Special Action Plan on Countermeasures to Cyber-terrorism of Critical Infrastructure (Provisional Translation)

December 15, 2000

1. Goals of the Special Action Plan

The goal of this action plan is to protect the critical infrastructure from attacks of cyber-terrorism, which have the potential for large impacts on people's lives and on the economic activities of business using telecommunications networks and information systems.

The government, primarily the Cabinet Secretariat, in close cooperation with the private sector, is working hard to implement this plan. In addition, as an objective of this plan, there are efforts to enhance the voluntary, independent participation by the businesses and regional public organizations associated with the critical infrastructure areas in the private sector (hereafter, called private sector critical infrastructure operators). Furthermore, the government will provide the necessary cooperation when the private sector critical infrastructure operators implement the plan.

2. The Threat of Cyber Terrorism

Many businesses and government activities have come to depend on information systems. It is also expected that there will be an acceleration in the use of information technologies and networking. For the critical infrastructure, like power supply, transportation, and electronic control, information systems also have a crucial role in maintaining public safety and stable supplies of indispensable services for the economic activities of business and the daily lives of the people.

An electronic attack using telecommunications networks and information systems (called a "cyber attack") on these important information systems that are fundamental to the critical infrastructure, has the potential to disrupt people's lives and business activities, as well as to cause large amounts of damage, placing people's lives at risk. This kind of attack, unlike a physical attack, can be made from a single computer by a person with the ability to intrude the information system. There is also the fear that systematic, large-scale attacks could be made for the purpose of causing disruption and confusion to business activities and people's lives.

Overseas, there have been cases of damage to financial information systems, and individuals known as hackers intruding critical information systems, denial-of-service attacks (DoS attack), as well as instances of large amounts of damage caused by the spread of computer viruses; so it is clear that this threat is already becoming a reality. The United States is developing a congressional plan

to handle the threat of financial damage, confusion, injury or death caused by attacks on critical networks by terrorist groups or criminal organizations having advanced technical skills.

Connections via the Internet and other networks continue to develop, and interdependence increases. There is also increasing standardization and commonality in the specifications of information systems. These trends increase the threat of cyber attacks, even on information systems that currently face little danger from outside intrusion. In addition, there is always the possibility of such attacks being made by inside personnel. It must be recognized that even an information system that is not connected to any other networks is not immune to the danger of an outside attack.

3. Critical Infrastructure Fields

At the present time, the critical infrastructure fields that are considered likely to have the largest impact on financial activities and people's daily lives in the event of a cyber-terrorist attack are telecommunications, finance, aviation, railroads, electrical power, gas, and government/administrative services (including regional public organizations).

The ministries and agencies with jurisdiction over each of these critical infrastructure areas are making efforts to appropriately implement this plan for each of the areas.

In order to protect the critical infrastructure of Japan from the threat of cyber-terrorism it is also important for fields other than these critical infrastructure fields to refer to this special action plan and strengthen the countermeasures as needed.

4. Preventing Damage (Raising Security Level)

In order to prevent damage, risk analysis will be performed for the information systems of the target critical infrastructures, and measures will be implemented as needed according to the importance of the information system. It is also necessary to continually raise security level in each of the fields with critical infrastructure.

(1) Raising security level in private sector critical infrastructure fields

- Private sector critical infrastructure operators are working to raise security level by referring to "Guidelines for IT Security Policy" (issued July 18, 2000 by the IT Security Promotion Committee), the guidelines on information security from the various ministries and agencies, and the OECD security guidelines, and establishing risk analysis and information security

policies.

- When private sector critical infrastructure fields as well as regional public organizations (hereafter called "private sector, etc.") use information system with a common standard specification, or are connected to other information systems, there shall be proper handling of the shared risk for that field. To achieve this, investigations shall be made to establish countermeasure guidelines for these private sector, etc. groups.
- In order for the government to contribute to improving security level for the private sector, etc., efforts are being made to provide information, advice, and instruction, and to support the efforts of the private sector etc. groups.

(2) Raising security level to establish electronic government

- The various ministries and agencies implementing the necessary measures to improve security level, starting by establishing an electronic government foundation by 2003, and following the policies established according to the "Guidelines for IT Security Policy".
- The special advisory team of the Cabinet Secretariat is providing technical surveys and advice on security countermeasures for information systems for the various ministries and agencies.

5. Establish and Enhance Communication and Coordination Systems between Government and the Private Sector

For the various critical infrastructure fields, it is necessary to establish and enhance systems for the government and private sector to coordinate prevention, response, and sharing of security data (data required to improve security) as well as warning information (information needed for emergency response and warnings, such as data on the occurrence of cyber attacks).

Particularly, as the threat of cyber terrorism grows, it is necessary to quickly establish a communication and coordination system between government and the private sector to handle cyber terrorism, and based on the situation in each field, it is necessary to develop the next level of systems, within one year of establishing this plan.

(1) Communication and coordination systems for private sector etc. critical infrastructure groups

Build a communication and coordination system between operators associated with cyber-terrorism countermeasures, while making use of existing communication mechanisms, to fulfill the following roles.

- Collect, distribute and share the common security information in the various fields, as well as the warning information.
- A communication system for when a cyber attack occurs, or when there is a danger of such an

attack

- Implement unified, centralized communications for the government and related agencies

(2) Communication and coordination systems with other critical infrastructure operators

In cases of interconnection to other information systems and operators of important infrastructure in other fields through networks, develop, as needed, the communication and cooperation systems for cyber-terrorism countermeasures.

(3) Establishing a communication and cooperation system for government

The government, centering on the Cabinet Secretariat, will fill the following roles in developing the communication and cooperation systems

- Collecting, distributing and sharing security information and warning information
- Collecting information when a cyber-attack occurs, or when there is a danger of such an attack
- Within government departments, communication with related agencies and the private sector etc. critical infrastructure groups

(4) Handling of data

For the information collection and sharing, the appropriate data will be provided by the private sector etc. critical infrastructure groups. To achieve this, there must be efforts made to build a relationship of trust between all interested parties, such as obtaining a consensus on handling this data rigorously and correctly.

(5) Cooperation with private sector etc. critical infrastructure groups

The government will make efforts to cooperate with the private sector etc. critical infrastructure groups, including providing security and warning information.

6. Detection of Cyber Attacks and Emergency Response Through Government and Private Sector Cooperation

In addition to determining the measures to be taken for each of the critical infrastructure fields in the event of a cyber attack, or when there is a danger of such an attack, it is necessary to strengthen the response capabilities of the government and private sector overall.

(1) Detection of cyber attacks

- The government and private sector etc. critical infrastructure operators shall determine in advance the appropriate handling measures for the situation, including type and extent of the

damage, and locations, in the event that damage occurs to a key information system, assuming that it is difficult to judge whether it is a cyber attack, based on adequate consideration of the potential scenarios.

- The government and private sector etc. critical infrastructure operators will collect security data and warning data from government agencies, organizations related to information security, and information system vendors, etc.

(2) Establishing an emergency response plan

- To establish countermeasures and an emergency response plan in the event of a cyber attack, or when there is a danger of such an attack on the private sector etc. critical infrastructure operators, investigate while making use of the communications systems established as described in section 5.

  (Expected issues for the emergency response plan)

  Communication, containment of damage, verification of safety, recovery (temporary measures), prevention of recurrence, etc.

  Furthermore, it is important that this plan outlines the procedures over time after a cyber attack is detected, so that it is possible to respond quickly.
- The actions during an emergency will sometimes require a high-level judgement, so procedures like the emergency response plan will be determined so that the appropriate persons, having the proper authority and responsibility, can make decisions quickly.

(3) Information and communication procedures during an emergency

- In the event of a cyber-attack, or when there is an information indicating a danger of such an attack, the emergency information communication procedure is as follows.

  (a) Communication of information related to the cyber attack

  ① The ministry, agency or private sector, etc. critical infrastructure operator that is subject to a cyber attack, or obtains information indicating the danger of such an attack, in addition to quickly taking the appropriate steps, will also provide the relevant information to the specified personnel in other key private sector infrastructure fields, local government offices, and related agencies.

  ② The ministries and agencies that receive this information will provide guidance and advice to the private sector, etc. critical infrastructure operators subjected to the attack, as well as informing the Cabinet Secretariat of the relevant information.

  ③ The Cabinet Secretariat will coordinate the related ministries and agencies, and collect information.

(b) Communication of warning information

① The Cabinet Secretariat notifies the various ministries and agencies of warning information when it is necessary based on the contents of the information indicating an attack or the danger of an attack.

② When the various ministries and agencies receive warnings from the Cabinet Secretariat, they will quickly notify the local private sector etc. critical infrastructure operators.

- The government and private sector, etc. critical infrastructure operators will run drills of cyber terrorism countermeasures as necessary.
- In the event that people's lives or business economic activities are affected due to damage from an attack, the government and private sector, etc. critical infrastructure operators will make every effort to quickly provide the relevant information to those involved.

(4) Strengthening the government's emergency response system

- In the event of a cyber attack, or when there is a danger of such an attack, the Cabinet Secretariat will collect information and coordinate the cooperation and efforts of the various ministries, as well as organizing the ministries and agencies for the action guidelines when it is necessary for the government to take action.
- The Cabinet Secretariat will establish the required communications systems with the cooperation of the various ministries and agencies. In addition, the information gathering system and the response systems for cyber terrorism will be enhanced by the various ministries and agencies.

7. Establish Foundations of Information Security

Training of personnel, research and development, widespread application, and appropriate laws and regulations on information security fundamentals is required in order to further develop countermeasures to cyber terrorism.

To provide protection from cyber attacks on critical infrastructure, the operators and users of general information systems, not just those of the key systems, must be aware of the threat of cyber attacks, deepen their understanding of the need for security measures, and take the necessary security countermeasures so that there is a widespread general awareness and effort to handle this issue.

(1) Promote development of human resources

- The government and private sector, etc. critical infrastructure operators will work to continuously train educate personnel, and to develop specialists in security technology.

(2) Promote research and development

- The government and private sector, etc. critical infrastructure operators will promote cooperation and communication between the government and the private sector on research of the technology, countermeasures, threat analysis, and development of the required technology to build a strong foundation against the threat of cyber terrorism.

(3) Promote widespread application

- The government will announce the occurrences of illegal access, publicize information on defense against illegal access, and raise general awareness on cyber terrorism threats both inside and outside Japan.
- The government will promote research and study of information security for the personnel of the private sector, etc. critical infrastructure operators.

(4) Add and revise legislation

- The government will consider changes to the law, such as the basic criminal law, from the perspective of maintaining safety for the telecommunications networks and international harmony.

8. International Cooperation

Cyber attacks can be made without regard for national boundaries, so international cooperation and coordination is required in order to handle such attacks.

- The government and private sector, etc. key infrastructure operators will work to accumulate information from information security organizations outside Japan.
- The government will promote cooperation with the international organizations related to cyber-terrorism of the OECD and G8.
- The government will work to strengthen international cooperation, information exchanges and shared training with the counterparts in other nations.

9. Action Plan Revisions

This action plan is the first version, focused on establishing a means of communication and coordination between the government and the private sector. The government will periodically review and revise this plan as required, according to future progress and developments.