CIIP Country Survey

United States

The Country Survey of the United States 2004 was written with the help of John A. McCarthy and Emily Frye, Critical Infrastructure Protection Project, George Mason University School of Law, Arlington, and Scott C. Algeier, US Chamber of Commerce, Washington.

United States

Critical Sectors

Critical Infrastructure Protection (CIP) in the United States 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.[440]

In the US, critical infrastructures are defined[441] according to the *USA Patriot Act* of 2001, section 1016(e): "[…] the term 'critical infrastructure' means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[442]

In the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*[443] and in the *National Strategy to Secure Cyberspace*[444], both from February 2003, the following critical infrastructure sectors are identified:

- Agriculture and Food,
- Banking and Finance,
- Chemicals and Hazardous Materials,
- Defense Industrial Base,
- Emergency Services,
- Energy,

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

[441] In the Homeland Security Presidential Directive/HSPD-7, 17 December 2003 (see below). http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html.

[442] http://www.epic.org/privacy/terrorism/hr3162.html ("Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" is the full title of the USA PATRIOT Act of 26 October 2001).

[443] The White House. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (Washington, February 2003). http://www.dhs.gov/interweb/assetlibrary/Physical_Strategy.pdf.

[444] The White House. *The National Strategy to Secure Cyberspace* (Washington, February 2003). http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf.

- Higher Education,
- Insurance,
- Law Enforcement,
- Oil and Gas,
- Postal and Shipping,
- Public Health,
- Telecommunications and Information Technology,
- Transportation,
- Water.

Moreover, the following key assets are identified for major protection initiatives:

- Commercial Key Assets,
- Dams,
- Government Facilities,
- National Monuments and Icons,
- Nuclear Power Plants.[445]

Varying definitions of the critical infrastructure sectors are in use, and this listing is not a static list. As different sectors become more important, or more crucial to maintaining basic operations, different sectors will be included (or perhaps excluded) from this list.

The protection of all of these infrastructure sectors is related to cyberspace at a fundamental level because of their reliance on interconnected computers, servers, routers, switches, and fiber-optic cables that ensure their functionality.

Initiatives and Policy

There have been several efforts since the 1990s to better manage Critical Infrastructure Protection and Critical Information Infrastructure Protection (CIIP) in the US. CIIP plays an important role in the overall US security strategy. The US government views CIIP as an element of its homeland security strategy. Where traditionally, national security has been recognized as the responsibility of the federal government and is underpinned by the collective efforts of the military, the foreign policy establishment, and the

[445] The National Strategy for Physical Protection of Critical Infrastructures and Key Assets. http://www.dhs.gov/interweb/assetlibrary/Physical_Strategy.pdf.

intelligence community with respect to defense, homeland security is viewed as a shared responsibility that requires coordinated action across many sectors.[446]

The US government is especially committed to CIIP, as evidenced by President George Bush signing a US$ 37.4 billion Homeland Security appropriations bill for 2004. US$ 839.3 million was allocated specifically to the *Information Analysis and Infrastructure Protection Directorate*, which has responsibility for cybersecurity. Among other things, this money will fund research and development in examining network weaknesses and evaluating threats and vulnerabilities.

The following government efforts are aimed at developing initiatives and creating appropriate policies to address CIIP.

Presidential Commission on Critical Infrastructure Protection (PCCIP)

Based on the recommendations of the *Critical Infrastructure Working Group* (CWIG), President Bill Clinton set up the *Presidential Commission on Critical Infrastructure Protection* (PCCIP) in 1996, the first national effort to address the vulnerabilities of the information age.

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.[447] The commission's most important decision was to foster cooperation and communication between the private sector and the government.

Presidential Decision Directives (PDD) 62 and 63

Clinton followed the recommendations of the PCCIP in May 1998 and issued *Presidential Decision Directives* (PDD) 62 and 63.[448] They established policy-making and oversight bodies making use of existing agency authorities and expertise. 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*.[449]

[446] Ibid.

[447] President's Commission on Critical Infrastructure Protection, Critical Foundations.

[448] Clinton, William J. *Protecting America's Critical Infrastructures: Presidential Decision Directive 63.*

[449] Clinton, Presidential Decision Directive 63.

Homeland Security Presidential Directive/HSPD-7

On 17 December 2003, President Bush released a new *Homeland Security Presidential Directive/HSPD-7,* which supersedes PDD 63 of May 1998, and any Presidential directives issued prior to this HSPD-7.

This new directive establishes a national policy for federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and protect them from terrorist attack. Basically, it identifies which government agencies are responsible for protecting specific infrastructure sectors. A key element of this directive is the requirement that *Sector-Specific Agencies* will collaborate with appropriate private sector entities.

Also, the HSPD-7 says that by July 2004, the heads of all Federal departments and agencies shall develop plans for protecting the physical and cyber critical infrastructure and key resources that they own or operate, including identification, prioritization, protection, and contingency planning. On an annual basis, the Sector-Specific Agencies shall report to the Secretary on their efforts.[450]

The *Secretary of Homeland Security* will serve as the "the principal Federal official to lead, integrate, and coordinate implementation of efforts among Federal departments and agencies, State and local governments, and the private sector to protect critical infrastructure and key resources."

National Plan for Information Systems Protection

On 7 January 2000, Clinton presented the first comprehensive national masterplan for CIP as "*Defending America's Cyberspace. National Plan for Information Systems Protection – An Invitation to Dialogue Version 1.0*".[451] This plan reinforced the perception of cyber-security as a responsibility shared between the government and the private sector.[452]

[450] http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html.

[451] Clinton, William J. *Defending America's Cyberspace: National Plan for Information Systems Protection. An Invitation to a Dialogue.* Version 1.0 (Washington, 2000).

[452] http://www.ciao.gov/resource/np1final.pdf.

Homeland Security Executive Decisions

In the aftermath of 11 September 2001, President George Bush signed two *Executive Orders* (EO) affecting CIP. With EO 13228, entitled "*Establishing the Office of Homeland Security and the Homeland Security Council*" and issued on 8 October 2001, the *Office of Homeland Security* was established, headed by the Assistant to the President for Homeland Security.[453] One of its functions is the coordination of efforts to protect the country 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 "*Critical Infrastructure Protection in the Information Age*" 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".[454] Finally, the EO also established the *National Infrastructure Advisory Council* (NIAC).[455]

National Strategies

On 14 February 2003, the White House released two presidential national strategies that are follow-on documents to the *National Strategy for Homeland Security*, which was released in July 2002.

- The main aim of the *National Strategy to Secure Cyberspace* is to engage US citizens in securing the portions of cyberspace they own, operate, control, or with which they interact.
- The main aim of the *National Strategy for Physical Protection of Critical Infrastructure and Key Assets* is to reduce the nation's vulnerability to acts of terrorism by protecting the national critical infrastructure and key assets from physical attack.

The fact that the US government has further defined and elaborated on the *National Strategy for Homeland Security* in two separate documents highlights an important distinction between critical information infrastructure

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

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

[455] Bush, Executive Order 13231.

protection and critical infrastructure protection. However, several sectors have been identified as crucial to both types of vulnerable infrastructure.

The National Strategy to Secure Cyberspace

The *National Strategy to Secure Cyberspace* (NSSC)[456] recognizes that securing cyberspace is an extraordinary challenge that requires a coordinated effort from the entire society and government. In order to achieve this goal and to engage the public in securing cyberspace, a draft version of the NSSC has been released for public comment, and ten town hall meetings were held around the US to gather input on the development of a national strategy. This careful vetting process is a clear sign that cyberspace security is viewed as a public private partnership.

The NSSC defines cyberspace as an "interdependent network of information technology infrastructures," and depicts cyberspace as the nervous system or control system of society. The NSSC outlines an initial framework for both organizing and prioritizing national efforts in combating cyber-attacks committed by terrorists, criminals, or nation states, while highlighting the role of public private engagement.

Consistent with the National Strategy for Homeland Security, the strategic objectives of the NSSC are:

- To prevent cyber-attacks against the national CI;
- To reduce the national vulnerability to cyber-attack;
- To minimize damage and recovery time from cyber-attacks.

The strategy recognizes that the private sector is best equipped and structured to respond to cyber-threats. Therefore, public private engagement will take a variety of forms and will address awareness, training, technological improvements, vulnerability remediation, and recovery operations.

The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets

The *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* states that the CI sectors of the US provide the foundation for national security, governance, economic vitality, and the American way of life. An attack on the nation's critical infrastructures and key assets could not only result in large-scale human casualties and property destruction, but also damage the national prestige, morale, and confidence, as experi-

[456] Own shorthand expression.

enced in the 11 September 2001 attacks. As a result, the following strategic objectives are considered:

- To identify and assure the protection of those infrastructures and assets that are deemed most critical in terms of national-level consequences for public health and safety, governance, economic and national security, and public confidence;
- To provide timely warning;
- To assure the protection of other infrastructures and assets that may become terrorist targets over time.

By pursuing these objectives, coordinated action is required on the part of federal, state, and local governments, as well as the private sector and concerned citizens. The *Department of Homeland Security* (DHS) (see below) will provide overall cross-sector coordination in this new organizational scheme, acting as the primary liaison and facilitator for cooperation among federal agencies, state and local government, and the private sector. Cross-sector initiatives should be fostered in the areas of planning and resource allocation, in information-sharing, in personnel security (including background checks where appropriate) and awareness, in research and development, and in modeling, simulation, and analysis.[457]

Procedures for Handling Critical Infrastructure Information

In April of 2003, the DHS released regulations for handling critical infrastructure information.[458] These regulations, which were authorized in the Homeland Security Act of 2002, provide rules for the receipt, care, and storage of Critical Infrastructure Information, the maintenance of security and confidentiality, and methods for dealing with proprietary or business-sensitive information. The basic concept of the regulations again underscores the fundamental principles of public private partnership. It stipulates that business-sensitive information that businesses voluntarily submit to the *Department of Homeland Security* may be labeled CII and exempted from *Freedom of Information Act* (FOIA) disclosure. This change in the law has potentially broad effects on normal business operations, as disclosure of information held by government has traditionally been favored in the US.

[457] http://www.dhs.gov/interweb/assetlibrary/Physical_Strategy.pdf.

[458] Procedures for Handling Critical Infrastructure Information, 68 Fed. Reg. 18,524 (2003) (to be codified at 6 C.F.R. §29).

Organizational Overview

Public Agencies

Department of Homeland Security (DHS)

The attacks of 11 September 2001 provided the impetus to restructure the overall organizational framework of CIIP in the US. The most important change was the establishment of the *Department of Homeland Security* (DHS).[459] It is expected that the DHS will become a federal center of excellence for cybersecurity and critical infrastructure protection and will encompass the following roles:

- Developing a comprehensive national plan for securing the key resources and critical infrastructures of the US;
- Providing crisis management in response to attacks on critical information systems;
- Providing technical assistance and emergency recovery plans to the private sector and other government entities;
- Coordinating with other agencies of the government to provide specific warning information and protective measures, and to fund research and development;
- To circulate information regarding cyber-security to the private sector;
- To fund research and development.

The DHS brought together 22 existing federal agencies in the largest federal reorganization since 1947. The Department is divided into five major divisions or 'Directorates': (1) Border and Transportation Security, (2) Emergency Preparedness and Response, (3) Science and Technology, (4) Information Analysis and Infrastructure Protection and (5) Management. In addition to these five directorates, several other critical agencies are amalgamating with the new department or are being newly created, such as the *US Coast Guard*, the *US Secret Service*, the *Bureau of Citizenship*, and the *Immigration Services*.[460] In addition, the DHS maintains a special liaison office for the private sector, again highlighting the essential focus on public private collaboration.

The next section provides an overview of key public actors in CIIP today. Due to the consolidation brought about by the formation of the DHS, many of these entities are now part of the department. It is important to note that

[459] http://www.dhs.gov.

[460] http://www.dhs.gov/dhspublic/display?theme=9&content=1075.

there are other governmental entities and agencies besides the DHS that are focused on homeland security.

Directorate for Information Analysis and Infrastructure Protection (IAIP)

As one of the five major divisions of the US Department of Homeland Security, the *Directorate for Information Analysis and Infrastructure Protection* (IAIP)[461] is responsible for identifying and assessing current and future threats and vulnerabilities to the homeland, issuing timely warnings, and taking preventive and protective action. The directorate focuses special attention on the protection of critical infrastructure and cyber-security.

The IAIP leads and coordinates the national effort to secure the nation's infrastructure and fosters an active partnership with the private sector. With the creation of the IAIP, the government has established a central contact point for state, local, and private entities to coordinate protection activities with the federal government.

An especially high priority is placed on protecting the infrastructure of cyberspace from terrorist attacks whose possible consequences could cascade across many sectors, causing widespread disruption of essential services, damage to the economy, or risk to public safety. Therefore, the IAIP has unified and focused the key cyber-security activities of the *Critical Infrastructure Assurance Office* (CIAO), formerly part of the *Department of Commerce*; the *National Infrastructure Protection Center* (NIPC), from the FBI; and the *Federal Computer Incident Response Center* (FedCIRC), formerly of the *General Service Administration*. Because CI relies heavily on information and telecommunication services and interconnections, the IAIP also assumed the functions and assets of the *National Communications Systems* of the *Department of Defense*, which coordinates emergency preparedness for the telecommunications sector and some responsibility of the *Energy Security and Assurance Program of the Department of Energy.*[462]

While the IAIP directorate is still reviewing its restructuring and incorporating various entities into its structure, it is expected that its infrastructure protection component will be organized into four divisions. These will likely include the *Infrastructure Coordination Division*, the *National Cyber Security Division, the Protective Services Division*, and the *National Communications System*.

[461] http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0094.xml.

[462] http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0094.xml.

National Cyber Security Division (NCSD)

In June 2003, the *National Cyber Security Division* (NCSD) was created under the IAIP to combat Internet-based attacks against government and critical private-sector backbone networks. The NCSD's main tasks are to identify, analyze, and reduce cyber-threats and vulnerabilities, issue threat warnings and coordinate incident response, as well as provide technical assistance in operations continuity and recovery planning.

The NCSD builds upon the existing capabilities transferred to the DHS from the former *Critical Infrastructure Assurance Office* (CIAO), the *National Infrastructure Protection Center* (NIPC), the *Federal Computer Incident Response Center* (FedCIRC), and the *National Communications System* (NCS). The NCSD works together with the *National Institute of Standards and Technology* (NIST) regarding the security of federal systems and with federal law enforcement authorities.[463]

The division is organized around three units designed to:

- Identify risks and help reduce the vulnerabilities to the government's cyber assets and coordinate with the private sector to identify and help protect critical cyber assets;
- Oversee a consolidated *Cyber Security Tracking*, *Analysis and Response Center* (CSTARC), which will detect and respond to Internet events; track potential threats and vulnerabilities to cyberspace; and coordinate cyber-security and incident response with partners from the private sector and international partners at the federal, state, and local levels;
- Create, in coordination with other appropriate agencies, cybersecurity awareness and education programs and partnerships with consumers, businesses, governments, academia, and international communities.[464]

Critical Infrastructure Assurance Office (CIAO)

The *Critical Infrastructure Assurance Office* (CIAO)[465] was created in May 1998 and is now part of the IAIP. The *Planning and Partnerships Office* (PPO) within the IAIP assumed many of the responsibilities previously held by the CIAO, such as raising issues that cut across industry sectors and

[463] http://www.dhs.gov/dhspublic/display?content=916.

[464] http://www.dhs.gov.

[465] http://www.ciao.gov.

ensuring a cohesive approach to achieving continuity in delivering critical infrastructure services. Its main tasks are:

- To coordinate and implement the national strategy;
- To assess the government's own risk exposure and dependencies on CI;
- To raise awareness and public understanding and participation in CIP efforts;
- To coordinate legislative and public affairs to integrate infrastructure assurance objectives into the public and private sectors.

National Infrastructure Protection Center (NIPC)

In 1998, the *Office of Computer Investigations and Infrastructure Protection* (OCIIP) was expanded to become the inter-agency *National Infrastructure Protection Cente*r (NIPC).[466] The NIPC is located at the FBI headquarters, but is part of the DHS IAIP. It coordinates the federal government's response to incidents, mitigating attacks, investigating threats, and monitoring reconstitution efforts. It coordinates the federal government's response to incidents, mitigating attacks, investigating threats, and monitoring reconstitution efforts.

Office of Homeland Security

The *Office of Homeland Security* was established in October 2001. Its mission is to "develop and coordinate the implementation of a comprehensive national strategy to secure the US from terrorist threats and attacks."[467] Among its functions is the coordination of efforts to ensure rapid restoration of CI after disruption by a terrorist attack.[468] 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.[469]

Homeland Security Council

The *Homeland Security Council* is an executive entity charged with advising the president on homeland security matters. In order to more effectively coordinate the homeland security policies and functions of the government, the council assesses the objectives, commitments, and risks, and oversees

[466] http://www.nipc.gov.

[467] http://www.dhs.gov/dhspublic/theme_home1.jsp.

[468] Bush, Executive Order 13228.

[469] Interview with a representative of the US Chamber of Commerce, June 2002.

and reviews the homeland security policies of the government. The council makes recommendations resulting from these activities to the president.

The council comprises a Principals Committee as well as coordination committees. The *Secretary of Homeland Security*, the *Secretary of Treasury*, the *Secretary of Defense*, the *Attorney-General*, the *Secretary of Health and Human Services*, the *Secretary of Transportation*, the *Budget Director for Central Intelligence*, the *FBI Director*, the *FEMA Director*, the *Chief of Staff to the President*, and the *Chief of Staff to the Vice President* compose the Principals Committee.

One of the coordination committees within the council is focused on CI. It is centered on the protection of both physical and virtual infrastructure.[470]

US Department of State

With respect to the formulation of an international CIP program in the US, the *Department of State* has overall statutory authority to conduct foreign affairs and therefore takes the lead in the interagency process of coordinating international CIP matters. The *Department of State* works together with other departments and agencies (including the Departments of Homeland Security, Justice, Defense, Commerce, Energy, Treasury, and Transportation, as well as the intelligence community, and others) to coordinate their objectives in an overarching strategy. Further activities of the Department of State include chairing the interagency *International CIP Policy Working Group*, which has key coordination mechanisms, and monitoring the implementation of agreements.[471]

Congressional Focus

Both Houses of Congress have created bodies to focus on CIIP issues. As part of the House of Representative's Select Committee on Homeland Security, the *House Subcommittee on Cybersecurity, Science, and R&D* examines the following: security of computers, telecommunications, information technology, industrial control, electric infrastructure, and related data systems including science, research, and development; protection of government and private networks and computer systems from domestic

[470] http://www.whitehouse.gov.

[471] Russell, Erica B. International and Interagency Critical Infrastructure Protection Coordination. *Presentation at the PfP Seminar on 'Critical Infrastructure Protection and Civil Emergency Planning – New Concepts for the 21st Century* (Stockholm, 17–18 November 2003). http://www.krisberedskapsmyndigheten.se/english/documents/seminar/programme_pfp-seminar_17-18_nov2003.pdf.

and foreign attack; prevention of injury to civilian populations and physical infrastructure caused by cyber attack; and oversight of relevant sectors. This subcommittee has held a number of hearings on related topics.

Within the Senate Committee on the Judiciary, the *Subcommittee on Terrorism, Technology, and Homeland Security* has oversight of laws related to government information policy, electronic privacy, security of computer information, and the Freedom of Information Act.

Defense Community

In response to the May 1998 *Presidential Decision Directive/NSC-63* (PDD-63), the *Department of Defense* (DOD) assigned the additional duty of *Critical Infrastructure Assurance Officer* (CIAO) to the *DOD Chief Information Officer* (CIO). In addition, each of the armed services (air force, army, and navy) established CIAOs, typically as an additional duty for the respective department's CIO. The armed services' CIAOs were responsible for developing a plan for protecting their department's critical virtual and physical infrastructure, for coordinating remedial efforts and reported to the DOD CIO/CIAO. Further, regional and functional commanders-in-chief and the services began identifying and securing their critical, operationally relevant assets and related infrastructure components.

Initially, the DOD and the individual services vulnerability assessment teams (inside the fence) and the *Joint Program Office for Special Technology Countermeasures* (outside the fence) conducted scheduled vulnerability assessments by installation on a regional basis to identify single points of service that could be vulnerable to loss through natural causes, human error, or deliberate attack.

With the establishment of the *Department of Homeland Security* (DHS), the DOD has established an *Assistant Secretary for Homeland Defense* and implemented a campaign plan for domestic military missions. The DOD's Defense Planning Guidance for the fiscal year 2004 defines the military's role in homeland defense as the military protection of US territory, the domestic population, and critical defense infrastructure against external threats and aggression.

Further, this guidance also calls for DOD to routinely study state activities to deter potential aggressors and to prepare US military forces for action, if needed. The functions of the previous DOD and armed services CIAOs have been integrated into the DHS under the IAIP directorate with the *Planning and Partnerships Office* (PPO) within DHS-IAIP, assuming many of the responsibilities previously held by the military CIAOs.

In addition to the lead in CIIP taken by the various DHS offices, the White House, Congress, and the defense community, each critical sector has a lead agency that can regulate or suggest practices for CIIP. For example, the lead agency for the energy sector is the *Department of Energy*. The *Department of Energy* regulates the nuclear power plants, and has mandated certain computer security rules for the plants. Further, the *Department of the Treasury* has responsibility for the financial services sector.

Public Private Partnerships

The government has actively promoted cooperation between the public and private sectors. It is a critical component of the national strategies and a strategic objective of the administration. Because the private sector owns the majority of critical infrastructure assets in the US (80–90 per cent), public private collaboration is essential to achieving effective CIIP. Further, one of the *Department of Homeland Security*'s main tasks will be to facilitate partnership efforts between the government and the private sector. It will develop relationships with and among state, local, and private entities.

To date, a number of unresolved issues have prevented comprehensive sharing between the public and private sectors. For example, unresolved legal issues – such as the *Freedom of Information Act* (see above), as well as anti-trust and liability issues, have hampered effective information-sharing. According to experts, resolving these issues should enhance information-sharing and spur the growth of ISACs.[472]

Office of Private Sector Liaison, Department of Homeland Security

The *Department of Homeland Security* has demonstrated its commitment to working with the private sector and strengthening public private partnerships by establishing the *Office of Private Sector Liaison*.[473] This office provides businesses with a direct line into the department. It acts both as an advocate for the private sector, by informing the secretary of their concerns, and as a clearinghouse, by directing businesses to the appropriate agency or directorate. The office is coordinated by the *Special Advisor to the Secretary for the Private Sector*.

One of the Liaison Office's main services is coordinating with *Information Sharing and Analysis Centers* (ISACs), trade associations, and businesses whenever there is a change in the threat level. The office provides guidelines

[472] Interview with a representative of the US Chamber of Commerce, June 2002.

[473] http://www.dhs.gov/dhspublic/display?theme=37.

and suggestions to private sector entities, so they may properly respond to the changes. Additionally, the office clarifies liability and compliance issues for businesses affected by new homeland security laws or regulations.

Although the Liaison Office is a relatively new post, it is growing steadily in significance and responsibility. The department plans to develop regional divisions next year, and the Liaison Office will play an important part in community outreach. With over 25 million businesses to coordinate, the office faces a tremendous task.

Information Sharing and Analysis Centers (ISACs)

Today, most critical infrastructure industry sectors have established their own *Information Sharing and Analysis Center* (ISAC), or are about to do so. 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).[474]
- The telecommunications industry has established 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 NCC, and members decide whether the suspect behavior is serious enough to report to the appropriate federal authorities.[475]
- The electric power sector has created 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.[476] The government and industry work together in the NERC to ensure the resiliency of the electricity infrastructure to potential physical and cyberspace attacks.[477]

[474] http://www.fsisac.com.

[475] http://www.ncs.gov/ncc.

[476] http://www.nerc.com; Energy Information Sharing and Analysis Center, http://www.energyisac.com.

[477] http://www.nerc.com/cip.html.

- 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 is operated by Internet Security Systems.[478]
- Other ISACs include the Surface Transportation ISAC,[479] the Oil and Gas ISAC,[480] the Water Supply ISAC, the Chemicals Industry ISAC, the Emergency Fire Services ISAC, the Emergency Law Enforcement ISAC, the Food ISAC, the Health ISAC, and the Interstate ISAC.

In addition to the individual sector ISACs, several ISAC leaders have convened as an ISAC Council. This council strives to strengthen the relationship between the ISAC community and government, and to solve problems common to all ISACs.

InfraGard

InfraGard is a partnership between industry and the US government as represented by the FBI. The *InfraGard* initiative was developed to encourage the exchange of information by members of the government and the private sector. With help from the FBI, private sector members and FBI field representatives form local chapter areas. These chapters set up their own boards to share information among their membership. This information is then disseminated through the *InfraGard* network and analyzed by the FBI.[481] There are currently over 75 *InfraGard* chapters.

National Cyber Security Alliance (NCSA)

The *National Cyber Security Alliance* (NCSA) is a cooperative effort between industry and government organizations to foster awareness of cyber-security through educational outreach and public awareness. It tries to raise citizens' awareness of the critical role that computer security plays in protecting the nation's Internet infrastructure, and to encourage computer users to protect their home and small business systems.[482] The NCSA is sponsored by a variety of organizations ranging from America Online, Apple, AT&T, CISCO Systems, Microsoft, MITRE, and Symantec to CERT/CC, GSA, and InfraGard.

[478] https://www.it-isac.org.

[479] http://www.surfacetransportationisac.org.

[480] http://www.energyisac.com.

[481] http://www.infragard.net.

[482] http://www.staysafeonline.info.

Partnership for Critical Infrastructure Security (PCIS)

The *Partnership for Critical Infrastructure Security* (PCIS) grew out of initiatives outlined in *Presidential Decision Directive 63* (PDD 63). It is a private-sector coalition that works to secure CI and examines cross-sector issues.

On 18 September 2002, many private-sector entities released plans and strategies for securing their respective infrastructures. The PCIS has played a unique role in facilitating private-sector contributions to this strategy.[483] The PCIS maintains a CIP calendar of conferences and other events as well as an Awareness Resources Repository, a searchable index of information on critical infrastructure security.[484]

Early Warning Approaches

Information-sharing is one of the driving factors behind effective early-warning networks. Many entities focused on information-sharing are also engaged in early-warning activities.

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.[485] According to some reports, 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 high-quality information on law enforcement and intelligence. Under PDD 63, the NIPC as part of the FBI was given 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.[486] The NIPC, as discussed above,

[483] http://www.pcis.org.

[484] http://www.pcis.org.

[485] President's Commission on Critical Infrastructure Protection, Critical Foundations.

[486] Clinton, Presidential Decision Directive 63.

was incorporated into the DHS. The comprehensive early-warning system is now likely to be channeled through the US CERT, discussed below. The FBI still retains its responsibilities for addressing cybercrime.

Directorate for Information Analysis and Infrastructure Protection (IAIP)

The *Department of Homeland Security's Directorate* IAIP[487] was set up with a special focus on systematically analyzing all information and intelligence on potential terrorist threats within the US. This division compiles and analyzes information from multiple sources, including the CIA, the FBI, the Defense Intelligence Agency (DIA), and the National Security Agency (NSA), and issues early warnings of terrorist attacks.[488] In case of an attack, IAIP would aim to:

- Provide warning of threats against the US, including physical and virtual attacks;
- Issue threat advisories through the Homeland Security Advisory Systems;
- Provide information about terrorist threat to the public, private industry, state, and local government.[489]

The new *National Cyber Security Division* (NCSD) within the IAIP will issue alerts and warnings around the clock. Its three units are geared to early detection of cyber threats, especially the Cyber Security Tracking, Analysis & Response Center.

US-CERT

On 15 September 2003, the *Department of Homeland Security*, in conjunction with the *CERT Coordination Center* (CERT/CC) at Carnegie Mellon University, announced the creation of the US-CERT. The US-CERT works with the *National Cyber Security Division* (NCSD) of the IAIP to prevent and mitigate cyber-attacks and to reduce vulnerabilities to cybernetic attacks. The US-CERT is also the central element in the NCSD's *Cyber Security Tracking Analysis and Response Center*, which includes the *Federal Computer Incident Response Center* (FedCIRC).

The US-CERT initiative is designed to utilize the CERT/CC's capabilities to help accelerate the nation's response to cyber-attacks and vulnerabilities.

[487] http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0094.xml.
[488] http://www.whitehouse.gov/deptofhomeland/sect6.html.
[489] http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0094.xml.

The initiative also enables the DHS to provide expanded analysis, warning, and response coordination.[490]

Federal Computer Incident Response Center (FedCIRC)

The responsibility for detecting and responding to cyber-attacks on federal agencies 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 FedCIRC was incorporated into the IAIP as part of the DHS in March 2003 and is now part of the *National Cyber Security Division* (NCSD).

The Bush administration is expected to issue a guide for federal agencies to report computer security incidents to the FedCIRC. The guide is expected to outline the type of information required in an incident report that will give FedCIRC the data it needs to track and analyze incident reports.

CERT Coordination Center, Carnegie Mellon University

The CERT/CC is located at the *Software Engineering Institute* (SEI), a federally funded research and development center operated by Carnegie Mellon University. It was established in 1988 after the Morris worm crashed 10 per cent of the world's Internet systems. CERT/CC acts as a coordination hub for experts during security incidents, and works to prevent future incidents.[491]

The CERT/CC acts through several mechanisms. First, they research and assess network vulnerabilities and develop risk assessments. Second, they disseminate information to the public through regular security alerts and presentations to the public. Finally, members of the CERT/CC participate in various security groups to improve Internet security and network survivability. The CERT/CC will also now be a primary contributor to the US-CERT.

Internet Security Alliance

The *Internet Security Alliance* (ISAlliance) is a non-profit collaborative effort between the Carnegie Mellon University's *Software Engineering Institute* (SEI) CERT Coordination Center (CERT/CC) and the *Electronic Industries Alliance* (EIA), a federation of trade associations representing 2'500 companies. It was created to provide a forum for intellectual leadership and information-sharing on information-security issues. ISAlliance allows

[490] http://www.uscert.gov.
[491] http://www.cert.org.

its participants to access threat reports, learn of best security practices, and discuss risk management strategies.

Information-Sharing and Analysis Centers (ISACs)

The *Information Sharing and Analysis Centers* (ISACs) were planned to help create an early-warning database. The idea is that private-sector owners and operators will survey incidents and pass the information on to central point of contact for information-sharing and then distribute it to ISAC membership (see Chapter on 'Public Private Partnerships' above).

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