Secure Japan 2006

- First Step towards a Trustworthy Society -

Information Security Policy Council

15 June, 2006

Contents

Chapter 1 Basic Policy for Addressing Information Security

– Priority for FY 2006 "Establishing the System for Information Security Measures in the Public and Private Sectors" –

Information technology (IT) has improved people's social lives and the economic activities of Japan. Furthermore, it is expected to enrich both Japan and the rest of the world in the future. However, as IT comes to increasingly penetrate into people's social lives and the economic activities of Japan, some incidents take place in which the use of IT itself threatens the safety and comfort of people's social lives and economic activities. In order to substantially strengthen the measures against these incidents, the First National Strategy on Information Security was formulated to promote integrated and cross-sectoral information security measures in the public and private sectors. This is the mid- and long-term strategy concerning information security measures of Japan (decision by the Information Security Policy Council (ISPC), hereinafter referred to as the "National Strategy").

Following the National Strategy, "Secure Japan 2006" sets out priority measures for the information security of the Government of Japan in FY 2006, and the direction of priority measures for FY 2007.

Information security issues that occurred in 2005 include cyber attacks on the web-servers of government agencies, information leakages caused by using file-sharing software or by computer viruses, operation shutdowns caused by IT-malfunctions in critical infrastructures that have huge impacts, and cybercrimes committed by creating and using spyware, such as unauthorized computer access and online financial fraud. These incidents have raised concerns about the use and utilization of IT itself. Regrettably, approaches to the information security management of Japan have been taken separately by each entity: namely, the central government, local governments, critical infrastructures, businesses, and individuals. Furthermore, overall measures have not been sufficient.

The Government of Japan thereby makes it a priority objective for FY 2006 to **establish the system for information security measures in the public and private sectors** as the first step towards the realization of a Trustworthy Society, that is, "Secure Japan". Four basic policies listed in the National Strategy will be promoted in the following manner:

(1) Formation of a Common Recognition among Public and Private Entities

For ensuring the information security of each entity, initiatives of each entity that are in line with its own behavioral principles are essential. To promote such initiatives, the formation of a common recognition is necessary about for what purpose and to what degree of risk each entity will take information security measures.

In order to practically establish a common recognition shared by each entity in the public and private sectors based on these factors, the following points are necessary: each entity having a sense of participation in information security measures, each entity contemplating information security measures and participation in formulation of a common recognition, and each entity proactively taking information security measures and calling upon others to do likewise.

The Government of Japan thereby makes it a priority objective for FY 2006 to **encourage all the entities to share a sense of participation in information security measures,** and will make concerted efforts to promote various measures.

(2) Pursuing Advanced Technology

It is necessary to promote information security measures constantly encompassing elements of the most advanced R&D and technology development in order to address the wave of new information security threats, instead of taking measures only for immediate problems.

In doing so, it is important to: 1) make improvements, being aware of the risk of relying on a single source of technology or single infrastructure, and 2) introduce Internet Protocol version 6 (IPv6) and make further efforts in R&D and technology development from the perspective of establishing a new infrastructure with a built-in function of information security, in addition to technical solutions to existing infrastructure problems.

In order to practically pursue advanced technologies based on these factors, it is necessary to identify threats to information security, specify the area of advanced technology to be pursued and focus investments primarily on that area in a planned manner, and actively adopt available advanced technologies.

The Government of Japan thereby makes it a priority objective for FY 2006 to **take measures to pursue advanced technologies under a coherent policy of the entire government,** and will make efforts to promote various measures.

(3) Strengthening the Response Capability of the Public Sector

In order to further consolidate Japan’s strength as an information security advanced nation to the level of comparative advantage, it is essential to strategically improve the response capability of the public sector. In specific terms, for example, the following elements are necessary:

1) The public sector’s initiative in implementing measures by actively following “Best Practice” of public and private organizations in both Japan and abroad;

2) Establishment of social infrastructure with diversity; and

3) Promotion of efforts from the perspective of national security and risk management, such as the strengthening of national defense, enhancement of countervailing power against crimes and terrorism, and measures for disaster relief in view of the emergence of new threats caused by the expansion of use and utilization of IT.

On the other hand, when the response capability of the public sector is improved, it is indispensable to constantly consider ensuring human rights, transparency and the legality of public activities.

In order to practically strengthen the response capability of the public sector based on these factors, it is necessary to establish and manage a framework to increase the level of information security measures of the public sector, to improve the response capability to incidents, and to establish and elaborate communication systems necessary for the public and private sectors.

The Government of Japan thereby makes it a priority objective for FY 2006 to **establish a framework to upgrade the level of information security measures of the public sector and communication systems necessary for the public and private sectors,** and will make efforts to promote various measures.

(4) Promotion of Partnership/Cooperation

In order to establish a "new public-private partnership model," it is necessary to seek partnership and the cooperation of each public and private entity in Japan, and to implement measures by bringing together their collective wisdom.

In addition, the issues confronting Japan, which became the world's broadband leader, are matters the rest of the world will face in the future. In view of the responsibility for finding solutions as a top nation, efforts for international cooperation and contribution are also indispensable. In doing so, it is necessary to present the "Japan Model" of information security by formulating the outcome for Japan in such a way as to be applicable to other countries, through, for example, the introduction of a system in which entities implementing information security measures are evaluated.

It is also necessary to take internationally responsible actions, while being constantly aware of the fact that IT infrastructure is always connected to the world, 24 hours a day, 365 days a year.

The Government of Japan, in order to ensure that all entities work with cooperation and partnerships with each other, thereby makes it a priority objective for FY 2006 to **establish an information sharing system of information security measures by all parties concerned**, and will make efforts to promote various measures.

Chapter 2: Strengthening of Information Security Measures in Four Implementation Fields

In line with the National Strategy, in the "Secure Japan 2006," information security measures are grouped into four areas according to the implementation entities, namely, the central government/local governments, critical infrastructures, businesses, and individuals.

Section 1: Central Government/Local Governments

A: Central Government

In FY 2006, the Government of Japan prioritizes the promotion of the following measures in the area of government agencies, with the purpose of 1) upgrading the level of the Standards for Information Security Measures for the Central Government Computer Systems[1] (hereinafter referred to as "Standards for Measures") to the world's highest level by FY 2008 and 2) enabling all the government agencies to implement the measures at the level meeting the Standards for Measures by the beginning of FY 2009.

1) Establishment of the Standards for Measures and of the PDCA Cycle through Evaluations/Recommendations Based on the Standards

In order to upgrade the level of information security measures of government agencies to the world's highest level, the Standards for Measures will be reviewed annually in accordance with changes in technologies and environment.

A Plan-Do-Check-Act Cycle (PDCA Cycle) of the whole government will be created by (1) inspecting and evaluating the implementation of security measures at the government agencies within the necessary scope, based on the Standards for Measures, and (2) linking the recommendations obtained from the evaluations to the improvement of the measures and to the upgrading of the Standards for Measures. Moreover, the results of evaluations are disclosed with due regard to maintenance/ensuring of information security.

Furthermore, since contents, experience and other related knowledge of government agencies are desired to serve as a reference to companies, local governments and incorporated administrative agencies, the knowledge will be disclosed and disseminated in an understandable manner as "Best Practice". It is also important to give sufficient consideration to assurance of the level of information security measures of contractor.

[Specific Measures]

A) Implementation of the review of the Standards for Measures

a) Review of the Standards for Measures (Cabinet Secretariat)

[1] The "Standards for Information Security Measures for the Central Government Computer Systems" is decided by ISPC on December 13, 2005.

In light of changes in technologies and environment, the Standards for Measures will be reviewed in FY 2006.

B) Establishment of PDCA Cycle

a) Establishment of a PDCA Cycle at each government agency (All government agencies)

Based on the standards of government agencies, which reflect the Standards for Measures, specific operation procedures will be developed, and implementation of information security measures will be self-assessed and audited, etc., thus establishing a PDCA Cycle in FY 2006.

Seminars for all government employees will be designed and held at each government agency to ensure thorough compliance with the standards of government agencies, operation procedures and so forth.

b) Establishment of PDCA Cycle of the entire government (Cabinet Secretariat and all government agencies)

A PDCA Cycle of the entire government will be created in FY 2006, by inspecting and evaluating, within a necessary scope, and based on the Standards for Measures, the implementation of measures taken by the government agencies, and linking the recommendation obtained from the evaluations to the improvement of the measures and to the upgrading of the Standards for Measures.

c) Evaluation and disclosure of the results (Cabinet Secretariat)

During the first half of FY 2006, trial-based evaluations will be conducted on priority items in line with the Standards for Measures, and a method for full-fledged evaluation will be sought within FY 2006 that can be objectively comparable and effective for the establishment of a PDCA Cycle, referring to the evaluation methods of other countries as a reference.

Evaluation results will be disclosed with due regard for the maintenance and ensuring of information security.

C) Support for formulation of operation procedures, provision of technological information, and share of information (Cabinet Secretariat)

In order to support the promotion of information security measures of each government agency, the competent agency will support the formulation of operation procedures and provide technological information. Meanwhile, such information will be made publicly available and promulgated in a sequential manner from FY 2006 after being tailored to reflect the practices of each government agency so that they can be used as “Best Practices” by private corporations, local governments, and incorporated administrative agencies.

D) Response to information leakage caused by computer viruses (All government agencies)

In order to prevent information leakage caused by such problems as computer viruses that infect computers via file-swapping software, information management, based on the Standards for Measures, will be thoroughly implemented in FY 2006 by, for example, enforcing strict control on the taking out of internal information, and using private computers for office work at each government agency.

E) Ensuring the level of information security measures taken by contractors

a) Use of the Conformity Assessment Scheme for Information Security Management System, etc. (Cabinet Secretariat and all government agencies)

In order to verify the level of information security measures taken by outsourcing candidate contractors, the Compatibility Evaluation System for Information Security Management System and the Benchmark for Information Security Countermeasures will be used on an as-needed basis in FY 2006 as criteria for selection in government procurement.

b) Use of information security auditing system (Cabinet Secretariat and all government agencies)

In order to appropriately evaluate and verify the level of information security measures taken by contractors, an information security auditing system, which is based on management standards pursuant to international standards, will be used in FY 2006 on an as-needed basis.

c) Use and dissemination of Guidelines for Improving Reliability of Information Systems (Cabinet Secretariat)

In light of the fact that malfunction of information systems, the socio-economic infrastructure, have imposed great impacts on people’s lives, the Industrial Structure Council (The sub-committee on information service and software, Information economy committee) will formulate “Guidelines for Improving the Reliability of Information Systems” in June 2006. The Guidelines will stipulate means and measures to improve information systems targeting all information systems from a comprehensive viewpoint, including the process management aspect, such as development and operation, technical aspect, and organizational aspect, etc. Subsequently, discussions will be conducted in FY 2006 on the feasibility of the use and dissemination of the aforementioned Guidelines in the government agencies.

2) Improvement of Security Measures of Incorporated Administrative Agencies, etc.

Upgrading of the level of information security of incorporated administrative agencies and the like will be promoted based on the Standards for Measures. Particularly, the incorporated administrative agencies will formulate security policies if they have not done so yet, in accordance with current situations of information assets and risks of each institution. If security policies have already been set forth, the incorporated administrative agencies will review them.

[Specific Measures]

A) Development of information security policies of incorporated administrative agencies, etc. (Cabinet Secretariat and all government agencies)

Development process of information security policies of incorporated administrative agency, etc. will be examined in FY 2006. Based on the study result, incorporated administrative agencies will promote formulation/review of the information security policies, using the Standards for Measures as a reference.

B) Development of an environment for improving information security measures of incorporated administrative agencies, etc. (Cabinet Secretariat)

Based on the organizational and operational patterns of incorporated administrative agencies, an environment for improving the information security measures of incorporated administrative agencies will be developed in FY 2006, such as extracting issues on the application of information security policies and provision of necessary information, etc.

3) Strengthening and consideration of mid- and long-term security measures

The government will make efforts for the implementation of the following information security measures that should be performed in cooperation with all government agencies, such as standardization of required specifications on information security, and emergency responses in the middle of a fiscal year, etc.

(a) Coordination with development of common operations and systems among all or some Ministries and Agencies to be optimized

In optimization of common operations and systems among all or some Ministries and Agencies, the government will promote newly developed (installed) systems in such a way as to standardize required specifications on information security and use highly reliable products through the clarification of information security functions, while seeking coordination with the Standards for Measures, etc.

[Specific Measures]

A) Strengthening of cooperation between the Cabinet Secretariat and the deputy Chief Information Officers (CIO) of each government agency (Cabinet Secretariat and Ministry of Internal Affairs and Communications)

Regarding optimization of common operations and systems among all or some Ministries and Agencies, cooperation between the Cabinet Secretariat and the deputy CIO of each government agency will be strengthened, and effective installation of information security functions in the development of the target system will be promoted in FY 2006.

B) Promotion of the use of highly safe and reliable IT products, etc. (Cabinet Secretariat and all government agencies)

In order to establish highly safe and reliable information systems, when procuring IT products, etc., priority is given to the products that are approved by Evaluation and Certification/Validation Scheme under CCRA (Common Criteria Recognition Arrangement)[2] based on the Standards for Measures.

(b) Consideration for the introduction of a new system (function) contributing to security enhancement and its realization

Toward establishment of the next generation E-Government, it is essential to consider the construction/development of a common platform for the basis of operations and systems of the entire government. In order to strengthen the security platform, the government will consider a comprehensive way of installing a new system (function), such as an IPv6, IC card for identification of government officials, data encryption, electronic signature, and biometrics, etc., and promote the realization of the system.

Particularly, in order to expedite the use of IPv6 in the information system of all government agencies, information and telecommunications equipment and software will be made compatible to IPv6 in principle by fiscal 2008, in accordance with the new development (installation) or modification of information system of each government agency.

[Specific Measures]

A) Development of a discussion framework for the establishment of next generation E-Government (Cabinet Secretariat and Ministry of Internal Affairs and

[2] Evaluation and Certification/Validation Scheme under CCRA (Common Criteria Recognition Arrangement) is the system in which the security function and target level of security assurance of IT products and systems are evaluated by a third party based on ISO/IEC 15408, and the results are officially verified and made publicly available.

Communications)

A framework will be built in FY 2006 to conduct technical and functional considerations necessary for creating and developing a common platform which serves as a foundation of operations and systems of the entire government for the establishment of next generation E-Government.

B) Development of next generation OS environment to realize advanced security functions (Cabinet Secretariat, Cabinet Office, Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry)

While maintaining the environment for the existing OS and applications, development of a Virtual Machine (VM) will be promoted in FY 2006, which can intensively provide information security functions independent of the existing OS and applications environment, and a minimum level of OS functions to back up the operation of VM (hereinafter collectively referred to as "Secure VM") as a framework of urgency to ensure the reliability of IT through cooperation between industry, academia and government.

C) Establishment of evaluation criteria for the quality of OS security used for E-Government (Cabinet Secretariat and Ministry of Internal Affairs and Communications)

Discussions will take place in FY 2006 toward establishing evaluation criteria for the quality of OS security which supports information systems of E-Government, and efforts will be made to establish all the necessary evaluation items and criteria usable for system procurement. Technological survey will also be conducted in FY 2006 on the system installation of the OS and others toward a full-fledged launch of E-Government.

D) Transition to IPv6 of E-Government systems (Cabinet Secretariat, Ministry of Internal Affairs and Communications and all government agencies)

Considering that the use of IPv6 in E-Government is effective for strengthening security, such as protection against unauthorized computer access/information leakage in E-Government services, interactivation and establishment of a common inter-agency system, and also, from the perspective of preparation for the possibility of depletion of current IPv4 addresses as early as 2010, each government agency will make efforts to transfer its information and communications equipments and software to IPv6, in principle, by FY 2008, in accordance with the development (installation) or renewal of each information system. The following measures will be taken for a smooth implementation.

1) The Ministry of Internal Affairs and Communications will formulate guidelines for deploying IPv6 networks in E-Government in the first half of FY 2006, in principle.

2) Each government agency will consider the effects of the transition to IPv6 in each E-Government system based on the guidelines above, and will formulate specific plans on the transition to IPv6 in each information system, in principle by the end of FY 2006.

3) In order to allow IPv6 to be used for access by the general public to e-applications, Internet services providers need to cater IPv6 connection services to individual users. The Ministry of Internal Affairs and Communications will provide information pertaining to the availability of IPv6 connection services of the Internet service providers on the website in FY 2006.

E) Formulation of Guidelines for Authentication in E-Government (Cabinet Secretariat, Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry)

With respect to e-authentication whose methods are independently adopted by each e-administration service of government agencies, authentication levels will be sorted and clarified according to the risks involved, and the Guidelines for Authentication in E-Government (tentative) will be formulated in FY 2006 in order to promote cooperation between administrative services while maintaining safety.

(c) Prevention of spoofing as a government agency

In order to prevent a malicious third party from spoofing a government agency, inflicting damage to the people or private companies, etc., an extensive use of digital certification and use of domain names[3] that certify the identity of government agencies will be promoted to make the genuine government agencies easily identifiable.

[Specific Measures]

A) Promotion of the use of domain names that authenticate the identity of government agencies (Ministry of Internal Affairs and Communications and all government agencies)

Websites, for which the domain names that authenticate the identity of government agencies have not been used yet, will start using them, in principle, by September 2006.

Furthermore, each government agency will make efforts to disseminate information among the general public about the domain names that authenticate the identity of government agencies.

[3] Domain name that certifies the identity of government agency refers to “go.jp” among the organizational type jp domain name, or to the domain name reserved as the one associated with the administration and others among the Japanese domain names in the general use jp domain.

B) Prevention of spoofing and falsifying of e-mail sent by government agencies and e-documents downloaded from websites of government agencies (Cabinet Secretariat, Ministry of Internal Affairs and Communications and all government agencies)

In order to prevent spoofing and falsifying of e-documents of government agencies, discussions will commence in FY 2006 about the development of an environment where users such as the general public and private corporations are able to use e-documents reliably, by attaching e-signatures to e-mails sent by government agencies and e-documents downloaded through websites of government agencies: specifically, discussions on a unified specification for intra-government systems for setting up e-signatures.

(d) Promotion of the use of safe data encryption in government agencies

In order to ensure safety and reliability of E-Government, the safety of recommended cryptographic methods used by E-Government will continuously be monitored and studied and appropriate method of using data encryption will be considered in accordance with the advancement of technologies as well as international movements.

[Specific Measures]

A) Ensuring the safety of data encryption used by government agencies (Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry)

Monitoring of E-Government recommended ciphers, study and research for ensuring safety and reliance of the E-Government recommended ciphers, and formulation of standards will all be conducted in FY 2006.

B) Deliberations on the promotion system for the safe use of ciphers in government agencies (Cabinet Secretariat, Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry)

In FY 2006, deliberations will be made about ways, steps and implementation systems to be taken in case E-Government Recommended Ciphers are compromised, and at the same time, discussions will also commence about a promotion system within the government regarding the use of data encryption, including review of the nature of the E-Government Recommended Ciphers.

C) Promotion of the use of cryptographic modules that are highly safe and reliable (Ministry of Economy, Trade and Industry)

In order to promote the use of highly safe and reliable cryptographic modules[4], the Japan Information Technology Security Evaluation and Certification Scheme that is adopted by the Information-Technology Promotion Agency, Japan (IPA) will be expanded to newly develop a framework for cryptographic module authentication, followed by test operations in FY 2006.

D) Promotion of security measures for files (electronic documents) (Japan Defense Agency)

In FY 2006, production and installation of file protection software will be promoted in view of ensuring security at the time of data transfer to portable storage media.

4) Reinforcement of Governmental Capacity of Emergency Response to Cyber Attacks, etc.

Efforts are necessary to promptly and appropriately respond to emergencies, such as cyber attacks, and adapt to technology or environmental changes. Specific measures to that end are to promptly share information among the government bodies and analyze the information in an integrated manner, and at the same time, it is necessary to strengthen the response capacity by improving the capacity of related responding agencies, by developing a response systems, and by incorporating the knowledge obtained from the emergency responses in the past into the improvement of Standards for Measures or human resource development of the government, etc.

[Specific Measures]

A) Strengthening of functions for cross-sectoral solutions to cyber attacks against government agencies

a) Strengthening of functions for information gathering and analysis (Cabinet Secretariat)

In order to prevent the occurrence of cyber attacks against government agencies, information leakages and system malfunctions in government agencies, and to strengthen the function to gather and analyze cross-sectoral information in order to rapidly and accurately respond to the incidents, test monitoring of the web-servers of each government agency will start in FY 2006. Moreover, a function (tentatively named the “Analysis Scheme of the Public and Private Sectors”) will be established to conduct cross-sectoral analysis on attacks in cooperation with both national and international organizations. In doing so, use of state-of-the-art technologies developed by various institutions is encouraged.

[4] Cryptographic modules include hardware, software and firmware and their combinations, that are equipped with various cipher functions.

b) Strengthening of advisory function to other government institutions and mutual cooperation function (Cabinet Secretariat)

In order to contribute to the prevention of and response to IT-malfunctions in each government agency, an advisory function to the government agencies will be strengthened in FY 2006, based on the results of the analysis in the above-mentioned (a), and at the same time, comprehensive coordination will be facilitated to promote the exchange of response information among government agencies. In doing so, a liaison (coordinator), who acts as a nodal point of communication and response, will be designated at each government agency, and periodical meetings will be convened to exchange information.

c) Research and study of most advanced technologies for information assurance (Japan Defense Agency)

In order to secure the information assurance of information systems, the trend of cyber attacks and the most advanced countermeasure technologies against cyber attacks will be studied and researched, and studies will be performed on a centralized response system, etc., in FY 2006.

B) Strengthening of emergency response capability of each government agency

a) Establishment of an emergency response system in each government agency (Cabinet Secretariat)

A guide to initial responses taken by each government agency to rapidly and accurately respond to IT-malfunctions, and a draft of training specifications for the staff engaged in this system will be formulated in FY 2006.

b) Strengthening and development of a system concerning measures against cyber terrorism (National Police Agency)

In order to respond to the advancement of methods of cyber attacks which can be used in cyber terrorism, a system concerning measures against cyber terrorism taken by the police will be strengthened and developed in FY 2006, including implementation of training within and outside of the department to maintain and improve incident response capability and the skills of personnel to combat cyber terrorism.

c) Promotion of analysis/response and research concerning cyber attacks (Japan Defense Agency)

Considering the recent advancement of methods of cyber attacks, there is a need to upgrade analysis and response capability concerning countermeasures for cyber attacks against information systems of the Japan Defense Agency. Therefore, in FY 2006, basic research will be performed on monitoring and analyzing technology of unauthorized computer access, analysis technology of cyber attacks and active protection technology, etc.

5) Human Resource Development of Government Agencies

In order to proceed with information security measures of the entire government in an integrated manner and in view of the importance of development and securing of human resources with necessary knowledge and expertise, the government will promote the development of officials in charge of information system management of government agencies, utilization of human resources with expertise in information security, efforts in human resource development in cooperation with educational institutions, and the awareness raising of both executive and general officers. All officers specializing in information security operations in the information system management sections of government agencies will eventually obtain qualifications in information security.

[Specific Measures]

A) Deliberations concerning human resource development of government officials (Cabinet Secretariat and all government agencies)

Deliberations will be conducted concerning human resource development of government officials to promote information security measures in an integrated fashion, and basic policies and specific measures of the entire government to strategically develop human resources will be presented in FY 2006.

B) Deliberations on the method of human resource development with emergency response capability (Cabinet Secretariat)

Deliberations will be made to gather know-how on emergency response to IT-malfunctions to be reflected in human resource development strategies of each government agency, and basic policies and specific measures will be formulated in FY 2006 to strategically promote the strengthening of emergency response capability, from the human resource perspective, as the entire government.

C) Deliberations concerning the increase in the number of qualification holders of information security (Cabinet Secretariat and all government agencies)

In the departments in charge of information system management of government agencies, the situations of the qualification holders of Information Technology Engineers Examination, etc., will be surveyed, the future direction will be discussed, and specific measures to increase the number of qualification holders will be presented in FY 2006.

B: Local Governments

The government prioritized the promotion of the following measures in FY 2006, with the purpose of: (1) reviewing the Guidelines for ensuring the information security of local governments, hopefully in September 2006, and at the same time, monitoring and training of information security will be promoted, and (2) developing information sharing systems among local governments by the end of FY 2006.

1) Review of the guidelines for ensuring information security

Guidelines for ensuring information security of local governments will be reviewed, and at the same time, implementation of measures will be promoted based on the relevant guidelines in each local government.

[Specific Measures]

A) Promotion of formulation and review of information security policies of local governments (Ministry of Internal Affairs and Communications)

Guidelines for ensuring the information security of local governments will be reviewed, hopefully in September 2006, and at the same time, implementation of measures will be promoted based on the relevant guidelines in each local government.

B) Provision of evaluation tools for information security level (Ministry of Internal Affairs and Communications)

Evaluation tools will be provided to local governments in FY 2006 that will enable each local government to objectively evaluate its own information security level, set appropriate achievement goals, and implement measures for protecting personal data and information security in a planned and phased manner.

2) Promotion of information security auditing

With respect to information security measures implemented by each local government, information security auditing will be promoted in order to contribute to the continuous improvement to the level of measures through evaluation and review of their effectiveness.

[Specific Measures]

A) Promotion of implementation of information security auditing by local governments (Ministry of Internal Affairs and Communications)

In order to contribute to constant improvement of the level of information security measures taken by each local government through evaluation and review of effectiveness, information security auditing will be promoted in FY 2006.

3) Promotion of establishment of "Information Sharing and Analysis Center of Local Government" (tentative)

In order to contribute to preemptive prevention of IT-malfunctions and its expansion, prompt resumption and prevention of recurrence and to improve the security level of all local governments, the government will promote the establishment of "Information Sharing and Analysis Center of Local Government" (tentative). The Center will have functions of gathering, analyzing and sharing of information on security of local governments and sharing of information provided by the central government and others.

[Specific Measures]

A) Promotion of establishment and support for operation of Information Sharing and Analysis Center of Local Government (tentative) (Ministry of Internal Affairs and Communications

In order to contribute to preemptive prevention, prevention of expansion of suffering and prevention of recurrence of IT-malfunctions, and prompt resumption from IT-malfunctions, and to upgrade the level of information security of the local government, test operations will be performed on the Information Sharing and Analysis Center of Local Government (tentative) that serves the function of gathering, analyzing and sharing information on information security of local governments, sharing of information provided from the central government and others, and developments of the Center will be promoted by the end of FY 2006 and necessary support for operations will be provided.

4) Support for training of officers, etc.

In addition to the above, the government will support the development and introduction of advanced technologies and staff training, etc., in efforts to try to strengthen the security of local governments.

[Specific Measures]

A) Development and verification of technologies for protecting personal data and information security measures taken by local governments (Ministry of Internal Affairs and Communications)

Development and verification of cutting edge technologies that lead to the strengthening of protection of personal data and information security measures taken by local governments will be performed in FY 2006.

B) Implementation of information security training for local government officials (Ministry of Internal Affairs and Communications)

Training for local government officials will be supported in FY 2006, including training to develop human resources with advanced knowledge and skills who would play a central role in information security measures, as well as training for a wide range of personnel engaged in various local government functions.

Section 2: Critical Infrastructures

Aiming at reducing the number of IT-malfunction in critical infrastructures as close as possible to zero by the beginning of FY 2009, the government separately sets forth information security measures for critical infrastructures in the Action Plan on Information Security Measures for Critical Infrastructures (decision made on December 13, 2005 by the ISPC), and the following measures will be primarily promoted in FY 2006.

1) Improvement of "Safety Standards" on information security assurance for critical infrastructures

Based on the "A Principle for Formulating of 'Safety Standards, Guidelines, etc.'[5] concerning Assurance of Information Security of Critical Infrastructures"[6] , the level of necessary or desirable information security in each critical infrastructure sector will be stipulated in the Safety Standards, Guidelines, etc.. The guidelines will be reviewed annually or whenever necessary, and Safety Standards, Guidelines, etc. will be reviewed on an as-needed basis in accordance with changes in environment surrounding information security.

[Specific Measures]

A) Formulation and review of "Safety Standards, Guidelines, etc." in each sector of critical infrastructures

a) Formulation and review of "Safety Standards, Guidelines, etc." (Agencies surrounding critical infrastructures[7])

Aiming for September 2006, efforts will be made to clarify the necessary or desirable level of information security measures for "Safety Standards, Guidelines, etc." in each sector of critical infrastructures, based on "A Principle for Formulating of 'Safety

[5] "Safety Standards, Guidelines, etc." refer to documents formulated as criteria or references used by business entities engaged in critical infrastructures for making various decisions and actions.

[6] "A Principle for Formulating of 'Safety Standards, Guidelines, etc.' concerning Assurance of Information Security of Critical Infrastructures" (decision made on February 2, 2006 by the ISPC)

[7] "Agencies surrounding critical infrastructure" refer to ministries and agencies that directly deal with Business entities engaged in critical infrastructures in accordance with laws and regulations (according to the definition in the Section 1, "Purpose and Scope" of the Action Plan on Information Security Measures for Critical Infrastructures) (decision made on December 13, 2005 by the ISPC: the same hereinafter))

Standards, Guidelines, etc.' concerning Assurance of Information Security of Critical Infrastructures" (hereinafter referred to as the "Principle"). In doing so, the release of guidelines for improving the reliability of information system shall be used as a reference.

b) Development of Safety Standards in the area of telecommunications (Ministry of Internal Affairs and Communications)

In accordance with the Action Plan on Information Security Measures for Critical Infrastructures, the Safety Standards will be developed by the end of September 2006, in cooperation with the Information Security Conference on Telecommunications (ISeCT), which is comprised of telecommunications operators, telecom industry bodies, etc. Consequently, the Safety Standards is expected to contribute to strengthen information security measures taken in the area of telecommunications.

B) Understanding and evaluation of the formulation process of Safety Standards, etc. (Cabinet Secretariat)

The formulation process of the "Safety Standards, Guidelines, etc." will be monitored in cooperation with the agencies surrounding critical infrastructure, and evaluation of the "Safety Standards, Guidelines, etc." will be implemented while considering the implementation of interdependency analysis in FY 2006.

C) Review of the Principles (Cabinet Secretariat)

Through constantly following the occurrence of IT-malfunctions, cross-sectoral issues of measures that are common to the sector of critical infrastructures will be analyzed and examined. At the same time, the guidelines will be reviewed, hopefully within FY 2006, in cooperation with the agencies surrounding critical infrastructure, using Standards for Measures and other related documents as a reference.

2) Enhancement of information sharing system

The government and other entities will provide information concerning IT-malfunctions to business entities engaged in critical infrastructures in a timely and appropriate manner, and will enhance the information sharing system among the business entities engaged in critical infrastructure sector and among the interdependent critical infrastructure sectors. This is in view of the following aspects: 1) preemptive prevention of IT-malfunctions, 2) prevention of expansion of suffering, and rapid resumption, and 3) prevention of recurrence through analysis/verification of causes of IT-malfunctions.

(a) Development of an environment for information provision/connection between public and private sectors

In cooperation among related organizations, information, such as caution, to be provided to business entities engaged in critical infrastructures to contribute to the measures taken by them will be collected and provided through CEPTOAR (to be hereinafter described), etc..

The government will promote the development of an environment in which business entities engaged in critical infrastructures provide the government with information on incidents, failures, and operational delays, etc., to be submitted under laws and regulations, as well as with unique and crucial information deemed to be disclosed to the government.

[Specific Measures]

A) Development of information sharing systems and strengthening of functions (Cabinet Secretariat)

Information provided by the business entities engaged in critical infrastructures and information collected from central government agencies concerning information security[8], incident response relevant agencies[9], and related organizations will be analyzed, and the information will be appropriately provided to the agencies surrounding critical infrastructure and business entities engaged in critical infrastructures. Furthermore, the competent agency will develop an environment for the operation of the central functions[10] in FY 2007 to coordinate necessary responses to emergency situations among concerned parties.

B) Strengthening of systems for information provision/communications (Agencies surrounding critical infrastructures)

Based on the Detailed Rules on Information Provision/Connection[11] (tentative) formulated by the Cabinet Secretariat, a system will be enhanced to transfer the information to the Cabinet Secretariat that has been sent from business entities engaged in critical

[8] Central government agencies concerning information security refer to the National Police Agency, Japan Defense Agency, Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry.

[9] Incident response relevant agencies refer to the National Police Agency, Japan Defense Agency, Fire and Disaster Management Agency, Japan Coast Guard, etc.

[10] Central functions refer to a center with functions for coordinating communication among business entities engaged in critical infrastructures in the occurrence of IT-malfunction emergency: “Action Plan on Information Security Measures for Critical Infrastructures” (Section 7 “Issues to be addressed by each entity and entity cross-sectoral measures (1) B. 3))

[11] “Detailed Rules on Information Provision/Connection” (tentative) refer to “Detailed Rules on Information Provision/Connection under the ‘Action Plan on Information Security Measures for Critical Infrastructures’”

infrastructures through liaisons designated in the agencies surrounding critical infrastructure. The system will also be strengthened to provide information that has been sent from the Cabinet Secretariat through CEPTOAR to the business entities engaged in critical infrastructures. To that end, the liaisons (concurrently served by the Cabinet Secretariat) will be deployed as early as possible, who are responsible for the information sharing system established by the Cabinet Secretariat under appropriate information management.

(b) Development of CEPTOAR (Capability for Engineering of Protection, Technical Operation, Analysis and Response) in each critical infrastructure

Information provided by the government for preemptive prevention of IT-malfunctions, prevention of expansion of suffering and rapid resumption, and prevention of recurrence will be appropriately made available to business entities engaged in critical infrastructures and will be shared among them. This will eventually contribute to the upgrading of capacity to maintain and reconstruct services of each business entities engaged in critical infrastructures. In order to serve this purpose, the government will promote the development of Capability for Engineering of Protection, Technical Operation, Analysis and Response (CEPTOAR) within each critical infrastructure sector.

[Specific Measures]

A) Promotion of the development of CEPTOAR

a) Promotion of the development of CEPTOAR in each critical infrastructure (Agencies surrounding critical infrastructures)

Discussions will be launched between agencies surrounding critical infrastructures and business entities engaged in critical infrastructures, and the government aims at developing CEPTOAR in each critical infrastructure by the end of FY 2006. In newly added sectors (water works, medical services, and logistics), the government aims to reach a basic agreement between agencies surrounding critical infrastructures and business entities engaged in critical infrastructures by the end of FY 2006.

b) Strengthening of a system for sharing and analyzing security-related information in the area of telecommunications (Ministry of Internal Affairs and Communications)

In accordance with the Action Plan on Information Security Measures for Critical Infrastructures, CEPTOAR will be built up by the end of FY 2006, in cooperation with ISeCT (mentioned in Chapter 2, Section 2 A). Consequently, CEPTOAR is expected to contribute to strengthening the system for sharing and analyzing security-related information in the area of telecommunications.

B) Compilation of a “Map for Understanding the Characteristics of CEPTOAR” (tentative) (Cabinet Secretariat)

In cooperation with agencies surrounding critical infrastructures, the competent agency will follow the development process of each CEPTOAR established in each critical infrastructure sector, and at the same time, will grasp the functional characteristics by different business types, which reflect the nature of the business in each sector, and compile a “Map for Understanding Characteristics of CEPTOAR” (tentative) with visual devices, which would facilitate the ease of understanding of the characteristics, hopefully by the end of 2006.

(c) Promotion of establishment of “CEPTOAR-Council (tentative)”

In order to promote cross-sectoral information sharing among business entities engaged in critical infrastructures and utilize knowledge for maintenance and resumption of services, the government will promote the establishment of “CEPTOAR-Council (tentative)” as an instrument for cross-sectoral information sharing among each CEPTOAR.

[Specific Measures]

A) Discussions on establishment of CEPTOAR-Council (tentative) (Cabinet Secretariat)

The competent agency will establish a discussion forum comprising representatives of CEPTOAR (scheduled to be established within FY 2006) in cooperation with the Agencies surrounding critical infrastructures and business entities engaged in critical infrastructures.

3) Implementation of analysis of interdependence

In order to grasp the cross-sectoral situation toward improving critical infrastructure measures throughout the entire nation, the government will make efforts to get a grip of what the potential threats are in each critical infrastructure and of interdependence as to what impact will ripple through other critical infrastructures when an IT-malfunction occurs in a critical infrastructure.

[Specific Measures]

A) Pilot analysis of interdependency (Cabinet Secretariat)

Based on the study results of analysis methods conducted in FY 2005, the government, in cooperation with the agencies surrounding critical infrastructures, will establish a framework in FY 2006, which allows visualization of interdependent relations (static analysis of interdependency), and will perform pilot analysis of interdependency, while giving due consideration to the characteristics and situations of each critical infrastructure.

4) Implementation of cross-sectoral exercises

Based on a stereotype of a specifically envisioned threat scenario, cross-sectoral exercises will be performed under cooperation among presiding ministries of each critical infrastructure, each business entities engaged in critical infrastructures and CEPTOAR in each infrastructure sector. Through the exercises, effectiveness and propriety of each measure, such as safety standards, guidelines, etc., an information sharing frameworks, functions for information sharing and analysis, analysis of interdependency, will be periodically evaluated in stages. Furthermore, through these exercises and other training and seminar sessions, personnel with advanced IT skills will be developed and secured, primarily for presiding ministries of each critical infrastructure and business entities engaged in critical infrastructures.

[Specific Measures]

A) Implementation of “the exercises for research” (Cabinet Secretariat and agencies surrounding critical infrastructures)

Aiming to set up the concept of exercises and exercise tasks, and to understand the method, the competent agencies will carry out exercises involving a study group (“the exercises for research”) in FY 2006, while giving consideration to the characteristics and situations of the critical infrastructure sector.

B) “The Tabletop Exercise”[12] (Cabinet Secretariat and agencies surrounding critical infrastructures)

The competent agencies will conduct “The Tabletop Exercises” in FY 2006 on a group of similar businesses or on a group of common themes applicable to the critical infrastructure sector in order to clarify the key points of discussions and identify specific tasks.

C) Efforts for strengthening responses in each critical infrastructure

a) Exercise for cyber attacks in the telecommunications field (Ministry of Internal Affairs and Communications)

By the end of FY 2008, aiming at strengthening cooperation in case of emergency, among concerned operators, and between operators and governments; and developing human resources with advanced IT skills to exercise regulatory functions; the competent agencies will conduct exercises in FY 2006 simulating cyber attacks that may disrupt

[12] “The Tabletop Exercise” refers to exercise in which participants discuss a certain scenario in conference format.

communications networks across critical infrastructures, with focus on telecommunications operators.

D) Coordination with cyber exercises conducted in each sector (Cabinet Secretariat and agencies surrounding critical infrastructures)

The competent agencies will start discussions within FY 2006 about coordination between the cyber exercises conducted in each sector, such as telecommunications and electricity, etc., and the exercises implemented by the Cabinet Secretariat, while giving consideration to the forms of exercises and consistency with the objectives

Section 3: Businesses

Aiming at bringing the implementation of information security measures of businesses up to the world’s top level by the beginning of FY 2009, the government prioritizes the promotion of the following measures in FY 2006.

1) Development of an environment that will link information security measures of businesses to market valuation

The government will promote the establishment and operation of corporate governance with consideration for corporate social responsibility and an internal control framework that supports the governance from the perspective of information security. To that end, efforts will be made to disseminate and improve the Information Security Measures Benchmark, Information Security Report Model, and Guidelines for Formulating a Business Continuity Plan. Furthermore, evaluation on the level of information security will be made one of the conditions for public bidding for information system, etc., if necessary. The evaluation will be able to use, for example, the said systems or third party evaluation results. In addition, consistency of the government’s approach concerning information security will be ensured.

[Specific Measures]

A) Promotion of the establishment of Information Security Governance (ISG)

a) Establishment of Information Security Governance (ISG) in corporations, etc. (Ministry of Economy, Trade and Industry)

In order to establish ISG in corporations, efforts will be made to disseminate the Information Security Measures Benchmark, Information Security Report Model, and Guidelines for Formulating a Business Continuity Plan in FY 2006. In addition, as required, these tools will be reviewed and new measures to establish ISG will be examined.

Furthermore, the competent agency will launch campaigns in FY 2006 to encourage each corporation to refer to the “Guidelines for Improving Reliability of Information Systems” when establishing and operating information systems.

b) Strengthening of information security management in telecommunications services (Ministry of Internal Affairs and Communications)

The competent agency will formulate Information Security Management Guideline for Telecommunications (ISM-TG) in FY 2006 in cooperation with operators and operators’ associations, to contribute to the establishment and management of the information security systems of telecommunications operators.

B) Review of bidding conditions (Cabinet Secretariat, Ministry of Internal Affairs and Communications and Ministry of Finance and all government agencies)

Discussions will be commenced and brought to conclusion within FY 2006 on evaluation of the information security levels required for bidders as bidding conditions.

C) Ensuring consistency between information security-related systems and internal control systems (Cabinet Secretariat, Ministry of Finance and Ministry of Economy, Trade and Industry)

In order to ensure the consistency of the information security measures promoted by the government within the entire government, measures will be examined in FY 2006 regarding information security-related issues under IT control of the internal control systems, whose establishment is currently under consideration, while giving consideration to the relationship with information security-related systems, such as the existing standards of measures.

2) Promotion of the provision of high quality products and services related to information security

The information security measures have characteristics that their functions different from original business are to be implemented according to risks, the measures themselves are hard to visualize, etc. Due to these characteristics, it is necessary to create an environment so that businesses are able to easily choose necessary measures to implement. To that end, the government will make efforts to promote the provision of high quality products and services related to information security through the promotion of the use of third party evaluations, such as IT security evaluation and certification system, the Compatibility Assessment System for Information System Management Systems (ISMS), information security audits, in addition to the promotion of study on quantitative evaluation technique for information security-related risks of businesses.

The government will also make efforts to streamline the evaluation of third parties and to promote an environment so that there are incentives to accelerate the investment in businesses which utilize high quality information security-related products, etc.

[Specific Measures]

A) Research on quantitative evaluation techniques for information security related risks (Ministry of Economy, Trade and Industry)

In order to visualize the information security measures of corporations, research studies will be performed within FY 2006 for quantifying risks associated with information security.

B) Promotion of the use of third party evaluation

a) Promotion of dissemination of the Conformity Assessment Scheme for Information Security Management Systems (Ministry of Economy, Trade and Industry)

In order to develop an environment that supports appropriate evaluation on the level of information security of organizations when conducting domestic and international business, campaigns will be organized in FY 2006 to disseminate the Conformity Assessment Scheme for Information Security Management Systems.

b) Promotion of dissemination of the Information Security Auditing System (Ministry of Economy, Trade and Industry)

In order to develop an environment that supports appropriate evaluation on the level of information security of organizations when conducting domestic and international business, discussions will be conducted in FY 2006 about viable standards for providing high quality audit services that meet various needs.

c) Promotion of standardization of information security management (Ministry of Economy, Trade and Industry)

JISQ 27001 (Information technology -- Security techniques -- Information security management systems -- Requirements) (=ISO/IEC 2700) and JISQ27002 (Information technology – Security techniques – Code of practice for information security management) (=ISO/IEC17799) will be established in FY 2006 as the standards for effectively establishing, introducing, managing, monitoring, maintaining and improving the information security management systems of organizations.

d) Streamlining of third party evaluation and promotion of dissemination of high quality information security-related products (Ministry of Economy, Trade and Industry)

With regard to the IPA, the Common Criteria (CC) Ver.3-based operations will commence in July 2006, which is a new standard to facilitate the improvement of operation of the Program.

C) Preferential tax treatment

a) Preferential tax treatment for acquiring information security equipments (Ministry of Internal Affairs and Communications)

Preferential tax treatment will be provided in FY 2006 when corporations and sole proprietors acquire information security equipments under certain conditions.

b) Preferential tax treatment for investing in information systems that provide highly advanced information security to corporations (Ministry of Economy, Trade and Industry and Ministry of Internal Affairs and Communications)

The competent agencies will promote investment in information systems that provide highly advanced information security in FY 2006 through dissemination and PR activities of the tax system for strengthening the information infrastructure for industrial competitiveness.

3) Securing/Development human resources engaged in information security of businesses

Understanding of top management about information security and human resource engaged in information security within businesses are still insufficient. Therefore, the government will make efforts to increase understanding of top management about information security through improvement of the environment in which information security measures of businesses are linked with market valuation, and to promote nationwide PR activities for personnel in charge of information systems. Furthermore, more efforts will be expended to maintain motivation of personnel in charge of information security measures in each company.

[Specific Measures]

A) Support for training activities to develop human resources in information and telecommunications security (Ministry of Internal Affairs and Communications)

The competent agency will support the establishment of a human resource development center to provide multi-dimensional, bi-directional and practical approaches to attacks on and illicit intrusions into information and communications network systems in FY 2006. Support will also be provided for training activities to develop human resources, including security personnel who have professional knowledge and expertise in the area of information and telecommunications.

B) Training of experts in information security (Ministry of Economy, Trade and Industry)

The competent agency will discuss the nature of human resource development for information security in corporations and universities in FY 2006, and commence deliberations on indices to objectively measure the level of information security measures for IT users in organizations.

C) Holding of information security seminars for small- and medium-sized enterprises (Ministry of Economy, Trade and Industry)

In order to deepen understanding of information security among owners of small- and medium-sized enterprises and information system personnel, the scale of the “Information Security Seminar,” co-hosted by IPA and the Japan Chamber of Commerce and Industry, will be expanded and the content will be further enhanced in FY 2006.

4) Strengthening systems to rapidly respond to computer viruses and vulnerability, etc.

In order to appropriately respond to information security issues of businesses, it is necessary to make efforts to achieve rapid information sharing, and smooth formulation and dissemination of measures among concerned parties, including information-related businesses. To that end, the government will set up a communication system and enhance a coordinated response system to rapidly respond to computer viruses or vulnerabilities, etc, with proactive cooperation of information-relate businesses.

[Specific Measures]

A) Strengthening of the Information Security Early Warning Partnership (Ministry of Economy, Trade and Industry)

In order to ensure rapid information sharing among concerned parties, and smooth response to security issues that evolve to be more sophisticated on a daily basis, such as computer viruses, unauthorized computer access, and vulnerability, etc., the competent agency will enhance the “Information Security Early Warning Partnership” implemented by IPA and the Japan Computer Emergency Response Team/Coordination Center (JPCERT/CC) in FY 2006.

B) Deliberations on standards required for safe websites (Ministry of Economy, Trade and Industry)

In order to ensure the safety of websites, the competent agency will commence deliberations in FY 2006 on standards regarding security requirements to be presented by the consigners to the developers (consignees) when creating web applications.

Section 4: Individuals

Aiming at reducing the number of individuals who feel insecure about using IT to as close as possible to zero by the beginning of FY 2009, the government will intensively promote the following measures in FY 2006.

When promoting the specific measures of 1) and 2), it is important to develop an environment where an individual considers information security as a must within the scope of their ability, and to conduct PR activities and send messages in an understandable way for the general public. Thus the Cabinet Secretariat and the relevant agencies will closely cooperate with each other while maintaining consistency.

1) Enhancement/promotion of information security education

The government will promote information security education from primary and secondary schools and inter-generation information security education.

[Specific Measures]

A) Promotion of information security education from primary education

a) Promotion of information security education at primary and middle schools (Ministry of Education, Culture, Sports, Science and Technology)

In order to promote information education for children and students, including information security, the competent agency will further improve the teaching ability of teachers in FY 2006 by collecting cases concerning effective teaching methods and conducting dissemination forums to raise awareness.

b) Research and development of methods to foster ICT media literacy[13] (Ministry of Internal Affairs and Communications)

In order to promote appropriate use by children of ICT media such as the Internet and mobile phones, the competent agency will conduct research and development activities on new methods to foster ICT media literacy, such as the development of instruction manuals and teaching materials concerning comprehensive literacy required for the use of ICT media in FY 2006, and the dissemination and PR activities will be conducted in FY 2007.

[13] ICT media literacy refers not only to the ability to access and use ICT media, but also to the ability to understand the characteristics of each ICT medium and actively select transmitted information, and the ability to create communication through ICT media.

c) Dissemination and PR activities using slogans for information security measures (Ministry of Economy, Trade and Industry)

In FY 2006, in order to contribute to reducing the damage by computer viruses or hacking, the IPA will solicit slogans for raising awareness on information security measures from students of primary, middle and high schools and publicize the winners' works.

B) Promotion of cross-generational information security education

a) Implementation of nation-wide activities for dissemination and PR (Ministry of Economy, Trade and Industry and National Police Agency)

While improving and enhancing the contents of the "Internet Safety Class", by methods such as reflecting the trends of new threats, the competent agency will disseminate basic knowledge on the information security of general users in FY 2006 by continually holding such classes throughout the country.

b) Implementation of e-net caravan (Ministry of Internal Affairs and Communications and Ministry of Education, Culture, Sports, Science and Technology)

Caravan courses for campaigns about safe and secure use of the Internet, primarily targeting guardians and teachers, will be conducted on a national scale in FY 2006, in cooperation with telecommunications-related organizations.

2) Enhancement/promotion of PR activities/information transmission

The following efforts will be promoted: continuous implementation of nationwide PR activities and information transmission; holding of events recognized as landmarks (creation of "Information Security Day", etc.), establishment of a framework of the routine campaigns/information provisions (consideration of implementation of Information Security Forecast (tentative)), dissemination of National Strategies on information security of Japan both nationally and internationally.

[Specific Measures]

A) Continual implementation of nation-wide promotions and PR campaigns

a) Promotion of dissemination and PR activities (Cabinet Secretariat, National Police Agency, Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry)

In order to raise the awareness of the people about information security, based on the reality of rapidly advancing and complicating threats to information security, the competent agencies will actively provide each individual with appropriate information, and implement promotions and PR activities using media, etc. in FY 2006, through such approaches as "*@police,*" "Information Security Website for the Public," "Antiphishing Japan," and "Council for Promoting Measures against Phishing," etc.

b) PR for prevention of unauthorized computer access and dissemination of knowledge (National Police Agency, Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry)

Based on the Unauthorized Computer Access Law, the competent agencies will conduct campaigns and disseminate knowledge about unauthorized computer access in FY 2006 through such approaches as disclosure of the occurrence of unauthorized computer access and the progress of research and development for access control functions.

c) Promotion of preventive measures against damage from improper Internet use (National Police Agency)

In order to prevent damages from cybercrime, the competent agency will accept information pertaining to cybercrimes, and efficiently implement PR campaigns in FY 2006 by effectively using a network consultation system.

d) Strengthening of dissemination and PR activities to maintain stable utilization of radio waves (Ministry of Internal Affairs and Communications)

With the advent of ubiquitous society, the use of wireless broadband services is becoming inevitable, and the need for protecting the environment in which one can use radio waves safely and securely is rapidly increasing.

Thus, promotion of purchasing and using appropriate radio equipments is becoming more important in order to maintain stable utilization of radio waves, including prevention of radio interference and jamming. In order to create an environment where people are able to purchase and use radio equipments safely, the competent agency will implement dissemination and PR activities in FY 2006 to encourage people to check the "label to verify the compliance with technology standards", which is attached to the radio equipments, through the use of mass media, posters and Internet throughout the nation.

B) Implementation of landmark events

a) Establishment of "Information Security Day" (Cabinet Secretariat, National Police Agency, Ministry of Internal Affairs and Communications, Ministry of Education, Culture, Sports, Science and Technology and Ministry of Economy, Trade and Industry)

To promote fostering of the awareness of the people about information security, the competent agencies will establish "Information Security Day" in FY 2006, and undertake nation-wide PR activities on the occasion of the Day. Along with this, the competent agencies will establish a system to recognize the contributions of individuals, corporations, local governments, and educational and research institutions, etc.

C) Establishment of a framework to rouse public opinion and information provision on a daily basis

a) Rouse of public opinion and information provision on a daily basis (Cabinet Secretariat)

In order to rouse public opinion and provide information pertaining to information security on a daily basis, the competent agency will issue e-mail magazines and establish an information security portal site of the entire government.

E-mail magazines will be published as early as possible in FY 2006 and will be distributed on a more than once a month basis. The information security portal site will be available within FY 2006.

b) Establishment of Information Security Award (tentative) (Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry)

In order to recognize the contribution of individuals and corporations and others to information security, an Information Security Award (tentative) will be established in FY 2006. In doing so, consideration will be given to consistency with the ‘Establishment of “Information Security Day”’ (Chapter 2, Section 4 B-(a)).

D) Dispatch of a message, both within and outside the country, about Japan’s basic policies for information security

a) Dispatch of a message about Japan’s information security strategies both within and outside the country (Cabinet Secretariat)

Using PR media such as websites and advertisement, etc., the competent agency will actively send a message about Japan’s information security strategies both within and outside the country.

Specifically, an English website of the National Information Security Center (NISC) will be launched in FY 2006 to make the English version of the First National Strategy on Information Security available online.

3) Promotion of an environment in which individuals are able to use information-related products and services without much burden

The government will promote an environment where information-related businesses can develop and supply products and services ("Information Security Universal Design") which individuals can use without much burden while enjoying highly advanced information security functions.

[Specific Measures]

A) Establishment of a framework to block cyber attacks (Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry)

In order to make measures available to prevent infections by computer viruses (i.e. bot programs), which enable malicious third parties to carry out cyber attacks by remote operations, and to rapidly and effectively block spam mails and cyber attacks from entering through bot-infected computers without imposing too much burden on individual users, discussions, including the technical and practical aspects, will commence in FY 2006 with an aim to establish a comprehensive framework by FY 2010.

B) Ensuring security toward creating ubiquitous environment by IPv6 (Ministry of Internal Affairs and Communications)

Aiming for deploying an IPv6 compatible ubiquitous security support system[14] by FY 2009, empirical experiments, which model the user environment, will start in FY 2006 to solve the issues associated with security assurance toward creating a ubiquitous environment by IPv6.

C) Security measures for wireless LAN (Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry)

In FY 2006, the competent agencies will further promote dissemination of the guidelines entitled "For Safe Use of Wireless LAN" and at the same time, the contents of pamphlets and handouts concerning the safe use of wireless LAN, such as the pamphlet on the "Internet Safety Class", will be improved.

[14] IPv6 compatible ubiquitous security support system is the system supporting the complex security measures installed in a considerable number of ubiquitous devices, not only from the users' side, but also from the side of the Internet network.

Chapter 3: Formation of Cross-Sectoral Information Security Infrastructure

To promote the formation of awareness as to for what purpose and to what degree of risk each entity will take for which information security measures, and to maintain continuous and rigid information security measures of the public and private sectors, it is necessary to construct an infrastructure of the whole society as its basis. To that end, the government is required to comprehensively address policies from the perspectives of the promotion of strategies concerning information security technology, development and securing of human resources engaged in information security, promotion of international partnership and cooperation, crime control, and protection and redemption of rights and interests.

Section 1: Promotion of Strategy concerning Information Security Technology

With a clear division of the roles in efforts between the government and private sector, the government will intensively take the following measures as technological strategies regarding information security in FY 2006.

1) Establishment of an implementation system effective for research and development (R&D) and technology development

In order to implement R&D and technology development effectively and efficiently with limited investments, the government will try to grasp the current situations and conduct periodical reviews of R&D and technology development of information security of Japan. Furthermore, in order to improve investment efficiency, the government will establish a system to perform R&D and technology development, keeping in mind the use of outcomes, and to launch new R&D and technology development efforts on the premise of outcomes being used by the government.

[Specific Measures]

A) Grasp of the implementation progress and continuous review (Cabinet Secretariat and Cabinet Office)

The ISPC, in cooperation with the Council for Science and Technology Policy, will commence discussions in FY 2006 to grasp the implementation progress of R&D and technology development relating to the information security of Japan through cooperation between industry, academia and government.

B) Introduction of continuous assessment on effects of investment (Cabinet Secretariat and Cabinet Office)

The ISPC, in cooperation with the Council for Science and Technology Policy, will commence assessments (1:ex-ante, 2:mid-term, and 3:ex-post) on the effects on investment in R&D and technology development relating to information security technologies in FY 2006, and results will be promptly made available.

C) Discussions on policies on the use of outcomes for government procurement (Cabinet Secretariat and all government agencies)

The competent agencies will commence discussions in FY 2006 about policies as to how the government can maximize the direct use of outcomes of R&D and technology development of information security through procurement.

2) Prioritization of information security technology development and improvement of the environment

In order to advance information security technology and upgrade the organizational/human resource management methods, the government will promote R&D and technology development to achieve mid and long-term objectives that are tied to enhancement of IT infrastructure. At the same time, with respect to R&D and technology development for which short term objectives have been laid out, the government will evaluate the investment efficiency and inject a well-balanced investment. The government will take an active role as an incubator for emerging R&D programs for which efforts of the private sectors are not expected although high investment efficiency is predicted.

[Specific Measures]

A) Measures of mid- and long-term R&D and technology development

a) Promotion of R&D and technology development to achieve mid- and long-term objectives (Cabinet Secretariat, Cabinet Office, National Police Agency, Japan Defense Agency, Ministry of Internal Affairs and Communications, Ministry of Education, Culture, Sports, Science and Technology and Ministry of Economy, Trade and Industry)

In relation to the objectives that are directly linked with the strengthening of IT as an infrastructure, the competent agencies will conduct discussions to give priorities to the investment of public research funds, and basic policies and specific measures will be presented in 2006.

b) Research and development of Next Generation Backbone (Ministry of Internal Affairs and Communications)

With an aim to develop technologies that enable safe operation of the entire IP[15] by detecting and controlling abnormal traffic that would never occur in normal networking, the competent agency will promote research and development of a Next Generation Backbone in FY 2006.

c) Research and development on detection of, recovery from and prevention of route hijacks[16] (Ministry of Internal Affairs and Communications)

Aiming to develop technology that enables detection of and recovery from route hijacks within a few minutes, and to establish technology that enables the prevention of route hijacks by FY 2009, the competent agency will launch research and development on the detection of, recovery from and prevention of route hijacks.

d) Research and development on information security technologies in the area of information and telecommunications (Ministry of Internal Affairs and Communications)

In order to further improve information security, the competent agency will undertake research and development in FY 2006 on security technologies to ensure the safety and reliability of the network itself and information that runs through the network, and comprehensive technologies that ensure the security of information, as well as technologies that facilitate immediate and accurate access to disaster prevention and disaster alleviation information without being disconnected in case of major disaster.

e) Research and development of next generation access control technology (Ministry of Economy, Trade and Industry)

The competent agency will implement research and development in FY 2006 of next generation access control technology, authentication technology and software technology that are not bound to conventional technologies founded on the existing information systems.

f) Development of information processing and management technologies to achieve flexible and accurate information management (Ministry of Economy, Trade and Industry)

The competent agency will implement research and technology on information security technologies in FY 2006 with the purpose of enabling the owner/controller of information to justify the disclosure of the information and to determine the scope of the disclosed

[15] IP Backbone generally refers to backbone communication lines of the Internet protocol connecting relay facilities of telecommunications operators with each other.

[16] Route hijack is a communication failure that occurs when incorrect route data spreads through the network, in which routers of each Internet service provider have and exchange route data to establish communication routes.

information by himself/herself, and ensuring the disclosure.

g) Research and development on fail-safe technology of information security (Ministry of Economy, Trade and Industry)

Based on the premise that incidents may happen, the competent agency will conduct research and development activities in FY 2006 for the design and development of software based on the fail-safe concept, so that an adequate level of safety can be attained in case of actual system failure or some information leakage, rather than just simply protecting the information or system.

h) Research and development on risk quantification methods for information security (Ministry of Economy, Trade and Industry)

In order to advance the method of management relating to organizations and personnel, the competent agency will conduct research and development on risk quantification for information security in organizations, and on the measurement of cost efficiency of information security management in FY 2006.

B) Measures for short-term R&D and technology development

a) Discussions on improving the investment balance in R&D and technology development with short-term goals (Cabinet Secretariat, Cabinet Office, National Police Agency, Japan Defense Agency, Ministry of Internal Affairs and Communications, Ministry of Education, Culture, Sports, Science and Technology and Ministry of Economy, Trade and Industry)

With regard to R&D and technology development with short-term goals, such as improvement of existing technologies and development of operational technologies, etc., discussions will be conducted to understand the progress of efforts made by the public and private sectors, and to elaborate coordination of the investment portfolio to avoid under-investment or excess investment in various areas, and specific measures will be presented in FY 2006.

b) Development of next generation OS environment to realize advanced security functions (Cabinet Secretariat, Cabinet Office, Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry) [Reprise]

While maintaining the environment for the existing OS and applications, development of a VM will be promoted in FY 2006, which can intensively provide information security functions independent of the existing OS and applications environment, and a minimum level of OS functions to back up the operation of VM as a framework of urgency to ensure the reliability of IT through cooperation between industry, academia and government.

c) Establishment of evaluation criteria for the quality of OS security used for E-Government (Cabinet Secretariat and Ministry of Internal Affairs and Communications) [Reprise]

Discussions will take place in FY 2006 toward establishing evaluation criteria for the quality of OS security which supports information systems of E-Government, and efforts will be made to establish all the necessary evaluation items and criteria usable for system procurement. Technological survey will also be conducted in FY 2006 on the system installation of the OS and others toward a full-fledged launch of E-Government.

d) Strengthening of industry-universities-governments partnerships toward the establishment of Digital Forensics area[17] (National Police Agency)

Research studies on the Digital Forensics area by the Police will be promoted and information sharing will also be promoted through, for example, technical cooperation with private corporations and participation in their research studies on Digital Forensics in FY 2006.

e) Development and evaluation of information system with high level of assurance (Japan Defense Agency)

In FY 2006, the competent agency will test information systems that satisfy assurance requirements of EAL 6, which is the evaluation assurance level required by information security standards of ISO/IEC 15408, and development of evaluation methods will be promoted through evaluation tests.

f) Establishment of operation technologies for essential communications responding to an all-IP networking environment (Ministry of Internal Affairs and Communications)

In order to maintain essential communications in times of disaster, etc., under an all-IP networking environment, test systems will be developed in FY 2006, with the aim of the establishment of operation technologies for essential communications responding to IP networks, etc., by 2008.

C) Consideration of enhancement of investment in groundbreaking research and development

[17] The term, Digital Forensics, is a collective term for methods and technologies used at the time of occurrence of unauthorized access or information leakage to collect and analyze equipments, data, and electronic records necessary to determine the cause of the incidents and present legal evidence.

a) Formulation of basic policies on groundbreaking research and development (Cabinet Secretariat, Cabinet Office, National Police Agency, Japan Defense Agency, Ministry of Internal Affairs and Communications, Ministry of Education, Culture, Sports, Science and Technology and Ministry of Economy, Trade and Industry)

Leaving the area in which technology development is being undertaken in the private sector, to the initiatives of the private sector, discussions will be conducted about a portfolio coordination plan, such as investment of public funds, for the kind of groundbreaking research in which the private sector is not usually prepared to invest, and its basic policies and specific measures will be presented in 2006.

b) Research and development of electronic authentication infrastructure of trusted terminals (Ministry of Economy, Trade and Industry)

In FY 2006, the competent agency will perform research and development toward realization of a safe computing environment through the use of PCs equipped with a Trusted Platform Module (TPM), which has such security functions as code processing, protection of secret keys, and verification of the validity of the platform.

3) Promotion of the 'Grand Challenge' project for research and development (R&D) and technology development

Information security measures require built-in R&D which is based on mid and long-term perspective, not just measures for immediate problems. Therefore, for the R&D and technology development of information security, the government will pursue not only technology development for short-term solutions to issues, but also the Grand Challenge R&D project and technology development aiming to realize fundamental technology innovation with a long-term perspective.

[Specific Measures]

A) Consideration of themes for "Grand Challenge" (Cabinet Secretariat and Cabinet Office)

A panel to continuously discuss themes suitable for the Grand Challenge will be launched in FY 2006 with cooperation between the Council for Science and Technology Policy and the ISPC. In doing so, establishment of a framework will be discussed to promote comprehensive management of various technical elements and appropriate resource allocation for the major objectives. Such framework shall be a system, such as a program manager system, to promote R&D and technology development based on given themes.

Section 2: Development/Securing of Human Resources Engaged in Information Security

The government will make efforts in human resource development for measures of the government, for critical infrastructure measures, and for corporate measures, and will prioritize the promotion of the following measures in FY 2006.

1) Development of businesspersons and specialists with multidisciplinary and comprehensive capability

In information security-related higher education institutions (primarily graduate schools), proactive efforts will be promoted for the development and securing of human resources with multidisciplinary and comprehensive capability by, for example, accepting students and adults of other areas as well as providing recurrent education.

[Specific Measures]

A) Development of human resources with multi-disciplinary and comprehensive capability in higher education institutions related to information security (Ministry of Education, Culture, Sports, Science and Technology)

The competent agency will support creating centers to develop and implement advanced IT human resource programs in universities and graduate schools with cooperation between industry and academia in FY 2006.

B) Training of experts in information security (Ministry of Economy, Trade and Industry) [Reprise]

The competent agency will discuss the nature of human resource development for information security in corporations and universities in FY 2006, and commence deliberations on indices to objectively measure the level of information security measures for IT users in organizations.

C) Support for training activities to develop human resources in information and telecommunications security (Ministry of Internal Affairs and Communications) [Reprise]

The competent agency will support the establishment of a human resource development center to provide multi-dimensional, bi-directional and practical approaches to attacks on and illicit intrusions into information and communications network systems in FY 2006. Support will also be provided for training activities to develop human resources, including security personnel who have professional knowledge and expertise in the area of information and telecommunications.

2) Systematization of a qualification system concerning information security

The government will clearly define the appropriate skills required for highly competent information security engineers, CISO in each organization, and personnel in charge of the information systems of each organization, and promote systematization of a qualification systems concerning information security.

[Specific Measures]

A) Considerations for systematization of a qualification system concerning information security (Cabinet Secretariat, Ministry of Internal Affairs and Communications, Ministry of Education, Culture, Sports, Science and Technology and Ministry of Economy, Trade and Industry)

In 2006, discussions will be conducted, with cooperation between concerned agencies, about the appropriate skills suitable for highly capable information security engineers, for Chief Information Security Officers (CISO) in each organization, for information system operation consigners, for personnel in charge of information systems in each organization, and for information system users. Basic policies and specific measures will also be presented for systematization of a qualification system concerning information security, including examinations on information processing engineering, which would provide a career path for engineers engaged in information security.

Section 3: Promotion of International Partnership and Cooperation

With regard to promotion of international partnership and cooperation concerning the area of information security, the government will prioritize the promotion of the following measures in FY 2006.

1) Contribution to the establishment of internationally safe/secure infrastructure and the development of an environment

The government will empower partnerships such as information exchange with related organizations of other countries, through active participation in early warning, monitoring and alarm raising networks, etc. for the protection of critical infrastructures, in addition to the promotion of cooperation within a multinational framework, such as OECD and G8. In doing so, the government will clarify the function of Point of Contact (POC) of Japan to deal with cross-sectoral information security issues and to promote more effective and smooth coordination.

Furthermore, the government will contribute to the cultivation of culture and the improvement of literacy at an international level, and the development of an environment on an international scale.

[Specific Measures]

A) Promotion of international partnership/cooperation within a multinational framework (Cabinet Secretariat and all government agencies)

As threats to information security are becoming more ubiquitous, frequent and diverse, the competent agencies will more actively implement cooperation within multinational frameworks, such as G8 and OECD, in FY 2006, and will strengthen cooperation with the relevant organizations of other countries by actively participating in the Forum of Incident Response and Security Teams (FIRST), etc. Furthermore, in addition to understanding the reality of the information security measures of other countries, the competent agencies will contribute to the development of an infrastructure and environment for safety and security that are globally sought after, through information exchange, knowledge sharing and trust building among the relevant organizations in other countries.

B) Clarification of the presence to serve as the function of international POC (Cabinet Secretariat)

With regard to inter-agency information security issues without a clear point of contact (POC) for other countries, the NISC will clarify the presence of the function of POC in Japan, which will be made internationally known in FY 2006, to serve as an interface to facilitate effective and smooth cooperation with other countries.

C) Promotion of international PR activities regarding information security policies (Cabinet Secretariat)

In FY 2006, international PR activities will be conducted to disseminate the basic principles and strategies of information security measures of Japan, as an information security advanced nation, measures of the entire government, and status and functions of the NISC, etc.

D) Participation in efforts for analysis and information sharing of measures taken by OECD for protecting critical information infrastructures (Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry)

The competent agencies will participate in the efforts for analyzing measures taken by OECD for protecting critical information infrastructures, and contribute to the formulation of a report which is scheduled to be finalized within 2006.

E) Efforts to realize an international culture of security (Cabinet Secretariat)

In order to realize the “culture of security” defined in the “Guidelines for the Security of Information Systems and Networks”, which was formulated by OECD in 2002, the competent agency will contribute to the development of an environment so that awareness can be shared both nationally and internationally.

F) Holding of APT training/seminars (Ministry of Internal Affairs and Communications)

In order to contribute to the development of an environment for the security of the Asia Pacific region, the competent agency will hold international training/seminars on security in FY 2006, using the human resource development scheme of the APT[18].

2) International contribution of Japan in the area of information security

While making use of the strengths of Japan, the government will actively perform its role through the creation of high value-added innovation, international utilization of technology development with foresight, dissemination and enlightenment of “Best Practice”, and contribution to the development of international standards.

[Specific Measures]

A) International presentation and dissemination of Best Practices (Cabinet Secretariat and all government agencies)

In order to make contributions as the world’s most IT-advanced nation, the competent agencies will provide, ahead of other nations, multidisciplinary knowledge and achievements on various issues, including response to IT-malfunctions, disaster prevention and response, and response to common social issues encountered by each country, while strategically reflecting such knowledge and achievements in international standards, etc.

B) Support for strengthening of Computer Security Incident Response Team (CSIRT) abroad (Ministry of Economy, Trade and Industry)

Through JPCERT/CC, the establishment of CSIRT in the Asia Pacific region will be supported. In specific terms, in FY 2006, in cooperation with APCERT, a forum of CSIRT in the region, the competent agency will share accumulated incident response technologies and experiences of JPCERT/CC with relevant organizations in the region, in an attempt to upgrade the capability of these organizations.

[18] Asia Pacific Telecommunity is an international organization specializing in telecommunications in the Asia Pacific regions. It has 33 member states and 4 regions. Its activities include human resource development through training/seminars, regional policy coordination such as standardization and wireless communications, and solutions to regional issues on telecommunications.

C) International standardization of the Guidelines for Information Security Management in telecommunications business (Ministry of Internal Affairs and Communications)

With an aim to internationally standardize the Guidelines for Information Security Management, the competent agency will propose the Information Security Management Guidelines for Telecommunications (ISM-TG) described in Chapter 2, Section 3 A) to the International Telecommunications Union. Efforts will also be made to have it adopted as an international standard, thus contributing to enhancing the international level of information security management.

Section 4: Crime Control and Protection and Redemption of Rights and Interest

Based on the view that it is necessary to make cyberspace safe and secure to use, the government will prioritize the promotion of the following measures in FY2006.

1) Development of infrastructure to control cybercrimes and to protect and redeem rights and interests

The government will upgrade the standard of cybercrime investigation of law enforcement institutions and reinforce its system. At the same time, the government will crack down on cybercrimes through the amendment of the law systems along with the conclusion of cybercrime agreements and the strengthening of international cooperation. In addition, the government will further develop infrastructure for the protection and redemption of rights and interests in cyberspace, while giving due consideration to other rights and interests: namely, basic human rights, including confidentiality of communications.

[Specific Measures]

A) Strengthening of countermeasures against cybercrime

a) Improvement of technologies and skills for taking countermeasures against cybercrime (National Police Agency)

In order to appropriately respond to diversifying and more complicated cybercrimes, the competent agency will actively carry out inter-/intra-department training in FY 2006 for police officers throughout the country who are engaged in cybercrime investigations.

b) Enhancement and improvement of the system for taking countermeasures against cybercrime (National Police Agency)

In order to appropriately respond to cybercrimes that do not characteristically have geographical constraints, an investigative system will be enhanced and improved in FY

2006 to strictly take countermeasures against cybercrimes that are perpetrated across prefectural and national borders.

c) Improvement and strengthening of investigative and analytic equipments and materials for cybercrime control (National Police Agency)

In order to respond to increasingly diversified and sophisticated modus operandi, such as unauthorized computer access, and toward enforcement of a new legal framework following the ratification of cybercrime conventions, the competent agency will improve and strengthen equipments and materials for conducting on-site investigations and operation tests on computer viruses, etc. in FY 2006.

d) Promotion of legal framework to appropriately respond to cybercrimes (Ministry of Justice)

In light of the advancement of information processing in recent years, and in order to appropriately respond to cybercrimes, the competent agency will promote a legal framework in FY 2006 for the conclusion of cybercrime conventions. (Draft law for partial amendment of criminal laws and others to respond to globalization and organization of crimes and advancement of information processing was submitted to the 163rd Diet on October 4, 2005, currently under deliberation)

e) Promotion of international cooperation for cybercrime control (National Police Agency)

In FY 2006, bilateral cooperation with overseas law enforcement organizations engaged in cybercrime measures will be promoted, participation in international frameworks related to cybercrime measures, such as the G8 High-Tech Crime Subgroup meeting and ICPO, will be continuously promoted, and establishment of a multilateral cooperative relationship will be promoted through the expansion of the membership of the Cybercrime Technology Information Network System (CTINS) Annual Conference.

f) Expedition of international investigative assistance using a Central Authority System[19] (Ministry of Justice)

The competent agency will expedite mutual provision of assistance by designating investigative/judicial authority as a central authority, without going through diplomatic channels. Since agreement on mutual investigation assistance will enter into force between Japan and the US and between Japan and ROK in FY 2006, the competent agency will work on the conclusion of similar bilateral agreements in FY 2006, in order to

[19] Central Authority System is the system that enables mutual provision of assistance without going though diplomatic channels by designating a specific authority as a central authority.

appropriately respond to globalized cybercrimes. The competent agency will also discuss the designation of a "central authority" under the cybercrime convention, upon consultation with relevant agencies.

g) Strengthening of the measures against interference of critical telecommunications services (Ministry of Internal Affairs and Communications)

There have been incidents that threaten the lives and properties of people caused by reduction or suspension of system functions, due to interference and intervention against critical radiocommunications infrastructures, such as aviation radio or emergency radio. There is also concern about system malfunctions due to malicious manipulation of critical radiocommunications infrastructures, and therefore, rapid rejection of such incidents is increasingly important.

Thus, the competent agency will improve and enhance radio wave monitoring for appropriate response to declarations/consultations of interference and intervention against critical radiocommunications, and facilitate rapid rejection of interference and intervention, based on the "Three-Year Plan for Strengthening Radio Monitoring". In addition, the competent agency will strengthen radio wave monitoring by renovating the radio wave monitoring facilities and increasing the number of radio wave monitoring staff by the end of FY 2006.

B) Studies on infrastructure for protection and redemption of rights and interest in cyberspace (Cabinet Secretariat)

The competent agency will carry out studies, such as fact-finding studies, about the necessity of the development of infrastructure for protection and redemption of rights and interest in cyberspace in FY 2006, in close cooperation with concerned agencies.

2) Development and dissemination of technologies to increase safety and reliability in cyberspace

The government will promote the development and dissemination of identification technology to identify the user at the other end of the communication line is under the approval of all the concerned parties in communications as well as in terms of the technology to improve safety and reliability in other cyberspace contexts.

[Specific Measures]

A) Technology development to realize highly advanced network authentication infrastructure (Ministry of Internal Affairs and Communications)

In order to enable safe and secure communications on the Internet, the competent agency will make efforts in technology development to establish a network infrastructure equipped with strict identification authentication functions, and basic technology will be developed in FY 2006.

B) Promotion of joint research between public and private sectors on measures against cyber terrorism (National Police Agency)

The competent agency will carry out joint research on the detection of signs of cyber attacks by analyzing the logs of firewalls, etc., in cooperation with private corporations and universities, etc.

Chapter 4: Policy Promotion System and Structure of Continuous Improvement

The government will comprehensively implement major policies described in the previous chapter in FY 2006 under the following system and persistent structure.

Section 1: Policy Promotion System

(1) Enhancement of the National Information Security Center (NISC)

The National Information Security Center (NISC) aims to reinforce the functions of the promotional system of the government so that the system will perform effectively for the compilation of the highest wisdom of both within and outside Japan. The NISC assumes the following tasks: preparation of basic strategies regarding information security policies of the whole government, designing of technological strategies concerning information security led by new R&D and technology development on the premise that the government will utilize the outcomes, inspection and evaluation of information security measures of the government, analysis of interdependency as to the information security measures among critical infrastructures, formulation and review of Guidelines for Formulation of 'Safety Standards, Guidelines, etc.' concerning Information Security Assurance of Critical Infrastructures, promotion of cross-sectoral exercises, and acting as an international Point of Contact (POC) on the cross-sectoral issues of information security, etc.

Furthermore, since a lot of knowledge on information security has been accumulated in the private sectors, the NISC will actively strive for utilization of manpower therein, and at the same time, will aim to function as a center for human resources development of government officials.

[Specific Measures]

A) Enhancement of the National Information Security Center (NISC) (Cabinet Secretariat)

The personnel structure of the NISC, which would play a core role in promoting information security measures of the entire government, will continuously be strengthened, ensuring at least 60 staff members by early FY 2006, and actively utilizing excellent human resources to mobilize the highest wisdom of the public and private sectors.

Under such system, the competent agency will implement the measures described in Chapter 2, Section 1 so as to make full-dress launch of the Standards of Measures and PDCA cycle based thereon and to strengthen the emergency response capability of the entire government, and will also carry out measures described in Chapter 2, Section 2 in line with the action plan etc. concerning information security measures for critical infrastructures.

In order to improve the functions of the NISC as an international Point of Contact (POC) in Japan concerning cross-governmental information security issues, and to enable the NISC to play a role as an international interface trusted by other countries, the competent agency will increase the recognition of the NISC as a POC, promote international trust relations, improve information collection, strengthen the functions of information sharing and analysis with relevant organizations, and ensure the core function of promoting cross-sectoral policies with regard to information security.

In view of disseminating the activities of the NISC as well as information security-related issues throughout the general public, e-mail magazine of the NISC will be issued periodically in FY 2006.

(2) Enhancement of Ministries and Agencies

In order to actively promote information security measures of the whole government, having the Information Security Policy Council and the NISC as its core, Ministries and Agencies will be committed to the improvement and strengthening of the information security system of its own. At the same time, in trying to change the traditionally bureaucratic sectional system, Ministries and Agencies will make efforts to implement every measure so that integrated and cross-sectoral information security measures will be facilitated in public and private sectors.

[Specific Measures]

A) Strengthening of the framework for information security measures and implementation of cross-organizational approaches of the government (All government agencies)

The competent agencies will strengthen the framework for their own information security measures, and will implement, in cooperation with each other, cross-organizational approaches, such as the share of operation procedures and outcomes of information security measures of the public and private sectors and standardization of the measures, etc.

Section 2: Partnerships with Other Related Organizations

The National Strategy stipulates mid and long-term strategies in view of the information security issues in Japan; however, information security is widely associated with people’s social lives and economic activities, and it is necessary to pursue cooperation with various related organizations in implementing the strategies.

It is required to pay particular attention to the following facts; in terms of the relationship with IT Strategic Headquarters, information security policies are to be positioned as one of the primary factors of IT policies in various related organizations; and the National Strategy is to practically assume the part of the information security-related elements of the IT New Reform Strategy. In terms of the relationship with the Council for Science and Technology Policy, it is necessary to make sure that factors related to R&D and technology development within information security policies are consistent with the science and technology policies of the government. Thus, Information Security Policy Council and NISC will promote information security policies in cooperation with each other.

[Specific Measures]

A) Strengthening of cooperation with relevant organizations, etc. (Cabinet Secretariat and Cabinet Office)

The ISPC will intensify the exchange of opinions with other related organizations, such as the IT Strategic Headquarters, Council on Economic and Fiscal Policy and Council for Science and Technology Policy, to clarify the demarcation between them, and to promote information security measures of the entire government in an integrated manner, by closely cooperating with each other in proposing and implementing various measures.

In particular, with respect to the relationship with the Council for Science and Technology Policy, the competent agencies will maintain cooperation with the NISC, based on area-specific promotion strategies (i.e. information and telecommunications area) during the period of the Third Science and Technology Basic Plan[20]. Additionally, with regard to the nature of information security measures for disaster prevention and reduction, the competent agencies will cooperate more closely with other related councils, such as the Central Disaster Prevention Council, by intensifying the exchange of information, thus promoting information security measures for critical infrastructures in an integrated manner.

Section 3: Establishment of the Structure of Continuous Improvement

The situations surrounding the issues on information security change rapidly, namely new risk factors can emerge one after another, and unexpected incidents, disasters and attacks can occur, so it is necessary to constantly evaluate and improve the effectiveness of the policies. Therefore, the government is required to construct bases for continuous improvement as below.

(1) Formulation and Evaluation of the Annual Plan

In order to realize the National Strategy, the government will formulate the Annual Plan as an implementation plan of more specific measures every fiscal year, evaluate the

[20] Third Science and Technology Basic Plan (Cabinet decision of March 28, 2006)

implementation, and disclose the results as much as possible.

Meanwhile, in order to smoothly promote the measures, such as when a case must be responded to by related organizations other than the government, the government will consider a milestone setting that covers several fiscal years, for those requiring mid and long term plans, without adhering to an annual plan.

[Specific Measures]

A) Implementation and disclosure of evaluation (Cabinet Secretariat)

In FY 2006, while considering the method to appropriately evaluate Secure Japan 2006, the competent agency will implement evaluation on the progress of specific measures described in Secure Japan 2006, and the results will be disclosed every six months. In doing so, efforts are made to ensure coordination with deliberations by the Expert Evaluation Group of the IT Strategic Headquarters.

B) Discussions on a milestone toward strengthening information security measures of government agencies (Cabinet Secretariat)

In view of promoting advanced responses by related organizations other than government agencies toward the realization of the First National Strategy, in FY 2006, the competent agency will consider a milestone up to FY 2008.

C) Framework based on Action Plan on Information Security Measures of Critical Infrastructures (Cabinet Secretariat)

The competent agency will examine the progress of measures in FY 2006 based on the Action Plan on Information Security Measures for Critical Infrastructures by utilizing the Expert Panel on Critical Infrastructures.

(2) Implementing Measures to Respond to Emergencies during Execution of the Annual Plan

The government, while even executing annual plan, will implement measures to respond to emergencies in the event of incidents, disasters or attacks, etc.

[Specific Measures]

A) Consideration for reviewing the plan (Cabinet Secretariat)

In the event of an emergency such as a large-scale disaster or attack, or a sudden change in information security situations, suitable measures will be rapidly designed and carried out, even in the midst of implementing Secure Japan 2006.

(3) Development of Evaluation Criteria

No definite evaluation criteria for information security in each implementation area of measures have been set up thus far. However, since these criteria are indispensable for the evaluation of the degree of diffusion of information security measures in each implementation area, the government will promptly consider the criteria, aiming to utilize them for the evaluation of the implementation of the National Strategy.

[Specific Measures]

A) Establishment of evaluation indices for information security measures (Cabinet Secretariat, Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry)

From the perspective of visualizing a path toward the realization of the First National Strategies, the competent agencies will establish a system to consider indices for evaluation of the degree of penetration with respect to information security measures in each implementation area (i.e. government agencies, local governments, critical infrastructures, businesses, and individuals, etc.) at the earliest possible time in FY 2006, and the use of these indices within the government and international organizations will be promoted, upon establishing appropriate evaluation indices in FY 2006.

Meanwhile, in order to contribute to the aforesaid evaluation indices, the competent agencies will promote the formulation of the “Evaluation Indices for National Information Security Level (tentative)” by IPA, and will also consider the formulation of the “Evaluation Indices for the Security Level of Information and Telecommunications Infrastructures (tentative)”.

Chapter 5 Direction of Priority Measures for FY 2007

– Priority for FY 2007 "Upgrading Information Security Measures in the Public and Private Sectors" –

In Chapters from 2 to 4, specific measures to be taken in FY 2006 were described as the first step of the three-year basic policies, with emphasis on the **establishment of information security measures in the public and private sectors.**

Information security measures of the whole nation need to be taken by every concerned party, through role sharing which is suitable for each, with awareness of its own responsibilities, and common recognition about the importance of addressing information security issues. However, there are some entities that lack the awareness of the importance, and cannot take appropriate measures to protect themselves under the circumstances, and they cannot be covered by "establishing a system". Therefore, it is extremely important to upgrade those entities that have fallen behind in taking measures, in order to achieve the goal of raising the overall level.

Major pillars of measures to upgrade the level of those entities that fall behind in taking measures include: 1) efforts in the area that can present good practices to the concerned entities that are behind and other concerned parties; 2) measures for the entities that are behind, and 3) efforts in strengthening and stabilizing cross-sectoral information security infrastructures to prevent any entity from falling behind.

Thus, besides continuing measures for FY 2006, in FY 2007, the government will place emphasis on **upgrading information security measures in the public and private sectors** to establish a solid path leading to FY 2008, which is the final year of the Three-Year Plan. The following measures will particularly be promoted.

Section 1 Upgrading Information Security Measures in the Model Area

With regard to the area of government organizations and the area of critical infrastructures, the National Strategy stipulates that all government agencies aim to implement the most advanced level of measures by the beginning of FY 2009, and to reduce the incidents of IT-malfunctions in critical infrastructures to as close as possible to zero, and these are the areas we expect to be a model for other entities. Local governments, meanwhile, are required to strengthen information security measures based on the efforts taken by the central government agencies. Thus, following the establishment of a system of FY 2006, the government will present good practices in FY 2007 to the individuals and entities that have fallen behind in these three areas by implementing the following measures.

[Specific Measures]

A) Upgrading information security measures in government organizations

a) Establishment of PDCA Cycle and promotion of full-scale evaluation (Cabinet Secretariat and all government agencies)

Each government agency will improve its own measures based on the results of self-assessment and monitoring of the implementation of information security measures, in an attempt to upgrade the entire organization by establishing PDCA Cycle. In addition, the Cabinet Secretariat will, based on the evaluation method established in FY 2006, perform full-scale objective evaluations on the implementation of measures of each government agency in a comparable manner, and disclose the result, in an attempt to promote effective measures of the government as a whole.

b) Presentation of a pioneering empirical model of information security measures (Cabinet Secretariat)

Although technology has been developed, some measures are lagging behind in the area of pioneering security measures, or some measures have yet to be implemented in government organizations. Based on the fact that propagation is taking time due to a lack of know-how, including transition methods or installations method suitable for the conditions of the implementation sites, the competent agency will formulate operation procedures, etc., by introducing these information security measures as an empirical model, and will promote the introduction of measures by providing technological information, etc., which can be used as an implementation reference for government organizations and other entities.

c) Strengthening of the functions of solving cross-sectoral problems associated with cyber attacks, etc., against government organizations (Cabinet Secretariat and all government agencies)

In order to prevent cyber attacks against government organizations, and information leakages and system failures in government organizations, and to rapidly and adequately respond to incidents when they occur, the NISC will strengthen relevant functions such as information collection functions, analyzing functions of attacks, etc., advisory functions to government organizations, and functions to promote intra-organizational cooperation (operation of the Government Security Operation Coordination Team: GSOC). In doing so, each government organization, led by the NISC, will strengthen the real-time monitoring and rapid response functions of each information system.

d) Strengthening of information collection and incident response capability (National

Police Agency)

In order to adequately and accurately respond to acts of cyber terrorism, the competent agency will appropriately understand new Internet observation functions, equipments for on-site operations, and the actual situation at the scene, and will also develop and advance equipments and materials to give commands and instructions, and promote the strengthening of international cooperation in the cyber terrorism measures of police agencies.

e) Education and training necessary for response to cyber attacks, analysis of attacks and evaluation of protective measures (Japan Defense Agency)

In order to carry out education and training for combatants against cyber terrorism, to analyze the method of attacks and to evaluate protective measures, the competent agency will promote the development of a system to simulate the modes of cyber attacks, etc. The competent agency will also promote such measures as technology for monitoring of and protection from unauthorized computer access, technology for analyzing cyber attacks, and active protection technology, etc., in order to rapidly and effectively carry out responsive actions against cyber attacks. Furthermore, the competent agency will develop an environment and improve and enhance research systems for promoting the efforts mentioned above.

B) Upgrading information security measures for critical infrastructures

a) Improving the ability to grasp the situation for the promotion of cross-sectoral measures for critical infrastructures (Cabinet Secretariat)

The competent agency will conduct risk analysis, etc., by combing regular threat analyses and the assessment of ongoing efforts in critical infrastructures, to grasp the current state of the threat. In addition, it will grasp the current situations of safety measures of the business entities engaged in critical infrastructures that require confidentiality, in cooperation with the agencies surrounding critical infrastructures.

b) Strengthening of the information sharing basis for smooth cooperative response between public and private sectors (Cabinet Secretariat)

In order to protect critical infrastructures from IT-malfunctions that may occur in any operation of critical infrastructures, it is necessary to conduct cooperative response activities between the public and private sectors more effectively and efficiently. Thus, in addition to human resources, the competent agency tries to establish the basis for an information sharing environment that incorporates assurance of confidentiality and infallibleness that allows adequate and rapid response to IT-malfunctions.

c) Promotion of analysis of dynamic dependence between critical infrastructures (Cabinet Secretariat and agencies surrounding critical infrastructures)

IT systems are not only essential for maintaining the services of business entities engaged in critical infrastructures for the people, but are also closely related to business entities engaged in critical infrastructures of other sectors. Since further advancement of IT use and increase in relations between different areas are expected, the protection of critical infrastructures through individual measures in each area does not provide sufficient panoramic analysis of and measures for the whole network system. Therefore, predictable dynamic simulation of the effect of the spread and extension of damages from IT-malfunctions will be promoted upon grasping the effect propagation mechanism of mutual dependency.

d) Promotion of exercises for critical infrastructure functions (Cabinet Secretariat and agencies surrounding critical infrastructures)

In order to verity whether information provision/sharing systems and various information security measures will effectively function at the time of actual incidents of IT-malfunctions, exercises for critical infrastructure functions will be performed according to the IT-malfunction propagation scenario (themes are set in accordance with the model of specific foreseeable threats), in cooperation with the agencies surrounding critical infrastructures, the business entities engaged in critical infrastructures, and CEPTOAR of each critical infrastructure, etc. In addition, an implementation plan for functional exercises[21] will be formulated to confirm the functions of a cooperation system between the public and private sectors, and to facilitate coordinated response activities.

e) Ensuring stable operation of Internet systems (Ministry of Internal Affairs and Communications)

An appropriate environment will be developed in order to ensure the stable operation of Internet systems, which have now become a basis for people’s social lives and economic activities, in preparation for the event of disturbance to the telecommunications services, such as cyber attacks, computer viruses, and information leakages, etc.

f) Strengthening of information security measures in the electricity area (Ministry of Economy, Trade and Industry)

A model system for a control and communications system for electricity, which is the

[21] Plan for functional exercises stipulates the plans for controlling a drilling scenario and the participation of CEPTOAR/critical infrastructure operators, etc.

core of a control system, will be established using general-purpose technologies, and security evaluation and measures based on cutting-edge technologies will be discussed. Furthermore, the competent agency will promote studies on dealing with information pertaining to threats using such general-purpose technologies.

g) Strengthening of partnership between public and private sectors in responding to cyber terrorism against critical infrastructures (National Police Agency)

The competent agency will conduct campaign activities to raise the awareness of business entities engaged in critical infrastructures about cyber terrorism based on the characteristics of the operation of business entities engaged in critical infrastructures, on an as needed basis. In addition, discussions will be conducted about entrusting research and study projects on the threats and countermeasures against cyber terrorism to private entities and also about conducting joint research on the early detection of cyber terrorism.

C) Upgrading the level of information security measures in local governments

a) Promotion of development of operation procedures for ensuring information security assurance in local governments (Ministry of Internal Affairs and Communications)

In order to ensure efficiency of the information security measures in local governments, the competent agency will promote the development of operation procedures on information security.

Section 2 Upgrading the Level of Measures Taken by Entities that Tend to be Slow in Taking Actions

Businesses and individuals are the areas in which there are some entities that tend to be slow in taking measures due to the influence of market principles and a lack of fundamental interest, even though they are susceptible to damage from information security incidents/accidents. Thus, in FY 2007, the government will take the following measures to upgrade the level of measures taken by some corporations and individuals that tend to be slow in taking actions, in addition to accelerating the measures of FY 2006 (see Chapter 2, Section 3 and Section 4),

[Specific Measures]

A) Improvement and development of portal site providing information of government organizations (Cabinet Secretariat and all government agencies)

A portal site providing a list of information of government agencies will be improved and developed. In addition, documents regarding the information security measures in each area of the government will be disclosed as much as possible and linked to this portal site.

B) Strengthening of dissemination and PR activities for general users (Ministry of Internal Affairs and Communications)

In order to allow general users of information telecommunications services to use the services safely and securely, the competent agency will strengthen dissemination and PR activities concerning information security.

C) Design and distribution of educational contents to learn security measures in an understandable and practical way (Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry)

In order to present the concept of safe use of Internet services to teachers and students of elementary, middle and high schools, and to prepare an environment to acquire literacy skills and acquire know-how, the competent agency will promote the use of educational contents in classes and lessons at elementary, middle and high schools while taking into account the latest movements on information security.

D) Promotion of damage prevention measures accurately reflecting the reality of cybercrimes (National Police Agency)

In order to surely prevent damages from cybercrimes, analysis of the reality of detected cybercrimes will be enhanced, and dissemination and PR activities based on the latest modus operandi will be conducted.

Section 3 Upgrading the Level of Cross-sectoral Information Security Infrastructures

What is missing to strengthen and stabilize the information security measures of our entire society from a long-term perspective can be the vulnerability of the information security infrastructures of the whole society. In specific terms, it refers to a framework to evaluate and disclose the condition of information security, human resource development and training measures for educators and specialists in information security, R&D and technology development and formulation of standards to allow everyone to use the IT systems safely, and upgrading the level of investigative organizations, etc. Thus, the government will promote the following measures in FY 2007.

Meanwhile, it is important to remember that the measures to upgrade the level of information security infrastructures cannot be completed overnight, but in many cases, it would require mid- and long-term efforts.

[Specific Measures]

A) Formulation and issuance of “White Paper on Information Security Measures (tentative)” (Cabinet Secretariat)

In order to visualize the condition of the information security of the entire society, the competent agency will formulate and issue the “White Paper on Information Security Measures (tentative).”

B) Development/training for educators and experts in information security (Cabinet Secretariat, Ministry of Internal Affairs and Communications, Ministry of Education, Culture, Sports, Science and Technology and Ministry of Economy, Trade and Industry)

The competent agencies will increase the opportunities for development/training for education and experts in information security, and also will discuss strategies toward the establishment of career paths that would help the general public appreciate the role of these personnel, and secure their occupational positions and recognitions.

C) Empirical use/development, etc. of next generation OS environment that realizes advanced security functions (Cabinet Secretariat, Cabinet Office, Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry)

The competent agencies will actively promote the empirical use of some of the outcomes of the “Development of Next Generation OS Environment to Realize the Advanced Security Functions,” which is implemented in FY 2006, and at the same time, they will promote the development of coded telecommunications systems for expansion of infrastructure functions, ID control and resource management through cooperation between industry, academia and government. In addition, based on the results of empirical tests, the competent agencies will promote formulation of government procurement specifications for system installation, such as the OS, aiming at developing an OS environment that would realize full-fledged and advanced security functions on the premise of the use by E-Government.

D) Dissemination of educational materials for developers (Ministry of Economy, Trade and Industry)

To create an environment that allows information related operators to develop and provide products equipped with information security functions, the IPA will produce and disseminate a booklet on the basics of information measures concerning built-in software.

E) Establishment of standards to be complied with by safe websites (Ministry of Economy, Trade and Industry)

The competent agency will organize integrated security requirements for creating a website in an attempt to formulate the standards to be complied with by safe websites.

F) Promotion of full-scale use of cryptographic module test authentication system (Ministry of Economy, Trade and Industry)

In order to promote the use of highly safe cryptographic modules, efforts will be made to start the full-scale use of a framework for the authentication of cryptographic modules by expanding the IT security evaluation and authentication systems used by the IPA.

G) Comprehensively upgrading the investigative capability on cybercrime cases (National Police Agency)

In order to respond to diversified and sophisticated modus operandi, such as unauthorized computer access, and to the enforcement of a new legal system following the conclusion of conventions against cyber crimes, the competent agency will promote the development and advancement of systems, equipments and materials to analyze electromagnetic records to appropriately respond to the fabrication of illicit electromagnetic records. In addition, the competent agency will strengthen and improve a system concerning digital forensics, implement inter- and intra-department training for police officers throughout the country engaged in cybercrime investigation, effectively and efficiently implement international cooperation and efforts for the control of other cybercrimes, and promote the development of improving investigative capability.

H) Ensuring safety of information processing infrastructure (Ministry Economy, Trade and Industry)

In order to ensure the safety of information systems and software against threats, which are making progress everyday, and against vulnerabilities, which are constantly found, the competent agency will develop an appropriate information processing environment through rapid information sharing, prompt provision of countermeasures against vulnerabilities, and the development of technological response measures meeting the needs of the age.

Furthermore, given the rapidly changing corporate organization systems and the development of new legal systems, the competent agency will improve the information security of the Japanese corporations through the provision of appropriate organization management measures and guidelines, etc.

I) Response to new information security threats against information telecommunications (Ministry of Internal Affairs and Communications)

In order to ensure ceaseless operation of information telecommunications networks, the competent agency will conduct fact-finding studies in an attempt to take immediate and accurate response to new threats to information security, and will also promote the necessary R&D and technology development programs, etc.