The Organization Framework, the Notification System and the Legal Norms of Critical Infrastructure Protection in the U.S.

1. Organization Framework

In the organization framework of critical infrastructure protection, there are mainly the public departments and the PPP organizations. The functions and task description of relevant organizations are as follows.

(1) Department of Homeland Security

After the September 11 attacks in America, the Homeland Security Act was passed in November 2002, and based on this act, 23 federal organizations, plans and offices were integrated to establish the Department of Homeland Security (DHS) to take responsibility for homeland security in America. The tasks include: (1) to analyze intelligence data collected from various departments such as the Central Intelligence Agency (CIA) and the Federal Bureau of Investigation (FBI) so that any threats to security can be discovered in time, (2) to protect and defend critical infrastructure, (3) to coordinate and lead America to prevent and respond to the attacks from nuclear weapons, biochemical weapons and other and (4) to coordinate the tasks of the federal government, including emergency and rescue. For the task regarding critical infrastructure and critical information infrastructure protection, the main units in charge are the Office of Infrastructure Protection (OIP) and the Office of Cybersecurity and Communications (CS&C) subordinate to National Protection and Programs Directorate (NPPD), Department of Homeland Security (DHS), to reduce the risk in both physical and cyber security to maintain national security[1]

(2) Congress

Relevant units and committees are established both in the Senate and the House of Representatives to be responsible for protection and making policies pertinent to important critical infrastructure and critical information infrastructure.

(3) Computer Crime and Intellectual Property Section

In 1991, the Department of Justice (DOS) established the Computer Crime and Intellectual Property Section (CCIPS), a section of the Criminal Division, to be responsible for all crime combating computer and intellectual property. Computer crime is referred to cases which include electronic penetrations, data thefts, and cyber attacks to the important critical infrastructure. CCIPS also prevents, investigates, and prosecutes computer crimes by working with other government agencies, the private sector, academic institutions, and foreign counterparts.

(4) Other Relevant PPP Organizations

[2]The Information Sharing and Analysis Center (ISAC) is responsible for the information security message sharing among the industries of each critical infrastructure to ensure the liaison and cooperation among industries. Finally, for the issue on critical information infrastructure, especially cyber crimes, both the National Cyber Security Alliance (NCSA) and the Cross Sector Cyber Security Working Group (CSCSWG) are designated to serve as crucial roles in governmental and non-governmental internet security prevention to be responsible for techniques and education.

2. Notification System

(1)Computer Emergency Response Team Coordination Center

The Computer Emergency Response Team Coordination Center (CERT/CC) run by Carnegie Mellon University is the oldest and most important early-warning organization for information security in the USA. With its experts studying internet vulnerabilities and risk assessment released regularly, it reminds people of the possible dangers which exist in the information age and the need to improve internet security.

(2)US Computer Emergency Readiness Team

The US Computer Emergency Readiness Team (US-CERT) was established in 2003. It is responsible for protecting the infrastructure of the internet in America and for coordinating and providing response support and defense against national cyber attacks. It interacts with federal agencies, industry, the research community, state government, and others to disseminate reasoned and actionable cyber security information to the public.

(3)Federal Bureau of Investigation

The Federal Bureau of Investigation (FBI), the first early warning center of critical infrastructure at the national level, is responsible for providing the information pertinent to legal execution presently and also taking responsibility for the investigation of cyber crime.

(4)Information Sharing and Analysis Centers

Currently, industry in America, including finance, telecommunications, energy, traffic, water resources, together established individual Information Sharing and Analysis Centers (ISACs) based on the policy made in PDD-63. The ISAC of the financial system established in October 1999 being the first established center. These ISACs further work together to form an ISAC Council to integrate the information from each of them and improve their interaction and information sharing.

3. Legal Norms

In reference to the laws and regulations of critical infrastructure protection, America has aimed at critical infrastructure protection and computer crime to formulate the following regulations.

(1) Federal Advisory Committee Act of 1972

According to the Federal Advisory Committee Act (FACA), the advisory committee can be established in every federal agency to provide the public, along with received open advice, with relevant objectives, and to prevent the public from being inappropriately influenced by the policies made by the government. However, to keep the private institutions which run the critical infrastructures from worrying the inappropriate leak of the sensitive information provided and consulted by them, Critical Infrastructure Partnership Advisory Council was established so that the Secretary of Homeland Security has the right to disregard the regulations of FACA and establish an independent advisory committee.

(2) Computer Fraud and Abuse Act of 1986[3]

The Computer Fraud and Abuse Act (CFAA) was enacted and implemented in 1986. It mainly regulates computer fraud and abuse. The Act states that it is against the law for anyone to access a protected computer without authorization. However, it also recognizes the fact that accessing a computer system of electronic and magnetic records does not mean a violation of the law. According to the CFAA, what is needed is one of the following requirements to be the wrongful conduct regulated in the Act: (1) whoever intentionally accesses a computer to obtain specific information inside the government or whoever has influenced the transmission function of the computer system; (2) whoever intentionally accesses a computer to obtain a protected database (including the information contained in a financial record of a financial institution or of a card issuer, or the information contained in a file of a consumer reporting agency on a consumer, or the information from any department of agency of the United States, or the conduct involving an interstate transaction); (3) whoever intentionally accesses any nonpublic computer of a department or agency of the United States, and causes damage. In addition, the Act also prohibits conduct such as transmitting malicious software, and defrauding traffic in any password or similar information. For any person who suffers damage or loss by reason of a violation of the law, he/she may maintain a civil action to obtain compensatory damages and injunctive relief or other equitable relief. However, the Computer Abuse Amendment Act (1994) expands the above Act, planning to include the conduct of transmitting viruses and malicious program into the norms whose regulatory measures were adopted by the USA Patriot Act enacted in October 2001[4]

(3) Homeland Security Act of 2002[5]

The Homeland Security Act provides the legal basis for the establishment of the Department of Homeland Security and integrates relevant federal agencies into it. The Act also puts information analysis and measures of critical infrastructure protection into the norm. And, the norm in which private institutions are encouraged to voluntarily share with DHS the information security message of important critical infrastructure is regulated in the Critical Infrastructure Information Act: Procedures for Handling Critical Infrastructure Information. According to the Act, the DHS should have the obligation to keep the information provided by private institutions confidential, and this information is exempted from disclosure by the Freedom of Information Act.

(4) Freedom of Information Act

Many critical infrastructures in America are regulated by governmental laws, yet they are run by private institutions. Therefore, they should obey the law and provide the government with the operation report and the sensitive information related with critical infrastructure. However, knowing that people can file a request at will to review relevant data from the government agencies based on the Freedom of Information Act (FOIA), then the security of national critical infrastructure may be exposed to the danger of being attacked. Therefore, the critical infrastructure, especially the information regarding the safety system, early warning, and interdependent units, are all exempted by the Freedom of Information Act.

(5) Terrorism Risk Insurance Act of 2002[6]

After the 911 Incident, Congress in America passed the Terrorism Risk Insurance Act to establish the mechanism to underwrite terrorism risk insurance, in which insurance companies are required to provide terrorism attack risk insurance and the federal government will also cover part of loss for severe attacks.

1.http://www.dhs.gov/xabout/structure/editorial_0794. shtm (last accessed at 21. 07. 2009).
2.http://www.thei3p.org/ (last accessed at 21. 07. 2009).
3.http://www.panix.com/~eck/computer-fraud-act. html (last accessed at 21. 07. 2009).
4.Mark G. Milone, Hacktivism：Securing the National Infrastructure, 58 Bus. Law, 389-390, 2002.
5.http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf (last accessed at 21. 07. 2009).
6.http://www.ustreas.gov/offices/domestic-finance/financial-institution/terrorism-insurance/pdf/hr3210.pdf (last accessed at 21. 07. 2009).

Release：2013/04

Tag