts or warnings of attack;
- Providing assistance in response to serious attacks;
- Collecting, analyzing, and disseminating information about the threat;
- Undertaking research into vulnerabilities;
- Offering specialist protective security advice and expertise.[424]

The NISCC provides a range of government and other organizations with access to resources, expertise, and knowledge. The NISCC either carries out research itself or sponsors work in a variety of fields connected with electronic attack and information security. It bases its threat assessments on a variety of sources, including sensitive intelligence, overseas security and intelligence partners, open-source material, and the reports of those who have experienced electronic attack.

The NISCC passes information, such as warnings of specific threats and vulnerabilities, to CI partners so that operators can install suitable defenses, and offers periodic assessments of the nature of the threat from electronic attack. NISCC information on vulnerabilities and alerts are disseminated through UNIRAS, the UK government CERT, a component of the NISCC.[425]

Other government departments and the NISCC

The following government departments contribute to the CIIP effort through the NISCC, in addition to their own wider departmental roles and responsibilities:

- The *Cabinet Office* contributes policy and coordination; its own units– the *Civil Contingencies Secretariat* (CCS) and the *Central Sponsor for Information Assurance* (CSIA) – work closely with the NISCC.

[424] http://www.gov.uk/cni/cniinfo.htm.

[425] http://www.niscc.gov.uk/cni/cniinfo.htm.

- The *Communications-Electronics Security Group* (CESG) is the information assurance arm of the *Government Communications Headquarters* (GCHQ), and is the national technical authority on information security. The CESG aims to protect the communications and information of central government departments, agencies, and other parts of the national information infrastructure by developing technical means of countering assessed threats. The CESG delivers information assurance policy and gives technical recommendations and authoritative advice on assessing current and foreseeable risks.[426]
- The *Department of Trade and Industry* (DTI) has several CIIP-related responsibilities, and assists the NISCC by promoting ISO-17799; having departmental responsibility for the energy and telecommunications sectors; and by encouraging information assurance for SMEs.
- The *Home Office* is the reporting line for the NISCC; chairs the NISCC Management Board; and its press office responds to press enquiries on the NISCC- or CIIP.
- The *Ministry of Defence* (MoD) contributes technical and research efforts; as part of the CNI, the MoD's own hierarchical set of CERTS work closely with UNIRAS. The *Defence Research Centre* (DSTL) carries out research into CIIP for both the MoD and the NISCC.
- *Police*: the crime prevention and attack investigation roles of police high tech crime units complement the CIIP effort of the NISCC. In particular, the *National High Tech Crime Unit* (NHTCU) is a close partner of the NISCC. The NISCC itself is not a criminal investigation or police authority; and where a CII incident requires a police response, the NHTCU would lead.
- The *Security Service* contributes expertise on threat investigation, intelligence, and protective security to the NISCC. Its CIIP contribution to the NISCC complements its physical counter-terrorist protective security role, as described above.

Central Sponsor for Information Assurance (CSIA)

The *Central Sponsor for Information Assurance* (CSIA) was officially formed as a unit within the UK Cabinet Office on 1 April 2003. CSIA promotes information assurance and information risk management across government as well as for industry and the public. The unit's responsibilities are:

[426] http://www.gchq.gov.uk/about/cesg.html.

- To provide a nationwide strategic direction for Information Assurance (IA);
- To co-ordinate and complement the activities of parties contributing to IA;
- To sponsor activities that benefit IA;
- To accredit pan-government systems and, in some cases such as the *Government Secure Intranet* (GSI), own the risk to shared information;
- To identify and address vulnerabilities in national telecommunications systems, and to resolve them in conjunction with other organizations such as the NISCC.

The Civil Contingencies Secretariat (CCS)

The *Civil Contingencies Secretariat* (CCS) is part of the Cabinet Office. It was established in July 2001, and reports to the prime minister through the S*ecurity and Intelligence Co-ordinator* and permanent secretary to the Cabinet Office. It was set up to improve the resilience of central government and the UK. Resilience is defined as the ability to handle disruptive challenges that can lead to or result in crisis. Disruptive challenges may arise from many causes – including, but not limited to, individual crises.

Like all Cabinet Office Secretariats, the CCS supports ministers collectively. Specifically, it services the *Civil Contingencies Committee*, which is chaired by the home secretary and deals with managing and exercising arrangements to handle individual crises as they arise. The CCS is organized around three divisions: An assessments division, which evaluates potential and evolving threats; an operations division, which develops and reviews departmental continuity and contingency plans; and a policy division, which gives the Cabinet Secretariat support in consequence management.

The aim of the CCS is to improve the UK's resilience to disruptive challenge through working with others inside and outside government on the anticipation, preparation, prevention, and resolution of threats. Its current objectives are:

- To identify and assess potential and imminent disruptive domestic challenges and assist in the development of an integrated response;
- To build partnerships with other organizations to develop and share best practices in horizon-scanning, and to develop the knowledge of the UK's critical networks and infrastructures;
- To ensure that the government can continue to function and deliver public services during crises, working with departments and other

secretariats in the Cabinet Office to ensure that plans and systems to cover the full range of potential disruption are in place and exercised;

- To improve resilience to disruption across government and the public sector, including supporting ministers in developing policy, agreeing priorities and planning assumptions, and ensuring that core response capabilities are developed accordingly;
- To improve the capability at all levels of government, the wider public sector, and the private and voluntary sectors to prepare for, respond to, and manage potential challenges through development of key skills and awareness.

The *Emergency Planning College* is an integral part of the CCS. It has a key role to play in the development and promulgation of the UK's resilience doctrine, and in the development of the cross-organizational communities to deliver it.

Public Private Partnerships

The NISCC's Public Private Partnerships

In addition to its assurance advice to specific CNI companies, the *National Infrastructure Security Co-ordination Centre* (NISCC) actively promotes two types of information-sharing initiatives.

The first type of initiative consists of *Information Exchanges*, where the NISCC facilitates and attends periodic confidential industry forums. Currently, representatives from over 50 private sector companies share information with each other and with the government under the initiative. There are currently three exchanges: telecommunications industry; finance, and those sectors that use process control or SCADA technologies. Sensitive information is shared in person at Exchange meetings, but is anonymized when passed to other Exchanges, or to a wider CIIP audience.[427]

Warning, Advice, and Reporting Points (WARPs) are an NISCC initiative designed to create and foster small, community-based, inter-linked information-sharing cells. They offer a cost-effective alternative to CERTs and ISACs. The first pilot WARP has been established for local authorities in London. A WARP 'toolbox' is being developed to make it easier to establish further WARPs. This will contain procedures, guidance, documentation,

[427] http://www.niscc.gov.uk/IAAC%20NISCC%20Sharing%20is%20Protecting%20v21.do, at p. 62.

and possibly software to operate the three core WARP services. The model is widely promoted beyond the CNI and has been adopted into other initiatives.[428]

Other Private-Public Partnerships

There is a wide range of private-sector bodies that work with the public sector to promote information assurance. Among these are:

The Information Assurance Advisory Council (IAAC), founded in 2000, is not part of the UK government, but has government representation. It fosters public private partnerships between corporate leaders, public policy makers, law enforcement, and the research community to address the challenges of information infrastructure protection. The IAAC makes policy recommendations to government and corporate leaders at the highest levels.[429] The IAAC facilitates cross-sectoral dialog, information exchange, and the emergence of new trusted long-term partnerships. The IAAC has active links with the NISCC, the Department of Trade and Industry (DTI), the Office of Science and Technology (OST), and the Office of the e-Envoy, as well as with the private sector and military communities. The IAAC has five working groups dealing with threat assessment, risk assessment, standards, research and development, and education and outreach.[430]

Other Public Private Partnerships include the *British Computer Society* (BCS),[431] the *Internet Security Forum*, the *National Computing Centre*[432], the *Internet Watch Foundation*,[433] and the *Confederation of British Industry*.[434] There is also an annual conference on 'Protecting Critical Information Infrastructures' that brings together private- and public-sector partners.[435]

[428] http://www.niscc.gov.uk/IAAC%20NISCC%20Sharing%20is%20Protecting%20v21.doc and http://www.niscc.gov.uk/warp_publications/WARPs.pdf, at p. 69.

[429] http://www.iaac.org.uk/start.htm.

[430] Parsons, T. J., Protecting Critical Information Infrastructures. The co-ordination and development of Cross-sectoral research in the UK. *Plenary Address at 'The Future of European Crisis Management*, Uppsala, Sweden (March 2001). http://www.krisestyring.dk/krisestyring/uppsala/uppsala.pdf.

[431] http://www1.bcs.org.uk.

[432] http://www.ncc.co.uk/index.cfm.

[433] http://www.iwf.org.uk/index.html.

[434] http://www.cbi.org.uk/home.html.

[435] http://www.hsaconferences.co.uk/pcii2001_info.htm.

Early Warning Approaches

Unified Incident Reporting and Alert Scheme (UNIRAS)

UNIRAS is the *UK Government Computer Emergency Response Team* (CERT) and is run by the *National Infrastructure Security Co-ordination Centre* (NISCC). It draws on technical support from the *Communications-Electronics Security Group* (CESG), the UK's national technical security authority. Its original customers were government departments and agencies, but in the last few years, this has been expanded to include companies holding sensitive government contracts, and most recently CNI organizations. UNIRAS has three main tasks:

- Response to electronic attack and other significant IT security incidents;
- Warning about IT security incidents and vulnerabilities; and
- Gathering information about IT security incidents.

UNIRAS provides ad-hoc advice on specific problems to individual members and warnings of IT security vulnerabilities by issuing 'Alerts' and 'Briefings'. These Alerts and Briefings are sent to the UNIRAS community by e-mail, but also posted on its website so that any company can make use of them.[436]

Ministry of Defence Computer Emergency Response Team (MODCERT)

The *UK Ministry of Defence* (MOD) is a member organization of both the international *Federation of Incident Response Security Teams* (FIRST)[437] and the *Trusted Introducer* (TI)[438] scheme, both of which provide a mechanism for sharing information on computer security incidents amongst communities of interest. MODCERT consists of a central co-ordination center and a number of monitoring and reporting centers, Warning, Advice, and Reporting Points (WARPs), and incident response teams. It also works closely with the government CERT, UNIRAS.[439]

[436] http://www.uniras.gov.uk.

[437] http://www.first.org.

[438] http://www.ti.terena.nl.

[439] http://www.mod.uk/cert.

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