



www.dds.org

National Dependability Policy Environments

United States of America

Report Version: Final
Report Preparation Date: 1 November 2002
Classification: Public
Preparation led by: RAND Europe (NL)

Contract Start Date: 1 June 2001 Duration: 18 months
Project Co-ordinator: RAND Europe (NL)

Partner: RAND Europe (NL, Project Coordinator); King's College London (UK);
Cell Network (S); IABG (D); Almaweb (I); LINK (P); ELIAMEP (GR);
Ernst Basler + Partner (CH), Isdefe (E)



IST-2000-29202

Project funded by the European Community
under the "Information Society Technology"
Programme (1998-2002)

Table of Contents

Overview of the Country’s Information Infrastructure 3

Main ICT Regulatory and Legal Developments 3

Assessment of Phenomena Undermining Dependability 6

Government Initiatives Aimed at Tackling Cyber-Security 6

Industry and Other Non-Governmental Activities Related to Dependability 10

Public-Private Partnerships 11

Research and Development 12

Overview of the Country's Information Infrastructure

As expected, the United States has been particularly proactive in its promotion of ICT and the protection of its complex infrastructures. ICT expenditure makes up 7.8 percent of the GDP, whilst the share of the ICT sector in total business enterprise expenditures on R&D is 22.1 percent.¹ 6.1 percent of the labour force, which comprises 7.4 million workers, work in the ICT industry.² 51. percent of US homes have personal computers, whilst 41.5 percent of US homes have Internet access.³ PC Internet presentation stands at 74 percent for US businesses.⁴ The number of secure web servers per million inhabitants is greater than 120 whilst the number of Internet hosts per 1000 inhabitants is 120.⁵ In 1998, there were 25.3 cellular mobile subscribers per 100 inhabitants. There were 69.97 fixed telephone lines per 100 inhabitants. The volume of B2B trade is estimated to hit US\$ 2.8 trillion by 2003⁶ (EUR 3.22 trillion), whilst current levels of B2C trade stand at US\$25.845 billion (EUR 28.6691 billion)⁷

The US economy is characterised by a pronounced focus on ICT expenditures and investments. The one sector where the US seems to under-perform with relation to its major trading partners is in the wireless penetration area, attached cellular telephony, and data networks. This situation may be partially due to the relatively dense nature of US terrestrial telephone networks, and to standards issues relating to the wireless architectures deployed by major US providers (i.e., TDMA vs. CDMA, and analogue formats, versus the GSM standard prevalent in Europe and elsewhere in the world).

ICT intensity is most prominent in the manufacturing sector, with smaller numbers visible in telecommunications and other services. As a rule, services are the recipients of efficiencies flowing from capital investments, rather than the other way around. This is particularly apparent in the ICT sector due to the 'trailing indicator' nature of business process changes enabled by technology investments. These changes are also highly qualitative in nature, making them difficult to detect in contemporary figures.

This issue is a highly controversial one, with economists only recently coming to terms with the mechanism through which ICT raises trend economic growth potential. The indicators provided focus on the increase in labour productivity as a consequence of efficiencies deriving from ICT investments.

Main ICT Regulatory and Legal Developments

The US has a strong tradition of private ownership of the telecommunications infrastructure. The regulatory approach adopted has favoured increasing competition among telecommunications providers,

¹ Information Society, OECD, *OECD Information Technology Outlook 2000*, 34.

² *Digital Economy 2000*, 43. These figures are for 1998.

³ Economics and Statistics Administration, National Telecommunications and Information Administration, US Department of Commerce, *Falling Through the Net: Toward Digital Inclusion*, (October 2000), 2.

⁴ Global One (quoting Gartner Group 2000), "Internet/IT Adoption (Business)", www.1globalplace.com/CountryResearch/CountryStatistics.asp?country=us

⁵ *OECD Information Technology Outlook 2000*, 79-80.

⁶ Estimates vary widely, due to differing definitions of what constituted B2B electronic commerce. Higher estimates tend to include EDI-Electronic Data Interchange-electronic data exchanges which facilitate supply-chain integration. See *Digital Economy 2000*, 15.

⁷ Figures are for 2000. Source: "Business to Consumer E-Commerce Statistics," a presentation at an OECD Workshop in Berlin (Germany), 13-14 March 2001 (webnet1.oecd.org/pdf/M00000000/M00000261.pdf)

especially following the break-up of AT&T in the 1980s. Since then, however, the regional bell operating companies (RBOCs) have each sought to compete in initially 'off-limits' areas in an attempt to leverage their technical investments against larger market opportunities. Constraints on RBOC mergers, market entry, and product offerings stemming from the original AT&T break-up are seen by many as the reason more competition failed to emerge in key telecommunications markets such as cable television networks, digital subscriber line (xDSL) technologies, and other fixed terrestrial networking areas. A number of issues arose out of the competitive environment created by the post-AT&T telecommunications system, most importantly that of unbundling – the separate pricing and provision of: long distance, local loop access, and data networks by providers. A significant amount of legislative, legal (court actions), and regulatory rule making has taken place in this domain, with many issues still in dispute.⁸

Recent bankruptcies in the broadband DSL and cable networking industry have weakened the environment for smaller firms, with larger competitors purchasing assets and customer-bases for low prices. Allegations of monopolistic behaviour by the RBOCs have thus far not resulted in significant regulatory action.⁹ The Bush Administration is still reviewing anti-trust and infrastructure policies in telecommunications, but in general is adopting a more free-market approach to structuring outcomes in the sector.

Regulatory and legal frameworks for telecommunications and information systems are currently under review. However, the federal agency in charge of regulating most telecommunications – the Federal Communications Commission (FCC) – has adopted a relatively 'hands-off' policy towards corporate mergers and acquisitions. This has allowed for an acceleration of the consolidation in long-distance telephony providers already evident during the 1990s. Furthermore, the increase in vertical concentration (linking content providers with network owner/operators) in telecommunications and information industries created new players such as AOL-Time Warner and Viacom. These entities are increasingly purchasing bankrupt, or nearly bankrupt, small broadband telecommunications providers, reducing competitive pressures in business-to-consumer broadband offerings. Industry segments in telecommunications, namely Internet service providers, local telephone system operators, and long-distance operators are each undergoing pronounced restructuring due to the shrinkage in consumer demand (or at least lower levels of growth). This slackening in business has resulted in a slow-down in new infrastructure investments and a consequently less aggressive rollout of new networking technologies. In short, a consolidation phase is under way in the telecommunications sector, underwritten by a market-oriented regulatory attitude from the federal government.¹⁰

A number of initiatives, both legislative and policy developments, have been undertaken to evaluate the value of information infrastructures to the US economy and society. As far back as 1996, the US Congress launched a 'Universal Service' Act designed to ensure the access to quality Internet services at affordable prices.¹¹ Other programmes launched by the federal government target particular schools, libraries, rural

⁸ For a summary of these issues, see Joseph Farrell and Michael Katz, "Public Policy and Private Investment in Telecommunications Infrastructure," *CRTP Working Paper #52*, August 1999: groups.haas.berkeley.edu/imio/crtp/publications/workingpapers/wp52.pdf

⁹ This regulatory action has provoked a resort to judicial oversight by some parties. See *Iowa Utilities Board v. FCC*, US Court of Appeals for the 8th Circuit: www.ca8.uscourts.gov/pndir/00/07/0963321P.pdf

¹⁰ FCC Report on Broadband Services: www.fcc.gov/Bureaus/Common_Carrier/news_Releases/2000/nrcc0040.html

¹¹ For details, see www.fcc.gov/ccb/universal_service

areas, and lower-income families. Internet access problems in each of these categories were investigated by a number of influential studies undertaken by both public and private agencies. Especially important in this area are a study of Internet access in public schools undertaken by the federal Department of Education and a demographic analysis of Internet access undertaken by the Department of Commerce.¹²

The Government Paperwork Elimination Act (GPEA), P.L. 105-277, Title XVII, allows citizens to use electronic technologies when filing information with, or retrieving it, from the Federal Government. The Act, signed into law in October 1998, directs Federal agencies to provide public access to government services and documents by 2003 and gives the public the option of submitting government forms electronically.¹³ By 21 October 2003, the GPEA requires Federal agencies to provide for options for electronic maintenance, submission, or disclosure of information, when practicable as a substitute for paper; and use and acceptance of electronic signatures, when practicable.

Alongside other legislative initiatives designed to provide legal frameworks for health insurance information shared over data networks, enhancement of Federal government paperwork reduction initiatives, and streamlining of health care financing data protection provisions, the Electronic Signature in Global and National Commerce Act established the legal force of electronic signatures in e-commerce. Taking effect in October 2001, this law establishes a legal basis for contracts undertaken through e-commerce mechanisms.

The Electronic Benefit Transfer Interoperability and Portability Act, enacted on 11 February 2000, amends the Food Stamp Act of 1977 to provide a national standard of interoperability and portability applicable to electronic food stamp benefit transactions. Section 508 of this law requires that all systems be accessible to persons with disabilities. The enforcement part of the law came into effect in the spring of 2001, requiring all IT products to be accessible to persons with deafness, blindness, and those with dexterity and mobility limitations (unless this caused a demonstrable undue burden to an agency).

The single most significant initiative in this area is the continuation of the current moratorium on imposing new taxes on goods and services purchased over the Internet.¹⁴ The major legislation in this area was the Internet Tax Moratorium Extension Act – H.R. 1552.¹⁵ Pending legislation in this area addresses issues from non-discrimination against revenue generated from on-line and off-line sources; the promotion of electronic commerce as a national priority; privacy concerns; protection of intellectual property; and the further expansion of e-government.¹⁶

¹² See [Internet Access in US Public Schools and Classrooms: 1994-2000](http://nces.ed.gov/pubs2001/2001071.pdf) (May 2001): nces.ed.gov/pubs2001/2001071.pdf; and [Falling Through the Net: Toward Digital Inclusion](http://www.ntia.doc.gov/ntiahome/fttn00/contents00.html) (October 2000): www.ntia.doc.gov/ntiahome/fttn00/contents00.html

¹³ [Government Paperwork Elimination Act 1999](http://egov.gov/documents/gpelaw.doc) (October 1998): egov.gov/documents/gpelaw.doc

¹⁴ In fact, goods and services sold over the Internet in the US *are* subject to normal sales taxes based on the locality of the purchaser. The problem is that vendors have no legal obligation to “collect and remit” these taxes to the consumers home jurisdiction if the vendor is in a separate legal jurisdiction. Much of the argument has stemmed from the difficulty of identifying the appropriate tax jurisdiction/venue for a particular transaction. Practicality has thus reinforced a separate policy debate about protecting an “infant industry” (electronic commerce) from onerous tax treatment.

¹⁵ See www.mbc.com/e-commerce/fedsummary.asp?federal=EnactedandPubID=20011031112821

¹⁶ See respectively, the [Internet Tax Nondiscrimination Act](http://www.mbc.com/e-commerce/fedsummary.asp?federal=PendingandPubID=2001111235953): www.mbc.com/e-commerce/fedsummary.asp?federal=PendingandPubID=2001111235953; the [Internet Growth and Development Act of 1999, H.R. 1685](http://www.mbc.com/ecmmerce/fedsummary.asp?federal=PendingandPubID=200111201019): www.mbc.com/ecmmerce/fedsummary.asp?federal=PendingandPubID=200111201019; the

Assessment of Phenomena Undermining Dependability

As with other countries, the US finds the amount of cyber-crime activity to be increasing. New viruses and worms, and distributed-denial-of-service (DDOS) attacks, cost millions of dollars in lost commerce, wages, and remedial activities.

Statistics kept at the System Administration, Networking, and Security (SANS) Institute (www.incidents.org) show that the US is the leading target of attacks over the Internet. Nationwide, the monitoring of Internet attacks is the job of the National Infrastructure Protection Center (NIPC). On 20 July 2001, Attorney-General John Ashcroft announced the formation of nine additional units in the Computer Hacking and Intellectual Property (CHIP) programme. This office is intended to work closely with the Federal Bureau of Investigation (FBI) and other agencies, to establish relationships between the high-tech community and law enforcement. The prosecutors assigned to this unit develop specialised expertise for dealing with cyber-crime and develop relationships that facilitate further case development.¹⁷

Between 1998 and 2000, a small number of criminal cases in cyber-crime and intellectual property offences were prosecuted. The number of investigative matters referred to US attorneys in this category did not vary significantly – changing from 192 cases referred in 1998 to 197 referrals in 2000. The number of defendants in these cases actually declined from 128 to 99.¹⁸ Sentences imposed after successful prosecutions predominantly recommended against imprisonment, or resulted in short terms of incarceration approximating one to 12 months.

No specific statistical information on trends in criminal exploitation of Internet technologies is readily available. Anecdotal accounts of identity theft, traditional fraud translated to the Internet, money laundering, and related crimes suggest that the e-commerce environment may present unique challenges to law enforcement investigators. These challenges are also likely to affect national security concerns relating to critical infrastructures and the Internet. Developing new models of detection, protection, and information sharing necessary for combating electronic variants of traditional crime is a crucial objective of the new Office of Homeland Security (OHS).

Although consumers periodically express distrust of the online environment for e-commerce, in fact commerce (both business-to-business and business-to-consumer) is increasing in cyber-space at reasonable rates. Trends favouring increased online use are expected to continue – subject to the inevitable influences of public confidence and broader societal and macroeconomic conditions.

Government Initiatives Aimed at Tackling Cyber-Security

Many of the current US government bureaucratic structures and office responsibilities and initiatives related to cyber-security stem from the 1997 report by the President's Commission on Critical

Uniformed Services Privacy Protection Act 2001: www.mbc.com/e-commerce/fedsummary.asp?federal=PendingandPubID=2001111412923; the Intellectual Property Protection Restoration Act 2001: www.mbc.com/e-commerce/fedsummary.asp?federal=PendingandPubID=2001111412323; and the E-Government Act 2001: www.mbc.com/e-commerce/fedsummary.asp?federal=PendingandPubID=2001523141445

¹⁷ See www.usdoj.gov/criminal/cyber-crime/ccpolicy.html.

¹⁸ Intellectual Property Cases – United States Attorney's Office, Fiscal Year 2000: www.usdoj.gov/criminal/cyber-crime/fy2000.htm

Infrastructure Protection (PCCIP).¹⁹ This document formed the basis for the Clinton Administration's inaugural critical infrastructure policy document, the Presidential Decision Directive (PDD) 63. This order mandated the creation of a national plan for information systems protection, encompassing national security objectives and domestic planning to protect critical infrastructures. This plan is to be prepared on an annual basis, with the first one having been issued in January 2000.

Although there are clear interconnections, the US federal government does not seem to have taken aboard the results of the Y2K experience. In February 1998, the President's Council on Year 2000 Conversion was established with the clear mandate of coordinating the overall Federal government Y2K issues. Its activities centred around the following three areas: ensuring that federal systems were ready for the data-change, coordinating Y2K efforts with interface partners and promoting Y2K problem among businesses and other governments. In order to achieve these objectives, the Council fostered information sharing by organising regular high-level round-tables, as well as creating a specific website and a toll-free information line. After the Y2K experience, the Council was dismantled and its experiences dispersed.

Following the events of 11 September 2001, US policy for the protection of the country's critical infrastructures has become more operationally oriented, focusing upon removing barriers to information-sharing and consequence-management by the entities charged with protecting critical infrastructures. Critical infrastructure protection analysts have long argued that a sophisticated opponent could use publicly-available information to attack computing and telecommunications systems vital to US economic and national security. These analyses have extended further, into conjectures on the shape and character of possible attacks, and on the increasing interdependence of different infrastructure systems.

The 11 September attacks seem to have validated these claims, and will have a definite long-term influence on policy development in CIP. Nonetheless, '9-11' as it has become known, is acting primarily as an catalyst of policy changes already in motion. Some of these changes are described below. The Bush Administration launched a thorough review of the PDD-63 CIP policy framework in March 2001. The results of this review appeared in October 2001 in the form of Executive Order 13231, Critical Infrastructure Protection in the Information Age, cited above. Key features of this new approach include co-operation with private sector critical infrastructure protection owners to implement national CIP objectives; protection of the critical networks and information resources under the control of the federal government; review and implementation of new national security programs to advance critical infrastructure protection.

The organisational structure for achieving these goals was also revised by this executive order. The new structure is defined by the creation of a new board – the President's *Critical Infrastructure Protection Board* (CIPB) – designed to co-ordinate federal government policy and programs in CIP. The responsibilities of the new board include recommending policies and co-ordinating programs for protecting information systems, for critical information systems, for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems.

A new special assistant to the President for Cyber-space Security chairs the CIPB. Richard Clarke is the first holder of this position. He reports to both the National Security Advisor (Condoleeza Rice) and the director of the Office of Homeland Security (OHS, Tom Ridge).

¹⁹ The report is available at www.info-sec.com/pccip/web/report_index.html (downloaded 4 December 2001)

The CIPB comprises the heads of major cabinet agencies (i.e., Secretaries of State, Defense, Treasury, and others), and the following additional members: Director of Central Intelligence (DCI), Director of the Office of Management and Budget, Director of the Office of Science and Technology Policy, the Chief of Staff of the President, the Chief of Staff of the Vice-President, the Chairman of the Joint Chiefs of Staff, and other senior officials as designated by the President.

The CIPB is also charged with preparing a national strategy for protecting critical infrastructures, and with making recommendations (co-ordinated with the Office of Homeland Security) to the Office of Management and Budget for department and agency programs to advance CIP objectives.

There are a number of institutions tasked by the US Government to tackle cyber-crime. The National Infrastructure Protection Center (NIPC) is housed within the FBI. It serves as a threat co-ordination centre focusing on threat warnings, vulnerabilities, and law enforcement. To date, NIPC has been criticised for an overemphasis on law enforcement activities (a traditional FBI role) to the detriment of early warning, vulnerability assessments, and the like. NIPC initiatives such as the Key Asset Program and Infraguard seek to identify critical infrastructures and important vulnerabilities in those systems for law enforcement (and national security) consequence management and planning.

The National Information Assurance Partnership (NIAP) is a collaboration between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). This programme fosters the development of objective measures and test methods for evaluating the quality of IT security products, and the development of commercial testing laboratories that can provide the types of evaluation services needed.

The NSA maintains that it is the national cryptologic organisation. It co-ordinates, directs, and performs highly specialised activities to protect US information systems and produce foreign intelligence information. A high technology organisation, the NSA is on the frontiers of communications and data processing. It is also one of the most important centres of foreign language analysis and research with the [US] Government. As the world becomes increasingly technology oriented, the Information Systems Security (INFOSEC) mission becomes increasingly challenging. This mission involves protecting all classified and sensitive information that is stored or sent through US Government equipment. INFOSEC professionals go to great lengths to make certain that Government systems remain impenetrable. This support spans from the highest levels of US Government to the individual war-fighter in the field. NSA conducts one of the US Government's leading research and development programs.²⁰

The NSA National Security Incident Response Center (NSIRC) supports other agencies in case of attacks on national security networks, performing real-time analysis and computer forensics, providing strategic warning regarding hacking and other activities by operating a central database with information on IT security problems. Generally, NSIRC also assists other agencies with technical INFOSEC information.

The US Government also supports dependability enhancement via the Federal Cyber Services, whereby a training initiative has been designed to exchange federal financial support for students of information assurance and computer security for a period of service in the federal government. The National Infrastructure Advisory Council (NIAC) is an advisory body made up of CEOs from private-sector critical infrastructures. NIAC advises the federal government on ways that information assurance policies and programs can best be integrated with private sector initiatives.

²⁰ www.nsa.gov/about_nsa/index.html (downloaded 4 December 2001)

The Federal Computer Incident Response Capability (FedCIRC) is a central co-ordination and analysis facility dealing with computer security-related issues affecting civilian agencies and departments of the federal government. Incident response and advisory activities use elements of the Department of Defense (DoD), law enforcement, the Intelligence Community, academia, and computer security specialists from federal civilian agencies and departments.

The Joint Task Force for Computer Network Operations (JTF-CNO) is located at the Defense Information Systems Agency (DISA). It reports to the US Space Command, which has overall responsibility for DoD information operations plans and policy (for defence, exploitation, and attack). The JTF-CNO runs an intrusion detection network for DoD and performs analysis on the outputs of that system.

The primary current activity of the US Government in addressing failures of critical information infrastructures falls within the general category of ‘counter-terrorism,’ after the events of 11 September. Responding to this event, in addition to the Executive Order 13231, a prior order established the Office of Homeland Security and the Homeland Security Council. Tom Ridge, the former governor of the state of Pennsylvania, is the first director of the Office, and is charged with co-ordinating government-wide efforts to increase preparedness against terrorist threats. In turn, the Office of Homeland Security is responsible for crafting a national strategy to counter terrorism, increase the effectiveness of US government detection efforts directed at terrorist threats, co-ordinating counter-terrorism planning with state and local governments, and a number of functional responsibilities connected with countering the activities of terrorist cells within the United States. As noted above, Richard Clarke reports to the director of Homeland Security – with a mandate to co-ordinate counter-terrorist planning against cyber-threats with those targeting more traditional physical terrorism challenges.

A number of legislative and executive policy changes will have significant impact on US CIP policymaking in the near future. These include the adoption of the USA PATRIOT (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) Anti-Terrorism Act, the opening for signature of the Council of Europe’s Cyber-crime Convention and an executive order establishing military tribunals for the prosecution of suspects involved in terrorist activities against the United States. Together, these legislative and administrative orders have transformed the law enforcement and intelligence community landscape for countering threats to critical infrastructures. Most pointedly, the new USA PATRIOT law associates acts normally considered criminal directly with terrorist activity. As such, most of the new law enforcement/intelligence community information sharing latitude that has been established will allow new investigative avenues to be explored in instances of critical infrastructure disruption.

At the same time, the penalties for cyber-terrorism – narrowly or broadly defined – now come fully into consistency with those available to pursue perpetrators of traditional terrorist acts. This last point is made evident in the USA PATRIOT law’s creation of a new definition of ‘federal interest computer’ for the purposes of establishing the jurisdiction of US law in a case of crime involving the Internet. While previously a computer had to be physically present in the United States (or controlled by a US-based entity or person) and involved in acts directly affecting US persons, the new definition allows for the assertion of US jurisdiction in cases where Internet traffic (IP packets) transit US servers. This potential expansion of jurisdictional claims seems partially consistent with the new Cyber-crime Convention, but at the same time opens up vast new areas of potential conflict with European and other authorities over extraterritorial clashes on sovereignty.

Industry and Other Non-Governmental Activities Related to Dependability

As indicated in the previous section, the central body for industry contacts with the US government on critical infrastructure protection policies and programmes is the National Infrastructure Advisory Council. This body is composed of up to 30 private sector CEOs. NIAC operations are run through a series of subcommittees (similar to the CIPB), which can have technical and policy-oriented mandates, as deemed necessary by the NIAC chair. Other private sector activities related to dependability are centred in industry and academic settings, with some private companies involved in marketing computer security products and services. This section lists some of these organisations and comments on convergences and conflicts of interest that affect private sector activities in CIP.

Academic and non-profit entities include CERT Co-ordination Center (CERTCC), operated by the Software Engineering Institute at Carnegie Mellon University, this is a centre of Internet security expertise. This organisation conducts academic studies of Internet security vulnerabilities, handles computer security incidents, issues public security alerts, and researches long-term changes in networked systems. CERTCC also develops education and training curriculum for information assurance improvement.

The SANS Institute is a co-operative research and education organisation through which more than 96,000 systems administrators, security professionals, and network administrators share the lessons they are learning and find solutions to the challenges they face. SANS was founded in 1989. It publishes newsletters, digests, research summaries, security alerts, and now offers a core curriculum for training security administrators – the General Information Assurance Certification. Funding from these activities is used to support ongoing research in information security.

The Software Engineering Institute (SEI) is a federally-funded research and development centre (FFRDC) operated for the US Government to provide leadership in software engineering technology and practice. Sponsors of SEI include the Office of the Secretary of Defense/Acquisition, Technology, and Logistics (OSD/AT&L); the Defense Advanced Research Projects Agency (DARPA); the Joint Program Office, and Carnegie Mellon University.

The Forum for Incident Response Teams (FIRST) is a coalition of government and private organisations bringing together a variety of computer security incident response capabilities. FIRST aims to foster co-operation and co-ordination in incident prevention, to prompt rapid reaction to incidents, and to promote information-sharing among members and the community at large. FIRST was founded in 1990, and currently has more than 100 members. FIRST provides a forum for the exchange of views and information on computer incident security response, holds technical colloquia on vulnerabilities, forensic investigative methods, and investigative tools and techniques, and sponsors conferences on information security for practitioners and policy professionals.

The Computer Security Institute (CSI) is a membership organisation specifically dedicated to serving and training the information, computer, and network security professional. Founded in 1974, CSI has been designing curricula on computer security and advice on protection of vital computing and networking infrastructures to both public- and private-sector institutions.

The Information Systems Security Association (ISSA) is a not-for-profit international organisation of information security professionals and practitioners that provides education fora, publications, and peer interaction opportunities aimed at enhancing the knowledge, skill, and professional growth of its members.

The International Association for Cryptologic Research (IACR) is a non-profit scientific organisation whose purpose is to further research in cryptology and related fields. The Information Technology Industry ISAC (IT-ISAC) is a not-for-profit corporation serving the information technology industry and established to report and exchange information concerning electronic incidents, threats, attacks, vulnerabilities, solutions, and countermeasures. The organisation collects, synthesises, and disseminates information about threats and co-ordinates the IT industry's response to such threats. There are currently 19 founding members of IT-ISAC. Membership is open to any IT company wishing to participate.

The Association for Computing Machinery (ACM) was founded in 1947 and is the world's first educational and scientific computing society. Today, ACM has over 80,000 members worldwide and organises academic conferences on computer science research, co-ordinates public policy discussions on computing and computer science topics, and publishes peer-reviewed journals on scientific topics.

The Institute of Electrical and Electronic Engineers (IEEE) is a non-profit, technical professional organisation with more than 350,000 individual members in 150 countries. IEEE is a leading authority in technical areas ranging from computer engineering, biomedical technology and telecommunications, to electric power, aerospace and consumer electronics, and other related areas.

These organisations are indicative of the nature and type of organisations involved in technical, policy-oriented work on dependability in the United States. Links between operational INFOSEC professionals and research in information security are provided by these organisations – either through curricula developed from real-world INFOSEC research, or through vulnerability-derived incidents that serve to catalyse private sector activities. The IT-ISAC is particularly significant because it was formed with the active encouragement of the US government following the promulgation of PDD 63 in 1998. As an industry-wide body involved in security issues, IT-ISAC is now an important private-sector partner to a government seeking to advance CIP/dependability initiatives.

Public-Private Partnerships

Public-private partnerships on dependability are driven by the realisation that the two sectors must work closely together in order to achieve a common goal – enhanced protection for critical information infrastructures. In the United States, the reasoning behind this collaboration is stark and obvious: the private sector owns or operates the infrastructures, and is almost completely deregulated; the federal government needs to ensure the functionality of critical infrastructures against both domestic and foreign threats. Short of a national emergency, government is unable to impose 'mandatory co-operation' on the private sector, hence the federal need to engender voluntary collaboration through co-ordinated and collective efforts.

PDD-63 created a policy framework for managing public private collaboration in CIP, arguing for the sector-specific creation of information-sharing and analysis centres (ISACs) designed to facilitate inter-industry, intra-industry, and public-private information-sharing on critical infrastructure problems. These entities have been somewhat slow to emerge due to overlapping problems of private sector distrust of government intervention, concerns over liability for infrastructure weaknesses, corporate distrust of commercial competitors, and antitrust concerns stemming from intra-industry co-ordination efforts.

Each of these concerns has been the subject of considerable legal, policy, analytical, and rhetorical activity. None of the concerns has entirely been overcome as a barrier to public-private action to improve dependability.

Research and Development

Research and development on CIP (dependability) is a co-ordinated activity in the US. The White House Office of Science and Technology Policy (OSTP) is charged under PDD-63 with co-ordinating federal government-wide CIP R&D activities. This task involves co-ordination of the CIP R&D programs of the designated lead and special responsibility agencies in CIP, and working with the Office of Management and Budget (OMB) to ensure that the President's CIP R&D strategy is implemented appropriately.

This basic model of federal activity in CIP R&D has been preserved during the Bush Administration, but with a refocused emphasis on the overlap between CIP and counter-terrorism. As such, longer-term research priorities have been reassessed in the light of the new homeland security mission.

The National Telecommunications and Information Administration (NTIA) is involved in the information and communications sector liaison mission, and is specifically tasked with the dissemination of the results of US government research and development actions in the area of CIP. The Department of Defense conducts its own network security information assurance programs and plans, and through the DARPA supports basic and applied research on networks, computer security, and information assurance.

In FY 2000, the US government spent approximately US\$451 million (EUR 518.4 million) on CIP R&D. These funds were spread across all agencies of the federal government – including the Department of Defense. This funding constituted 26 percent of all federal expenditures on CIP, and represents a commitment to enhance future capabilities while also funding current requirements at an increasing level.²¹ Priority areas for research include technology to support large-scale networks of intrusion detection monitors; artificial intelligence and other methods to identify malicious code (trap doors) in operating system code; methodologies to contain, stop, or eject intruders, and to mitigate damage or restore information-processing services in the event of an attack or disaster; technologies to increase network reliability, system survivability, and the robustness of critical infrastructure components and systems, as well as critical infrastructures themselves; and technologies to model infrastructure responses to attacks or failures; identify interdependencies and their implications; and locate key vulnerable nodes, components, or systems.²²

The Bush Administration has not articulated a set of substantive R&D objectives different to those presented above. Overall support for these programs is likely to increase, as a result of the enhanced salience of Homeland Security. What remains to be seen is the exact shape and character of the future R&D agenda, but its private-sector component may be the recipient of a more generous federal funding (or cross-subsidisation) orientation as a consequence of anticipated increases in the defence budget. Nevertheless, it is still possible to argue that basic, non-commercial dependability research will still mainly involve government-funded bodies, some of them are described in the following paragraphs.

The *Centre for High Assurance Computing Systems*, which is part of the National Research Laboratory network of the US Navy, conducts interdisciplinary research activities with the objective to devise techniques aimed at processing and communicating data while preserving critical system priorities. The *Defence Evaluation Research Programme Administrations (DARPA)* is funding the initiative *Composable High Assurance*

²¹ The National Plan for Information Systems Protection – Appendix B. Budget Trends: www.ciao.gov/CIAO-Documents_Library/national_plan_percent20_final.pdf (visited 21 December 2001).

²² US Government (The White House), Defending America's Cyberspace: The National Plan for Information Systems Protection version 1.0 – An Invitation to a Dialogue (2000): xxx1 - www.ciao.gov/publicaffairs/nplfinal.pdf.

Trusted Systems (CHATS). Its objectives are to devise technologies and services enabling core systems and network services to protect themselves from the insertion and execution of malicious code or attacks. This project is expected to fundamentally change the existing approach to the development and acquisition of high assurance trusted operating systems by fostering new security functionalities. Particular attention is also directed to open-source operating systems by devising long-term architectural framework for future trusted operating systems. The National Science Foundation is continuing its tradition of supporting advanced research projects in the field of information and network security and dependability overall through the *Trusted Computing* programme. Its goal is to devise a sound scientific and technological basis for managing privacy and security.

The US academic computer science community is increasingly interested in the areas of information security and dependability. In this context, particular focus should be directed to the activities of the *Computer Science Department* at the University of Virginia with its programme on survivable critical infrastructure systems. Similar initiatives are being carried out by the *High Dependability Computing Consortium* based at the Computer Science Department of Carnegie Mellon University. This consortium aims to provide sound, theoretical, scientific and technological basis for assurance constructions of safe and secure systems, as well as to reduce the effort and cost of assurance and quality certification processes. The consortium is also aiming at promoting software engineering education and services.