CIIP Country Surveys

United States

Concept of CIIP and Description of System

CIP in the US is about the protection of infrastructure critical to the people, economy, essential government services, and national security. The main goal of the US government's efforts is to ensure that any disruption of the services provided by this infrastructure is infrequent, of minimal duration, and manageable.[1] In the US, the following are defined as the critical sectors:

- Banking and finance,
- Energy,
- Information and communications,
- Transport,
- Vital Human Services.[2]

The five sectors are highly interdependent, both physically and in their greater reliance on CII.

CIIP Initiatives and Policy

CIIP Initiatives

There have been several efforts since the 1990s to better manage CIIP in the US.

Presidential Commission on Critical Infrastructure Protection (PCCIP)

Based on the recommendations of the Critical Infrastructure Working Group (CWIG), which was appointed as a reaction to the Oklahoma City bombing, President Bill Clinton set up the Presidential Commission on Critical Infrastructure Protection (PCCIP) in 1996,[3] the first national

1 Moteff, John D. *CRS (Congressional Research Service) Report for Congress. Critical Infrastructures: Background, Policy, and Implementation.* (Updated February 4, 2002). http://www.fas.org/irp/crs/RL30153.pdf.

2 Including emergency services, government services, and water supply systems.

3 http://www.ciao.gov/PCCIP, and http://www.ciao.gov/PCCIP/eo13010.pdf.

effort to address the vulnerabilities of the information age. Its tasks were to

- Report to the president on the scope and nature of vulnerabilities and threats to the nation's CI, focusing primarily on cyber-threats,
- Recommend a comprehensive national CIP plan,
- Determine legal and policy issues raised by proposals to increase protections,
- Propose statutory and regulatory changes necessary to effect recommendations.[4]

The PCCIP included representatives from all relevant government departments as well as from the private sector. The PCCIP presented its report to the president in October 1997.[5] The commission's most urgent recommendation was that greater cooperation and communication was required between the private sector and the government.

Presidential Decision Directives (PDD) 62 and 63

Clinton followed the recommendations of the PCCIP in May 1998 with his Presidential Decision Directives (PDD) 62 and 63.[6] They established policy-making and oversight bodies making use of existing agency authorities and expertise, and addressed operational concerns. PDD 63 set up groups within the federal government to develop and implement plans to protect government-operated infrastructure, and called for a dialog between the government and the private sector to develop a National Infrastructure Assurance Plan.[7]

CIIP Policy

National Plan for Information Systems Protection

On 7 January 2000, Clinton presented the first comprehensive national master plan for CIP as "Defending America's Cyberspace. National Plan

4 The President's Commission on Critical Infrastructure Protection (PCCIP). *Critical Foundations: Protecting America's Infrastructures.* (Washington, D.C., October 1997).

5 President's Commission on Critical Infrastructure Protection, Critical Foundations.

6 http://www.fas.org/irp/offdocs/pdd-62.htm, Clinton, William J. *Protecting America's Critical Infrastructures: Presidential Decision Directive 63.* (May, 22 1998). http://www.fas.org/irp/offdocs/pdd-63.htm.

7 Clinton, Presidential Decision Directive 63.

for Information Systems Protection, Version 1.0".[8] This plan reinforced the perception of cyber-security as a responsibility shared between the government and the private sector.[9] Version 2.0, due out in fall 2002, will be a comprehensive document that examines CIP at the level of federal, state, and local government, as well as the private sector.[10]

Homeland Security

In the aftermath of 11 September 2001, President George Bush signed two Executive Orders (EO) affecting CIP. EO 13228, signed 8 October 2001, established the Office of Homeland Security, headed by the Assistant to the President for Homeland Security.[11] One of its functions is the coordination of efforts to protect the US and its CI from terrorist attacks. The EO further established the Homeland Security Council, which advises and assists the president in all aspects of homeland security.

The second Executive Order (EO 13231), signed 16 October 2001 established the President's Critical Infrastructure Protection Board. The board's responsibility is to "recommend policies and coordinate programs for protecting information systems for critical infrastructure"[12]. Finally, the EO also established the National Infrastructure Advisory Council (NIAC). Its task is to provide advice to the president on the security of information systems. The council's functions include enhancing public-private partnerships, monitoring the development of so-called Information Sharing and Analysis Centers (ISACs), and encouraging the private sector to conduct periodic vulnerability assessments of CII systems.[13]

Information Analysis and Infrastructure Protection

In a recent development since June 2002, one of the four divisions of the planned Department of Homeland Security has been dedicated to "Infor-

8 Clinton, William J. *Defending America's Cyberspace: National Plan for Information Systems Protection. An Invitation to a Dialogue.* Version 1.0 (The White House: Washington, D.C., 2000).

9 Three new institutions work together for the security of the state's computer systems.

10 http://www.ciao.gov and interview with a representative of the US Chamber of Commerce, June 2002.

11 Bush, George W. *Executive Order 13228. Establishing the Office of Homeland Security and the Homeland Security Council.* (Washington, D.C., 8 October 2001). http://www.fas.org/irp/offdocs/eo/eo-13228.htm.

12 Bush, George W. *Executive Order 13231. Critical Infrastructure Protection in the Information Age* (Washington, D.C., 16 October 2001). http://www.ncs.gov/ncs/html/eo-13231.htm.

mation Analysis and Infrastructure Protection". It plans to merge the capability to identify and assess current and future threats to the homeland, map those threats against current vulnerabilities, inform the president, issue timely warnings, and immediately take or effect appropriate preventive and protective action. It would coordinate a national effort to secure the entire CI of the US.[14]

Law and Legislative Action

Defense Production Act of 1950

This act is aimed at management of consequences, rather than prevention, which is associated with the more modern approach to risk management that is necessary for CIP.[15]

Computer Fraud and Abuse Act (CFAA) of 1986

Legislative awareness of computer crimes grew dramatically in the early 1980s, as computers became increasingly important for the conduct of business and politics. The CFAA was the conclusion of several years of research and discussion among legislators.[16] It established two new felony offenses consisting of unauthorized access to "federal interest" computers[17] and unauthorized trafficking in computer passwords. Violations of the CFAA include intrusions into government, financial, most medical, and "federal interest" computers.

Computer Abuse Amendments Act of 1994

This act expanded the 1986 CFAA to address the transmission of viruses and other harmful code.[18] The measures provided by this act were further tightened on 26 October 2001 by the USA PATRIOT anti-terrorism legisla-

13 Bush, Executive Order 13231.
14 http://www.whitehouse.gov/deptofhomeland/sect6.html.
15 President's Commission on Critical Infrastructure Protection, Critical Foundations.
16 http://www4.law.cornell.edu/uscode/18/1001.html.
17 Federal interest computers are defined as two or more computers involved in a criminal offense, if they are located in different states.
18 See also http://www.digitalcentury.com/encyclo/update/comfraud.html Jones Telecommunications and Multimedia Encyclopedia.

tion.[19] Violations of the CFAA are investigated by the National Computer Crimes Squad at the FBI and supported by its Computer Analysis and Response Team (CART), a specialized unit for computer forensics.[20]

Much of the federal legislation concerning CI/CII was written before the emergence of "cyber-threats". Thus, it is questionable whether a timely and efficient response would be possible under the existing legal frameworks at both federal and state/local levels.[21]

Organizational Analysis

Public Agencies

The attacks of 11 September 2001 have given the crucial impulse to change the overall CIIP organizational structure in the US. The most important change will be the establishment of the Department of Homeland Security. It will incorporate 22 existing federal agencies. The department will be divided into four divisions: (1) Border and Transportation Security, (2) Emergency Preparedness and Response, (3) Chemical, Biological Radiological, and Nuclear Countermeasures, and (4) Information Sharing and Analysis Centers. In addition to consolidating the existing functions of various federal agencies and departments, the new department will also create a single "all hazards" emergency response plan and a center to collect, review, and analyze intelligence information submitted by the FBI, the CIA, the NSA, and other intelligence services.[22]

Since the final outcome of this change is not yet entirely clear, the next section includes a selection of public actors that play an important role in CIIP today. Under the Bush plan, the Critical Infrastructure Assurance

19 USA PATRIOT stands for: *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism*. For full text version see http://www.cdt.org/security/usapatriot/011026usa-patriot.pdf. Privacy and civil liberty advocacy groups have expressed concern over a number of legislative developments.

20 http://www.fbi.gov/hq/lab/org/cart.htm. Of further importance is also the recent enactment of the Gramm-Leach-Bliley (GLB) Act and the regulations that implement GLB, which address privacy concerns by setting forth a range of requirements to protect customer information. For text of GLB see http://www.ftc.gov/privacy/glbact.

21 President's Commission on Critical Infrastructure Protection, Critical Foundations, 81.

22 Interview with a representative of the US Chamber of Commerce, June 2002.

Office (CIAO) and the National Infrastructure Protection Center (NIPC) will be moved into the Department of Homeland Security. These agencies will maintain their current functions but move their entire operations to the new Department of Homeland Security.

Critical Infrastructure Assurance Office (CIAO)[23]

The Critical Infrastructure Assurance Office (CIAO)[24] was created in May 1998 in response to the Presidential Decision Directive (PDD-63) to coordinate the federal government's initiatives on CIP. The CIAO's main tasks are to

- Coordinate and implement the national strategy,
- Assess the government's own risk exposure and dependencies on CI,
- Raise awareness and public understanding and participation in CIP efforts, and
- Coordinate legislative and public affairs to integrate infrastructure assurance objectives into the public and private sectors.

Federal Computer Incident Response Center (FedCIRC)[25]

The Federal Computer Incident Response Center (FedCIRC) is the central coordination and analysis facility dealing with computer security issues affecting the civilian agencies and departments of the federal government. The FedCIRC's incident response and advisory activities bring together elements of the Department of Defense, law enforcement agencies, the intelligence community, academia, and computer security specialists from federal civilian agencies and departments.[26]

National Infrastructure Protection Center (NIPC)[27]

In 1998, the Office of Computer Investigations and Infrastructure Protection (OCIIP) was expanded to become the inter-agency National Infrastructure Protection Center (NIPC). The NIPC is located at the FBI headquarters. Its mission is to serve as the US government's focal point for threat assessment, warning, investigation, and response for threats or attacks against CI. It facilitates and coordinates the federal government's response to incidents, mitigating attacks, investigating threats, and moni-

23 http://www.ciao.gov.
24 It is currently part of the Department of Commerce.
25 http://www.fedcirc.gov.
26 http://www.fedcirc.gov.
27 http://www.nipc.gov.

toring reconstitution efforts. It is linked electronically to the rest of the federal government, including other warning and operation centers. In addition, private-sector Information Sharing and Analysis Centers (ISAC) have informal relationships with the NIPC. Also, the NIPC offers private sector firms from across all industries a program called INFRAGARD.

Office of Homeland Security

The Office of Homeland Security was established by Executive Order 13228 in October 2001. It is headed by the Assistant to the President for Homeland Security. Its mission is to "develop and coordinate the implementation of a comprehensive national strategy to secure the US from terrorist threats and attacks". Among its functions is the coordination of efforts to ensure rapid restoration of CI after a disruption by a terrorist threat or attack.[28] The Office of Homeland Security will remain an entity of its own within the Executive Office, as the administration sees the need for it to continue coordination among federal agencies.[29]

President's Critical Infrastructure Protection Board

The Board was established by Executive Order 13231 in October 2001. Its responsibility is to recommend policies and to coordinate programs for protecting information systems for CI.[30] The Board is directed to propose a National Plan, and, in coordination with the Office of Homeland Security, to review and make recommendations on that part of agency budgets that fall within the purview of the Board. The Board is to be chaired by a Special Advisor to the President for Cyberspace Security. The special advisor may, in consultation with the Board, propose policies and programs to appropriate officials to ensure the protection of the nation's CII.

The Department of Homeland Security[31]

The new department will concentrate all efforts in a single government agency, responsible for coordinating a comprehensive national plan for protecting the US infrastructure. An especially high priority will be placed on protecting the infrastructure of cyberspace from terrorist attacks by unifying and focusing the key cyber-security activities of the CIAO and the NIPC. The department will augment those capabilities with

28 Bush, Executive Order 13228.
29 Interview with a representative of the US Chamber of Commerce, June 2002.
30 Bush, Executive Order 13231.
31 http://www.whitehouse.gov/deptofhomeland.

the response functions of the Federal Computer Incident Response Center. Because information and telecommunications sectors are increasingly interconnected, the department will also assume the functions and assets of the National Communications System (Department of Defense), which coordinates emergency preparedness for the telecommunications sector.[32]

Cooperation of Public and Private Sectors

The government has very actively sought cooperation between the public and private sectors. As the federal government alone cannot protect CI, the goal is a close private-public partnership.[33] One of the new Department of Homeland Security's main tasks will be to facilitate partnership efforts between the government and private sectors. It will give state, local, and private entities one primary contact point. So far, unresolved legal issues – such as the Freedom of Information Act, as well as antitrust and liability issues – impede the comprehensive sharing of information between the public and private sectors. According to experts, resolving these issues should enhance information-sharing and spur the growth of ISACs.[34]

Information Sharing and Analysis Center (ISAC)

While the PDD 63 envisioned a single center serving the entire private sector, namely the NIPC, each sector is now establishing its own Information Sharing and Analysis Center (ISAC). Private sector ISACs are membership organizations managed by private companies. Each ISAC has a board of directors that determines its institutional and working procedures. The function of an ISAC is to collect and share incident and response information among ISAC members, and to facilitate information exchange between the government and the private sector. The following list gives an overview of important existing ISACs:

- A number of the nation's largest banks, securities firms, insurance companies, and investment companies have joined together in a limited liability corporation to form a Financial Services Information Sharing and Analysis Center (FS/ISAC),[35]

32 http://www.whitehouse.gov/deptofhomeland/sect6.html.
33 President's Commission on Critical Infrastructure Protection, Critical Foundations, 104.
34 Interview with a representative of the US Chamber of Commerce, June 2002.
35 http://www.fsisac.com.

- The telecommunications industry has agreed to establish an ISAC through the National Coordinating Center (NCC). Each member firm of the NCC monitors and analyzes its own networks. Incidents are discussed within the NCCs and members decide whether the suspected behavior is serious enough to report to the appropriate federal authorities,[36]
- The electric power sector has established a decentralized ISAC through its North American Electricity Reliability Council (NERC). Much like the NCC, the NERC already monitors and coordinates responses to disruptions in the nation's supply of electricity,[37]
- The IT ISAC started operations in March 2001. Members include 19 major hardware, software, and e-commerce firms, including AT&T, IBM, Cisco, Microsoft, Intel, and Oracle. The ISAC is overseen by a board made up of members and operated by Internet Security Systems,[38]
- New ISACs include the Surface Transportation ISAC [39] and an Oil and Gas ISAC.[40]

National Cyber Security Alliance (NCSA)

The NCSA fosters awareness of cyber-security through educational outreach. It tries to raise citizens' awareness of the critical role computer security plays in protecting the nation's Internet infrastructure, and to encourage computer users to protect their home and small business systems.[41]

Partnership for Critical Infrastructure Security (PCIS)

The PCIS grew out of initiatives outlined in Presidential Decision Directive-63. It works to secure CI and examines cross-sector issues.[42]

There are some additional efforts in public-private partnerships. For example, the San-Francisco-based Computer Security Institute has been working together with the FBI's Computer Intrusion Squad on conduct-

36 http://www.ncs.gov/ncc.
37 http://www.nerc.com; Energy Information Sharing and Analysis Center, http://www.energyisac.com.
38 https://www.it-isac.org.
39 http://www.surfacetransportationisac.org.
40 http://www.energyisac.com.
41 http://www.staysafeonline.info.
42 http://www.pcis.org.

ing an annual Computer Crime and Security Survey, a widely recognized study of dangers, cases, and countermeasures in IT security.

Early Warning

Federal Bureau of Investigation (FBI)

The 1997 PCCIP Report stated that efforts were required to establish a system of surveillance, assessment, early warning, and response mechanisms.[43] The Clinton administration envisaged an enormous database of every hacking or computer-hijacking incident. By 2003, they hoped to have created a constantly updated tool to forecast, identify, and combat cyber attacks that would be developed and maintained in close cooperation between the private and the public sector. The Federal Bureau of Investigation (FBI) was chosen to serve as the preliminary national warning center for infrastructure attacks and to provide law enforcement, intelligence, and other information needed to ensure the highest quality possible. PDD 63 assigned responsibility for developing analytical capabilities to provide comprehensive information on changes in threat conditions and newly identified system vulnerabilities, as well as timely warnings of potential and actual attacks, to the NIPC at the FBI.[44]

Federal Computer Incident Response Center (FedCIRC)

The responsibility for detecting and responding to cyber-attacks while they are in progress lies with the Federal Computer Incident Response Center (FedCIRC), which gives agencies the tools to detect and respond to such attacks, and coordinates response and detection information.

The Information Sharing and Analysis Centers (ISACs)

The Information Sharing and Analysis Centers (ISACs) were planned to help create the early warning database. The idea is that owners and operators will survey incidents and pass the information on to the NIPC, which serves as the private sector point of contact for information-sharing and coordinates and bundles reports from all different ISACs.

43 President's Commission on Critical Infrastructure Protection, Critical Foundations.
44 Clinton, Presidential Decision Directive 63.

Department of Homeland Security

The planned Department of Homeland Security will have a division focusing on information analysis and infrastructure protection. Set up with a special focus on systematically analyzing all information and intelligence on potential terrorist threats within the US, this division will fuse and analyze legally accessible information from multiple sources to provide early warning of terrorist attacks.[45]

Research and Development

CIIP research and development (R&D) efforts in the US focus on issues such as interdependency analyses, threat, vulnerability and risk assessment studies, system protection and information assurance, reconstitution of damaged or compromised systems, the security of automated infrastructure control systems; and intrusion detection and monitoring.[46] Generally, the private sector funds R&D to develop tools to address infrastructure outages, but the federal government does more fundamental R&D. The Department of Defense, which provides the bulk of information security R&D funding because of its mission needs, is sponsoring research at universities in its University Research Initiatives Centers of Excellence program.[47]

Investigation of the need for and solutions to CIIP R&D since the publication of Version 1.0 of the *National Plan for Information System Protection* is conducted under the auspices of the CIP R&D Inter-Agency Working Group (IWG), which includes a number of subgroups. The information and communications (I&C) sector subgroup deals with CII; it was established to further the development and exchange of information between the federal government and private sector regarding I&C CIP R&D programs.[48]

After 11 September 2001, the Bush administration took steps to develop a capability to coordinate cyber-security activities with the nation's

45 http://www.whitehouse.gov/deptofhomeland/sect6.html.

46 http://www.ciao.gov/CIAO_Document_Library/Report_on_Federal_CIP_R&D.pdf.

47 Kneso, Genevieve J., *CRS (Congressional Research Service) Report for Congress. Federal Research and Development for Counter Terrorism: Organization, Funding and Options.* (November 2001). http://www.ieeeusa.org/forum/PAPERS/CRSterrorismresearch.pdf.

48 http://www.ciao.gov/CIAO_Document_Library/2001Cong/05-CIP_RD.pdf.

counter-terrorism effort and to better link information security R&D to these efforts. The mechanism established parallels with the organization created by the Clinton administration. However, it differs in important ways and, potentially, has more authority, because it is closely linked to both the anti-terrorism effort and to the Office of Science and Technology Policy (OSTP), and has specific authority to work with agencies to develop priority R&D programs and budgets.[49] One of the tasks of the interagency President's Critical Infrastructure Board was to coordinate with the director of the OSTP to develop a federal R&D program to protect information systems for critical infrastructure.

49 For more information see Kneso, Federal Research and Development for Counter Terrorism.