Secure Japan 2007

- Upgrading of information security measures in order to create an environment in which people can use IT safely and securely -

Information Security Policy Council

June 14, 2007

Contents

Chapter 1: Action and Evaluation Based on Secure Japan 2006

Section 1: Background of action based on Secure Japan 2006

Information technology (IT) has contributed to enriching the lives for the people of Japan. IT infrastructure has penetrated deeply into people's lives, and has become intrinsically essential for every activity.

However, there have been incidences where the use of IT has threatened the safety and comfort of the people. Information security risks have increased: for instance, the advancement of electronic and virtual reality technologies in economic activities, such as online ticketing, and penetration of electronic money have brought about drastic improvement in processing speed and efficiency, as well as increased user convenience. However, response measures to handle IT malfunctions are not yet fully developed, leading to the risk of serious damage. It is also possible that immediate response will not be forthcoming due to a lack of human resources with specialist knowledge and skills in implementing information security measures. In 2005 Japan was affected by incidents such as cyber attacks on governmental web servers, information leakage caused by the use of file sharing software and computer viruses, operation suspensions due to IT-malfunctions in critical infrastructures, and cyber crimes, such as illicit access, etc.

In order to substantially strengthen measures to handle such issues, Japan formulated the First National Strategy on Information Security in order to promote integrated and cross-sectoral information security measures in the public and private sectors. This provides for mid- and long-term strategy for information security measures in Japan (decision made on February 2, 2006 by the Information Security Policy Council (ISPC), hereinafter referred to as the “National Strategy”). In response to the National Strategy, each implementing body, including government agencies, has undertaken the first-year measures, based on the annual plan (Secure Japan 2006 (decision made on June 15, 2006 by the ISPC) (hereinafter referred to as “SJ2006”)), which stipulates the government's priority measures for information security in Japan.

Section 2: Priority Goals and Pillars of Effort in FY2006

Focusing on the establishment of a framework for information security measures in the public and private sectors, SJ2006 set forth four priority goals: (1) to encourage all entities to share a sense of participation in information security measures in the public and private sectors, (2) to take measures to pursue advanced technologies under a coherent policy for the entire government, (3) to establish a framework to upgrade the level of information security measures in the public sector and communication systems necessary for the public and private sectors, and (4) to

establish an information sharing system of information security measures for all parties concerned

Furthermore, SJ2006 included 133 specific measures to be implemented by government agencies in FY2006, based on the three pillars of the National Strategy, namely "four implementation fields", "cross-sectoral information security infrastructure", and "policy promotion system and structure of continuous improvement" (enhancement of policy promotion systems, cooperation with concerned organizations, and establishment of a structure of continuous improvement).

Section 3: Evaluation of FY2006

National Information Security Center (referred to as "NISC" in the text of Chapter 1 and Chapter 2) has conducted evaluations, etc.,[1] on the conditions brought about by the efforts of SJ2006. "Evaluation, etc., of Information Security Policies in FY2006" (hereinafter referred to as the "Evaluation 2006") was formulated and reported to the Information Security Policy Council. This publication aims to draw out the directions suggested by the Evaluation 2006, identify the current conditions that predicate the formulation of the annual plan for FY2007, and evaluate the efforts made in FY2006. The major viewpoint here is not to comprehensively grasp the changes in society caused by information security policies and all the incidents associated with information security, but to understand the essential conditions prior to the discussion on policies for FY2007.

This publication, based on these recognitions of the current situation, describes basic policies for FY2007 in Chapter 2, and outlines specific efforts to be addressed in FY2007 in Chapter 3 to Chapter 5. Since mid-term issues can be drawn from the evaluations, Chapter 6 discusses the direction of priority measures in FY2008.

1. Evaluation/Analysis

The results of 133 specific measures to have been implemented within FY2006 in line with SJ2006 were classified and evaluated as follows:

○ A : Measures implemented as initially planned

[1] In Chapter 1 and Chapter 2 of this publication, "Evaluations, supplementary study and analysis, etc. in line with evaluation criteria" are expressed as "evaluations, etc.", in accordance with the definition of the "Operational Policies for Evaluations based on Evaluation Criteria" of the "Evaluations, etc., toward Realization of Secure Japan and Promotion of Reasonable and Continuous Improvements" (decision made on February 2, 2007 by the Information Security Policy Council).

Note: A dash is added if it is found from the progress of the operation related to the measures and from the hearing of the personnel in charge that there were problems with the systems and personnel that needed to be resolved in the future, although the measures had been implemented.

- ○ B^+ : Efforts have been steadily implemented, and the measures are to be completed within several months although not within the fiscal year
- ○ B : Measures have not been implemented as planned, but can be implemented in the end through continuous efforts
- ○ C : Measures failed to be implemented as planned without prospect for the future
- ○ － : Measures failed to be implemented due to factors beyond the control of government agencies.

According to the classification, 133 specific measures are evaluated as follows:

A: 110, A': 6, B+: 4 B:12 C: 0 －:1

The evaluation showed that about 87.2% (116/133) of the measures were implemented as planned. 110 measures rated "A", accounting for the majority of the measures. It is expected that these will make continuous or more progressive efforts. The measures rated "A'" were implemented as planned due to strenuous efforts of the responsible personnel, etc., of related organizations. However, two of the major measures at government agencies were rated "A'"; namely, "establishment of a PDCA Cycle at each government agency" and "establishment of a PDCA cycle for the whole government", which suggests that lack of a system and personnel, etc. is a critical issue.

Measures rated "B+" are those with procedures to be completed in the future following decisions by the Information Security Policy Council. The measures receiving a "B" failed to be implemented within the fiscal year following careful consideration, but are expected to be implemented in the end with continuous effort.

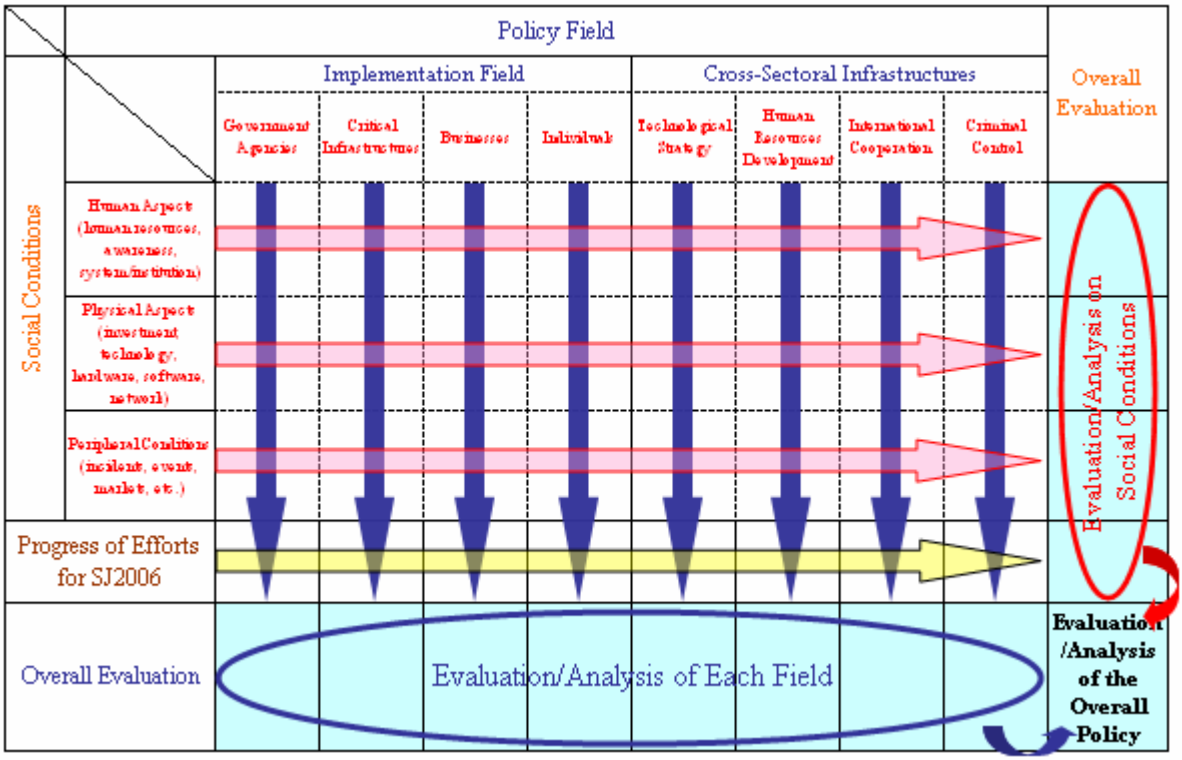
In summary, it is fair to conclude that 133 specific measures to be implemented within FY 2006 in line with SJ2006 have been launched at each government agency and have generally progressed steadily thanks to the hard work of responsible personnel, etc. However, many measures still need to be worked on or require increased effort. Thus, it is necessary to continue efforts from the next fiscal year onward. Some of the measures seem to lack a system or personnel to sustain the implementation and this issue must be resolved.

2. Evaluation/Analysis of Social Changes Brought about by Efforts to Implement Measures

In this section, in accordance with the framework set forth by the Evaluation 2006,

evaluations and analyses are made from both vertical and horizontal angles by discussing social conditions across policy fields as a vertical axis in terms of three aspects: namely, human aspects (human resources, awareness, system/institution), physical aspects (investment, technology, hardware, software, network), and peripheral conditions (incidents, events, market, etc.), in addition to the discussions along the horizontal axis, specifically, policy fields based on the National Strategy.

Discussion Framework concerning Evaluation/Analysis of Information Security Policies in FY2006



(a) Policy Field

(i) Central government/local governments

It is fair to conclude that the PDCA cycle of information security has generally been established in FY2006. Government agencies worked toward improvement, with an awareness of the necessity to improve measures identified as insufficient in the focused examinations. Some efforts were also observed for ensuring the necessary budget. Although an information security management system is being established, there is a lack of personnel to promote efforts on a practical basis. It is necessary in the future to examine whether the PDCA cycle of each government agency is being implemented and promoted steadily and effectively and whether it is functioning appropriately. Efforts for E-Government are being promoted, including optimization of various government operations and systems, but it is essential to take information security into account when

promoting these measures.

(ii) Critical infrastructures

In FY 2006 considerable efforts were made to implement expected measures based on the action plan for information security of critical infrastructures. However, it is too early to make an objective assessment on how information security conditions in each area of critical infrastructures have been improved as a result of these efforts, partly because this is only the end of the first year. Nonetheless, it is necessary to continue work on information security measures in the areas of critical infrastructures since the use of IT in people's lives and social and economic activity is expected to continuously increase and expand and also because the factors causing IT-malfunctions are constantly changing.

(iii) Businesses

It is fair to say that efforts are solidly undertaken in this sector, as seen in the improvement of the usage rate of antivirus software, etc., development of systems to ensure information security and formulation of business continuity plans. Awareness has been raised among business entities that causing information security incident will bring considerable economic damage to the company, partly due to court decisions that have recognized the liability of business entities that leaked personal data. Thus, the business sector as a whole seems to be making progress in implementing measures.

However, it is also a reality that information leakages are still occurring in rapid succession. Not all business entities have a high level of information security awareness and have taken appropriate measures. It is also assumed that there is a gap between progressive companies and non-progressive companies, and between large-sized enterprises and small- and medium-sized companies.

(iv) Individuals

Information security education and public relations activities, etc. targeting individuals are being strengthened. Sales of anti-virus software are steady, which implies that awareness of information security is on the rise and knowledge is increasing.

However, there are significant numbers of individuals without protection, and new risks have emerged. It seems that measures to handle these factors are the future tasks to be addressed.

(v) Promoting information security technology strategy

The IT field has seen a growth in security products but made-in-Japan security technology is still limited. Improvements are expected through such measures as intensive

investment of public research funds into research and development/technology development and through improvement of investment efficiency. The “Development of Next Generation OS Environment to Realize the Advanced Security Functions” through industry-academia-government cooperation, is expected to play a leading role in this area.

(vi) Developing/Ensuring human resources engaged in information security

Although efforts for developing human resources in information security in the public and private sectors are under way, it is undeniable that there is still a lack of human resources and skills. It seems, thus, that developing/ensuring human resources on a large scale is at the early stages.

(vii) Promotion of international partnership and cooperation

Awareness of the information security policies of Japan has been raised to some extent through the introduction of Japanese approaches at international conferences, etc., and through PR activities on the website of NISC.

However, this is still early stages and there is much room for further work, such as the reduction and elimination of risks associated with information security within a multinational framework and provision of Japan’s knowledge and experience to other countries.

(viii) Crime control and protection and redemption of rights and benefit

The evaluation showed some progress in FY2006, the first fiscal year of the National Strategy. However, crimes and illegal activities in cyberspace are now frequently taking place. Unless further measures are urgently enhanced, it is anticipated that anxiety concerning crimes which may be committed over Internet, etc. will increase.

(b) Social Conditions

(i) Human aspect (human resource, awareness, system/institution)

Developing and ensuring human resources in both government agencies and private companies has not achieved sufficient level yet.

In terms of awareness, it can be concluded that signs of increased awareness on information security have been observed, since awareness of business entities about IT control and Business Continuity Plan (BCP) has been raised and efforts for enlightenment have been promoted. It is believed that the following facts have greatly contributed to the increased awareness: 1) companies can afford information security measures due to economic recovery, and 2) reports on information leakages are often taken up by mass media and companies are more aware that problems associated with information security

cause economic loss.

However, the awareness is still at an “incipient” stage and it is believed that measures have not yet been taken as a matter of course.

With regard to systems/institutions, there is a tendency for companies to have enhanced response systems, and government agencies are gradually developing systems/institutions to promote information security measures in a concerted manner under the coordination of the Cabinet Secretariat.

(ii) Physical aspects (investment, technology, hardware, software, network)

In terms of investment in information security, the government agencies ensured the budget to build the Government Security Operation Coordination, the system to respond to threats to government agencies. Business entities are believed to have a tendency to make investment in view of the balance between the cost and economic loss caused by information security issues. Individuals tend to make investment where it is necessary; for example, purchase of software for information security measures has become popular. Also, it is observed that discussions were made on the improvement of efficiency of investment in research & development and technology development.

In the aspect of information security, there is a tendency to promote mainly the development of the products required for specific measures.

(iii) Peripheral conditions (incidents/events, market, etc.)

As information leakages caused by computer viruses, etc. continue to occur and new services that spread personal data on the Internet have emerged, new types of damages have been incurred. A change in attacks on the government agencies and businesses has been observed; specifically, sneaking malware into the computers. Thus, damages have become less noticeable. Efforts to reduce risks of using IT are promoted, but the methods of cyber attacks are also becoming more advanced.

With respect to IT-malfunction, for example, some incidents have surfaced which had not been previously considered, reflecting the advancement of globalization of socio-economic activities; for example, the impact of IT-malfunction has become more extensive, and not confined to one country.

3. Overall Evaluation

In summary, it is fair to conclude that improvements in information security measures were generally conducted smoothly in FY2006, and the development of systems for information security measures in public and private sectors has made progress. Also, FY2006 saw all

relevant entities in each implementation field realize the importance of such measures. Individual agencies traditionally worked alone, but cooperation has been progressively made in each implementation field under the leadership of NISC. In addition, NISC has served as a central point while looking at Japan as a whole, beyond the scope of each implementation field.

In other words, achievements through the efforts in FY2006 include 1) incipient awareness of each sector, 2) launch of specific efforts by each implementation body, 3) launch of specific efforts in cross-sectoral information security infrastructures, and 4) establishment of information security promotion systems and sustainable improvement structure.

However, it is the case that there is a lack of speed in implementation in some fields, and factors such as insufficiency of human resource seems to have great impact here. It cannot be said that risks associated with the use of IT have been greatly reduced. Considering the changes in risks along with the changing environment, efforts are being made to suppress severity of the risks from becoming more serious. Although work undertaken in the context of SJ2006 has been satisfactory, some objectives for FY2006 are still at an early stage.

With the aim of becoming a nation advanced in information security, continuous and incessant efforts are necessary in FY2007.

Chapter 2: Basic Policy for Addressing Information Security in FY 2007

Section 1: Issues in FY2007

Secure Japan 2007 (hereinafter referred to as "SJ2007") sets out priority measures for the information security of the government of Japan in FY2007, the second fiscal year of the efforts under the National Strategy, based on the efforts and their evaluation results of FY2006.

FY2007 is the second year effort of the three-year National Strategy and major tasks in FY 2007 include the maintenance of the systems to promote information security measures in public and private sectors, which were established in FY2006, and stabilization of promotion of measures including the upgrading of those that were previously insufficient.

In order to respond to these issues, it is primarily crucial to sustain or improve awareness about information security on the part of those responsible for implementation. Second, it is important for each implementing body to steadily carry out measures to be implemented based on the PDCA cycle (sustainable improvement structure) of the yearly unit program, as well as of the three-year unit National Strategy, under the system to promote information security measures in the public and private sectors, while maintaining proactive engagement. In particular, one major theme is to upgrade the information security measures of the public and private sectors. The fields which should serve as an exemplar for others, such as government agencies and critical infrastructures, need to present a model to those bodies lagging behind in efforts, by accelerating the speed of efforts in an attempt to upgrade the measures. It is also essential to upgrade the measures of bodies lagging behind among businesses and individuals and to improve the cross-sectoral information security infrastructures.

Section 2: Priorities of Information Security Measures in FY2007

Priorities of Japan's information security measures in FY2007 are to pursue a stable implementation of information security measures under the National Strategy, which was launched in FY2006, and at the same time to **realize the upgrading of information security measures in public and private sectors**. The following policies are in effect for the four basic policies listed in the National Strategy: 1) Maintenance and improvement of common awareness will be undertaken since the shared awareness has been infused into each body of public and private sectors, in general, 2) advanced technology will be continuously pursued, considering the discussions at the Information Security Technology Strategy Committee, 3) strategic and responsive capability in the public sector will be strengthened, while keeping the balance with protection of human rights and ensuring transparency and legality in the public sector, and 4)

promotion of international partnership and cooperation will be sustained and strengthened among international bodies.

Section 3: Necessity for Efforts Based on Mid-term Perspective and Timely Intensive Action

Information security policies intend to achieve the objectives of the National Strategy in three years by accumulating the efforts in line with the PDCA cycle on a yearly basis and to formulate the next three-year plan based on the results, and to formulate annual programs under the three-year plan. However, in terms of practical management of measures, a single year is too short to see full achievements, and action is therefore being taken on a mid-term basis, intensifying in accordance with the given situation at a given time, instead of at a yearly timeframe. These issues must be fully considered when formulating basic policies for FY2007, including the direction of priority measures for FY2008. From this viewpoint, the following three factors are considered important.

Developing and ensuring human resources engaged in information security, including strengthening the system of the department in charge of information security, is an important issue to be addressed in FY2007, in order to create an environment where IT can be safely used. However, since developing and ensuring human resources is the establishment/strengthening of a social infrastructure, namely information security infrastructure, it is necessary to consider it as a task requiring continuous and mid-term efforts beyond a yearly timeframe, rather than as a task for the single fiscal year of 2007.

Considering the facts that cyber space is beyond the framework of nation-states, that the impact of IT-malfunction is not confined to one county, that our socio-economic activities are not always conducted within one country alone, and that mutually dependent relationships in the international community are deepening, international partnership/cooperation is a task to be actively addressed from two-way approaches: “Japan in the world” and “the world for Japan”. Objectives of FY2006 in the relevant fields have been achieved in general with the steady implementation of efforts. However, the objectives are only the first step, and it is sill necessary to launch full-fledged action as an international instrument for information security measures. For these issues, acceleration of efforts with a mid-term vision should be considered a necessary task.

Furthermore, there are tasks to be undertaken rapidly and intensively as urgent issues in FY2008, including responses to risks that emerge suddenly. Since various efforts are presently in

place for the establishment of E-Government, it is important to take comprehensive measures, including establishment of system that promote verification and strengthening of measures from the information security perspective, in an appropriate manner and at an appropriate time.

Chapter 3: Strengthening of Information Security Measures in Four Implementation Fields

Information security measures in Secure Japan 2007, as in Secure Japan 2006, are grouped into four areas in accordance with the implementation entities, namely, the central government/local governments, critical infrastructures, businesses, and individuals, and specific measures are set forth according to the characteristics of each.

Section 1: Central Government/Local Governments

A: Central Government

The Central Government of Japan, in continuation of efforts from FY2006, prioritizes the promotion of the following measures in government agencies, with the purpose of 1) upgrading the level of the Standards for Measures[2] to the world's highest level by FY2008 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 pull up 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 established by (1) inspecting and evaluating the degree of 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 evaluation results to the improvement of the measures and of the Standards for Measures. Moreover, the results of evaluations are disclosed with due regard to preserving /ensuring 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 that contractor deploy.

[2] "The Standards for Measures" is the "Standards for Information Security Measures for the Central Government Computer Systems" (decision made on December 13, 2005 by ISPC. The same applied to hereinafter)

[Specific Measures]

A) Implementation of the review of the Standards for Measures (Cabinet Secretariat)

Based on the changes in technology and environment, Standards for Measures will be reviewed in FY2007. In so doing, analysis will be carried out on the IT-malfunctions that occurred within and outside the government agencies, and the results will be properly reflected.

B) Establishing PDCA Cycle

a) Establishing PDCA Cycle at each government agency (All government agencies)

Each government agency will pursue the upgrading through concerted action, by establishing a PDCA cycle within FY2007, such as taking initiatives in improving the measures based on the results of self-assessment and auditing of implementation of information security measures.

Particularly, in FY2007, by expanding education for all employees, each government agency will increase awareness of information security, ensure a thorough compliance with the standards of the government agency, improve and enhance the implementation system for self-assessment and auditing, and appropriately monitor the progress of measures.

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

The Cabinet Secretariat will stabilize the PDCA Cycle of the entire government in FY2007, by assessing and evaluating the progress of measures taken by the government agencies in accordance with the Standards for Measures, by linking the recommendations obtained from the evaluations to the improvement of the measures and upgrading of the Standards for Measures, and by developing an environment to ensure the systems necessary for each government agency.

C) Promotion of full-scale evaluations and disclosure of the results

The Cabinet Secretariat will conduct full-scale evaluation and promote improvement in information security measures in each government agency from the following perspectives. These efforts are based on the “Evaluations, etc., toward Realization of Secure Japan and Promotion of Reasonable and Continuous Improvements” (decision made on February 2, 2007 by ISPC) and “The Best Form of Japanese Society and Evaluation of Measures” (decision made on February 2, 2007).

Implementation of routine evaluations will, in principle, be enforced based on the predetermined schedule and inspection items presented to each government agency from

the Cabinet Secretariat, except for cases in need of urgency, etc.

The results of evaluations are regarded as contributing to the promotion of effective measures and to the accountability of the entire government and will be disclosed with consideration to preserving and ensuring information security.

a) Evaluations, etc. on implementation of measures (Cabinet Secretariat)

Evaluations on implementation of measures based on the Standards for Measures of each government agency will be conducted on a full-scale in an objectively comparable way, in line with the evaluation method established in the evaluations of FY2006 and based on the reports of implementation of measures, as well as on the intensive inspections on the specific prioritized items.

b) Evaluation, etc. on information security management (Cabinet Secretariat)

Evaluations on information security management of each government agency will be conducted to promote improvement of information security measures.

In the first half of FY2007, evaluations will be conducted on a trial basis on the efforts of each government agency made in FY2006 and method of full-scale evaluations will be established in such a form as to be effective for establishing a PDCA Cycle of the entire government and to enable objective comparisons.

D) Support for the efforts based on the Standard for Measures and promotion of effective operation

a) Provision of information security related information (Cabinet Secretariat)

In order to promote the support for information security measures in each government agency, the Cabinet Secretariat will continue providing each government agency with information security-related information and proper advice, including technical information.

b) Efforts to tackle common issues of government agencies on information security measures (Cabinet Secretariat and all government agencies)

In order to facilitate efforts based on the Standards for Measures, the Cabinet Secretariat will address common issues in a concerted manner by providing opportunities to study measures to common operational issues on information security measures with participation of government agencies.

c) Sharing of Best Practices for information security measures (Cabinet Secretariat and all government agencies)

In order to promote sharing of knowledge on information security measures in government agencies, the Cabinet Secretariat will organize information security measures implemented in each government agencies and the response measures obtained from above mentioned inspections, etc that are worth being referred to as “Best Practices” and will promote those materials to be shared among government agencies. These practices will be organized and disclosed in such a way as to be used by private corporations, local governments and incorporated administrative agencies, as much as possible.

d) Improvement of efficiency (Cabinet Secretariat)

In order to ensure solid implementation of information security measures in each government agency based on the standards for government agencies in line with the Standards for Measures, the Cabinet Secretariat will study methods of improving efficiency, including development of IT, etc., concerning operations associated with education, self-assessment and auditing, and present the result of the study to each government agency in the first half of FY2007.

e) Integrated understanding of information systems of each government agency (Cabinet Secretariat and all government agencies)

In order for each government agency to understand and implement the information security measures for the information systems it possesses in an integrated and appropriate manner, each government agency will record the information handled by each information system and items related to information security, including the classification of the relevant information in the information asset registry, etc, which is compiled by each government agency.

E) 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 continuously in FY 2007 by, for example, enforcing strict control on removing internal information, and using private computers for office work at each government agency.

F) 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 continuously in FY 2007 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 continuously in FY 2007 on an as-needed basis.

c) Use and spread of Guidelines for Improving Reliability of Information Systems (Cabinet Secretariat and Ministry of Economy, Trade and Industry)

Guidelines for Improving Reliability of Information Systems will be utilized and prevailed throughout government agencies. These Guidelines stipulate measures to improve reliability of all information systems from a comprehensive perspective, including the aspect of process managements, such as development and operations, technique, and organization.

G) Support for selection/procurement of information security oriented systems (Cabinet Secretariat and Ministry of Economy, Trade and Industry)

In order to effectively and efficiently perform the procurement of IT systems with consideration to information security in each government agency, Information-technology Promotion Agency (IPA) will develop a support tool to verify the IT security requirements, IT security evaluations and the suitability of the use of authentication products in the authentication system, and at the same time, the use of the relevant tool will be promoted through the feedback on the manuals related to the Standards for Measures.

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 don't have their own policies, 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 agencies overseeing incorporated administrative agencies)

Each government agency will request the incorporated administrative agencies under its jurisdiction to formulate/review their information security policies, referring to the Standards for Measures, and provide necessary support, etc. for them.

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

An environment will be developed for improving information security measures, by for example, providing incorporated administrative agencies, etc. with information necessary for the promotion of formulation/review of their information security policies.

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

The government will make efforts for the implementation of the 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 details of which are described below.

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

When optimizing 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 continuously in FY 2007.

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

and all government agencies)

Continuously in FY2007, 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 CCRA (Common Criteria Recognition Arrangement) Information Technology Security Evaluation and Certification Scheme[3] 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 comprehensively consider introducing a new system (function), such as IPv6, IC card for identification of government officials, data encryption, electronic signature, and biometric authentication, etc., and promote the realization of those systems.

Particularly, in order to expedite facilitating information systems being able to handle IPv6 at all government agencies, information and telecommunications equipments and software will be made capable of handling both IPv4 and 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 Communications)

Discussions will be further elaborated with regard to the technology and functions necessary for creating and developing a common platform to serve as a foundation of operations and systems of the entire government for the establishment of next generation E-Government, and a conclusion will be drawn by the end of FY2007.

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, Virtual Machine (VM) and a minimum level of OS functions to back up the operation of VM (hereinafter

[3] CCRA (Common Criteria Recognition Arrangement) Information Technology Security Evaluation and Certification Scheme 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.

collectively referred to as “Secure VM”) is urgently needed to ensure the reliability of IT and development of secure VM will be promoted through cooperation between industry, academia and government continuously from FY 2006. VM will enable intensively providing information security functions independent of the existing OS and applications environment.

C) Developing innovative machine reality technology equipped with a mechanism to consolidate and intensively manage information access right.(Ministry of Economy, Trade and Industry)

Development of innovative virtual machine technology (Secure Platform) will be launched in FY2007. It is equipped with a mechanism to consolidate and intensively manage information access right which have previously been configured separately by each information system, in addition to consolidating multiple information systems into single server.

D) Enhancement of information security measures in the police force (National Police Agency)

National Police Agency will start to install software which automatically encrypts information stored in external storage media into general business terminals in FY2007.

E) Establishment of evaluation criteria for the quality of OS security used for E-Government (Cabinet Secretariat)

After consideration on establishing evaluation criteria for the quality of the OS security that supports the information systems of E-Government, and the efforts made to establish all the necessary evaluation items and criteria usable for system procurement in FY2006, a technological survey on the system installation of the OS towards full-fledged launch of E-Government, etc will be conducted in FY 2007.

F) Migration 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 enable its information and communications equipments and software to handle 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) In FY2007, each government agency will examine the effect of enabling E-Government systems to handle IPv6, while referring to the guidelines on IPv6 application to E-Government systems formulated in FY2006, and develop detailed plan to enable information systems to handle IPv6.
2) In order to enable access to e-applications by the general public using IPv6, Internet service providers need to provide IPv6 connection services to individual users. The Ministry of Internal Affairs and Communications will provide information pertaining to the availability of IPv6 connection services by the Internet service providers on the website continuously in FY 2007.

G) Promotion of the use 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, for which methods are independently adopted by each e-administration service of government agencies, levels of authentication strength will be sorted and clarified according to the risks involved, and the use of the Guidelines for Authentication in E-Government (tentative) by government agencies will be promoted in FY 2007 in order to promote cooperation between administrative services while maintaining safety.

H) Consideration for the direction of developing personal authentication in E-Government from a mid- and long-term perspective (Cabinet Secretariat)

In order to contribute to the best form of personal authentication in Japan from a mid- and long-term perspective in view of improving safety and security regarding personal authentication in E-Government, the Cabinet Secretariat will examine various types of institutions and systems with regard to personal authentication deployed in other countries.

(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[4] that certify the identity of government agencies will be promoted to make the genuine government agencies easily identifiable.

[4] 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.

[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)

The use of domain names that authenticate the identity of government agencies is being expanded, and continuous efforts will be made to use the relevant domain names when government agencies transmit information to the general public, in principle by March 2008.

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 from government agencies, discussions will be held concerning the development of an environment where users such as the general public and private corporations are able to use e-documents safely, by performing e-signatures to e-mails sent by government agencies and e-documents downloaded through websites of government agencies: specifically, considerations will be made on a best forms of intra-government systems for performing e-signatures, and a conclusion will be reached within FY2007.

(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 2007.

B) Consideration 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 2007, responsive procedures and implementation systems to be taken in case E-Government Recommended Ciphers are compromised will be promptly furnished in

Cabinet Secretariat, and at the same time, considerations will be made on a promotion system within the government regarding the use of ciphers, including review of the nature of the E-Government Recommended Ciphers.

C) Response to reduced safety of the SHA-1 hash function (Cabinet Secretariat, Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry and all government agencies)

CRYPTREC (Cryptography Research and Evaluation Committees) Advisory Committee Group reports that it is not necessary to immediately suspend the use of the SHA-1 hash function, which is widely used for information systems in E-Government, but its encryption strength has been reduced. Therefore, the following measures will be taken in government agencies, considering the lifecycle, etc., of information systems in these agencies.

1) Each government agency will take either of the following actions when newly establishing (including renewals) information systems which use the hash function over a long period of time, such as e-signature or time stamp.

(i) Choose hash function with length of 256-bit or more.

(ii) Where SHA-1 is continuously used, develop a structure to allow for response measures, such as rapidly changing to a different algorism, immediately after an attack method of realistic threat is observed.

2) When changing the hash function choice, it is necessary to consider compatibility between related information systems. Thus, the Cabinet Secretariat will identify specific issues on information systems that affect wide areas, such as authentication infrastructure system and e-application system, etc., with cooperation from Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry and related government agencies. Based on the results, policies will be formulated on the change in the hash function by government agencies at an early date in FY2007.

3) Safety of SHA-1 will continue to be monitored by Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry. The Cabinet Secretariat will promptly provide each government agency with necessary information.

D) Promotion of the use of cryptographic modules that are highly safe and reliable (Cabinet Secretariat, Ministry of Economy, Trade and Industry and all government agencies)

In order to promote the use of highly safe cryptographic modules, Japan Cryptographic Module Validation Program (JCMVP) implemented by IPA will be promoted in FY2007. When procuring cryptographic modules, priority is given to the products certified by the relevant system as required.

E) Promotion of security measures for files (electronic documents) (Ministry of Defense)

Installation of file protection software, which was developed in FY2006, will be promoted in order to ensure security at the time transferring data to portable storage media.

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

In order to promptly and appropriately respond to emergencies, such as cyber attacks, and adapt to technology or environmental changes, specific system will be established that is capable of sharing information among the government bodies and analyzing the information in an integrated manner, and taking appropriate measure according to the analysis. At the same time, emergency response capability will be strengthened by improving the capability of related responding agencies, and thus equipping response systems, and also by incorporating newly acquired knowledge from the past experience of emergency responses into 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) Establishing inter-governmental response system (development of GSOC) (Cabinet Office and all government agencies)

In order to ensure prevention of occurrences of cyber attacks against government agencies, information leakage from government agencies, and system failures, etc., and to more rapidly and accurately respond in the unlikely event of difficulties, the Government Security Operation Coordination team (GSOC) will be established, envisioning a full-fledged operation in FY2008. The system will collect inter-governmental information, analyze attacks, etc., give advice to each government agency, promote mutual partnership and share information, in preparation for its full-fledged operation in FY2008.

In FY 2007 the following functions will be improved: the real time monitoring function on the information systems of some government agencies, the collecting function of intergovernmental monitoring information and analysis function of attacks, etc. in the Information Security Center, Cabinet Secretariat. At the same time, the system will be strengthened to give advice to each government agency based on the relevant analysis results, to promote mutual partnership between government agencies, and to conduct information sharing. In so doing, state-of-the-art technologies which have been developed by various organizations will be effectively utilized.

b) Research and study of the most advanced technologies for information assurance

(Ministry of Defense)

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., continuously in FY 2007.

B) Strengthening of emergency response capability of each government agency

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

In order to rapidly and accurately respond to IT-malfunctions in accordance with manuals in each government agency, response measures to individual IT-malfunctions which are likely to occur frequently in government agencies will be developed and disseminated in FY2007. Furthermore, in order to detect the symptom of relevant IT-malfunctions and to implement measures in accordance with response policies, ever changing characteristics of IT-malfunctions will be considered and reflected on the monitoring function and analysis function etc. of the information system of government agencies, and a system to facilitate items described above will be strengthened within FY2007.

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 2007, including providing 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 with regard to cyber attacks (Ministry of Defense)

In order to further enhance analysis and response capability concerning countermeasures for cyber attacks against information systems of Ministry of Defense, analysis equipment for cyber protection will be developed and start operations. Basic research will be performed on monitoring and analyzing technology against unauthorized computer access, cyber attacks and active protection technology, etc. continuously from FY2006.

d) Establishment of an integrated communication squadron (Ministry of Defense)

With respect to information communication of the self-defense forces, a permanent integrated squadron will be established in FY2007 to take on dynamic roles such as

appropriate and timely recovery of functions in the event of cyber attacks, in addition to static roles such as the maintenance of functions.

5) Human Resource Development of Government Agencies

In order to proceed with information security measures of the entire government in an integrated manner and taking the importance of developing and ensuring human resources with necessary knowledge and expertise into consideration, 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, human resource development efforts 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

a) Consideration for education programs for government officials (Cabinet Secretariat and all government agencies)

In FY2007, discussions will be held concerning integrated education programs for the government to furnish government staff with minimum knowledge about information security with a purpose of contributing to the use of safe information technology by government staff. The programs will be implemented in order of feasibility.

b) Consideration for education programs for government officials (Cabined Secretariat, Ministry of Internal Affairs and Communications and all government agencies)

In FY2007, discussions will be held concerning integrated education programs for government officials, including the use of existing training programs, with the purpose of contributing to the awareness/understanding of risks associated with information security. The programs will be implemented in order of feasibility.

c) Consideration for education programs for government officers in charge of information security measures (Cabinet Secretariat, Ministry of Internal Affairs and Communications, and all government agencies)

In FY 2007, discussions will be held concerning integrated education programs for the government officers in charge of information security measures, including the use of the Integrated Information System Training conducted by Ministry of Internal Affairs and Communications, with the purpose of contributing to the improvement of expertise of

responsible government officers. The programs will be implemented in order of feasibility.

d) Formulation of plan for developing/ensuring human resources (all government agencies)

In order to develop and ensure human resources with knowledge and capability, including information security, that contributes to the safe and secure use of information systems, each government agency will formulate the "Plan for the Developing/Ensuring IT Human Resources" based on the "Guidelines for Developing/Ensuring IT Human Resources in Administrative Agencies" (decision made on April 13, 2007 by the CIO (Chief Information Officer) Council at an early date by the end of FY2007.

B: Local Governments

The following measures will be intensively promoted continuously from FY2006, aiming to promote information security measures based on the guidelines for ensuring information security in local governments, which was reviewed in September 2006, and various measures, including information security auditing and training, etc., and to facilitate the function of the information sharing system of local governments (Local Government CEPTOAR) which was established in FY2006.

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) Formulation of manuals for information security measures in local governments (Ministry of Internal Affairs and Communications)

In FY2007, a manual will be formulated that serve as a reference for analyzing the current situation and issues and for specific implementation and operation of information security measures, with respect to information security measures (risk analysis of information assets, etc.) that are not sufficiently implemented by local governments.

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 a review of effectiveness, the Guidelines for Information Security Auditing by Local Governments will be reviewed in FY2007 and information security auditing will be promoted in line with the guidelines given above.

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

In order to contribute to proactive prevention of IT-malfunctions and its expansion, prompt restoration 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) Support for the Local Government CEPTOAR (Ministry of Internal Affairs and Communications)

The Local Government CEPTOAR was established in FY 2006 to share information pertaining to information security among local governments. In FY2007, support, such as necessary advice, will be provided so that the Local Government CEPTOAR can function effectively.

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

Training for local government officials will be supported in FY 2007, including training to bring up 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 operations of local government.

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 2007.

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 information security circumstances.

[Specific Measures]

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

a) Review of "Safety Standards, Guidelines, etc." (Agencies overseeing critical infrastructures[7])

In view of the revision of the principle which is scheduled in June 2007, confirmation/ verification of safety standards in critical infrastructures will be performed in around September 2007 and measures such as revision will be undertaken as necessary.

b) Understanding and verifying the situation of review of Safety Standards, etc. (Cabinet Secretariat)

The situation of review of Safety Standards, etc. in each critical infrastructure will be monitored with the cooperation of competent authorities from each critical infrastructure and verification based on the outcomes of interdependency analysis will be conducted within FY2007.

[5] "Safety Standards, Guidelines, etc." refer to documents formulated as criteria or references used by business entities that own or operate 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 overseeing critical infrastructures" refer to ministries and agencies that directly deal with Business entities that own or operate 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))

B) Implementation of studies on the dissemination of Safety Standards, etc. in each sector of critical infrastructure (Cabinet Secretariat and agencies overseeing critical infrastructures)

In FY2007, the Cabinet Secretariat will implement studies on the dissemination of Safety Standards, etc. in each sector of critical infrastructure, which was formulated/revised in FY2006.

C) Review of the Principles (Cabinet Secretariat)

Based on the outcomes of interdependency analysis, the Cabinet Secretariat will review the Principles within FY2007, with cooperation of agencies overseeing critical infrastructures.

D) Safety and reliability assurance of telecommunication systems responding to the transition of IP network (Ministry of Internal Affairs and Communications)

In order to ensure stable provision of ICT services to meet the progress of the IP network, Ministry of Internal Affairs and Communications will implement necessary measures for safety and reliability in network facilities and in operation and management within FY2007.

2) Enhancement of information sharing system

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

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

In cooperation with related organizations, information, such as caution, to be provided to business entities that own or operate 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 that own or operate critical infrastructures provide the government with information on incidents, failures, and operational delays, etc., to be submitted to the

government 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)

The Cabinet Secretariat will consider the functions/requirements to be added to the information sharing system between the public and private sectors, which was developed in FY2006, in response to the development of CEPTOAR as well as the changes in the development of CEPTOAR-Council (tentative) in each sector.

(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 that own or operate critical infrastructures and will be shared among them. This will eventually contribute to the improvement of capability of each business entities that own or operate critical infrastructures to maintain and reconstruct their services. In order to contribute to this mission, the government will promote the development of Capability for Engineering of Protection, Technical Operation, Analysis and Response (CEPTOAR) that perform information sharing and analysis within each critical infrastructure sector.

[Specific Measures]

A) Promotion of the development of CEPTOAR in each critical infrastructure (Agencies overseeing critical infrastructures)

Action will be taken to develop CEPTOAR in newly added sectors (water system, medicine, distribution) by the end of FY2007.

B) Follow-up of the “Map for Understanding the Characteristics of CEPTOAR” (Cabinet Secretariat)

Cabinet Secretariat will study the progress of discussions and development of functions/requirements of CEPTOAR in each sector within FY2007. Also, by the end of FY2007, follow-ups of the “Map for Understanding the Characteristics of CEPTOAR” will be performed.

(c) Promotion of establishment of "CEPTOAR-Council (tentative)"

In order to promote cross-sectoral information sharing among business entities that own or operate critical infrastructures and utilize knowledge for continuity and restoration 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 and agencies overseeing critical infrastructures)

Meetings will be held and related issues will be discussed aiming at reaching a basic agreement on the establishment of CEPTOR-Council within FY2007.

3) Implementation of analysis of interdependency

In order to grasp the cross-sectoral situation to improve critical infrastructure protection throughout the nation, the government will make efforts to understand what kind of potential threats each critical infrastructure has and what kind of interdependency exists as to what impact will ripple through other critical infrastructures when an IT-malfunction occurs in a critical infrastructure.

[Specific Measures]

A) Promotion of interdependency analysis between critical infrastructures (Cabinet Secretariat)

In response to further advancement of IT in critical infrastructure sectors and increased interdependency between sectors, and in order to improve the capability regarding communication/coordination function and the response capability of public and private sectors in the event of IT-malfunctions, including business continuity, the Cabinet Secretariat will deepen discussions on the similar types of threats observed both inside and outside the country, causal relations between threats and disruptions, relationship between disruptions and business continuity, and will also reflect the results in the exercise scenario. At the same time, the Cabinet Secretariat will promote dynamic dependency analysis to dynamically understand the propagation process of a chain reaction from occurrence of disruption to spread/expansion of damage in critical infrastructures. Thorough discussions will be held on the method of implementation, before actual implementation.

4) Implementation of cross-sectoral exercises

Based on a type of a specifically envisioned threat scenario, cross-sectoral exercises will be performed under cooperation among presiding ministries of each critical infrastructure, each business entities that own or operate critical infrastructures and CEPTOAR in each critical 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 step by step. Furthermore, through these exercises and other training and seminar sessions, personnel with advanced IT skills will be developed and ensured, primarily for presiding ministries of each critical infrastructure and business entities that own or operate critical infrastructures.

[Specific Measures]

A) Implementation of functional exercises in critical infrastructures[8] (Cabinet Secretariat and agencies overseeing critical infrastructures)

In order to improve communication/coordination functions and response capability of public and private sectors in the event of IT malfunctions, Cabinet Secretariat will select themes based on a specific type of assumed threat scenario and conduct cross-sectoral functional exercises in FY2007, while referring to the knowledge obtained from the interdependency analysis, with cooperation from agencies overseeing critical infrastructures, business entities, and CETOAR in each sector of critical infrastructure, etc.

B) Strengthening of response against cyber attacks in the telecommunications field (Ministry of Internal Affairs and Communications)

By the end of FY2008, in order to develop human resources with advanced ICT skills that will help strengthening cooperation and facilitating coordination, in case of emergency, among concerned operators, and between operators and governments, the competent agencies will conduct cyber attack response exercises in FY2007, as in FY2006, supposing cyber attacks that may occur on the internet that connect each critical infrastructures with focus on telecommunications operators.

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

In exercises conducted by the Cabinet Secretariat, coordination will be facilitated, while giving due consideration to consistency with the forms of cyber exercises implemented in each sector, such as telecommunications, etc., and with its objectives.

[8] Mock exercise for validation using the command and decision system of actual organizations

5) Review of "Action Plan on Information Security Measures for Critical Infrastructures"

[Specific Measures]

A) Review of "Action Plan on Information Security Measures for Critical Infrastructures" (Cabinet Secretariat)

In FY2007, investigation/understanding on the progress of the improvement of information security in critical infrastructures will be conducted/obtained, in preparation for the review of "Action Plan on Information Security Measures for Critical Infrastructures". In so doing, discussions will also be made on ensuring consistency and cooperation with other related cross-ministerial approaches, such as responses to disasters, etc. Also, discussions on public-private partnership will continue.

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 2007.

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, if necessary, evaluation results on the level of information security that is derived from said systems or third party evaluation will be used as one of the conditions for public bidding for procurement of information systems, etc. 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 (Ministry of Economy, Trade and Industry)

In order to establish Information Security Governance in corporations, discussions will be conducted in FY2007 as to how to disseminate best practices of information security measures in corporations and to promote information security classification by private organizations.

PR activities will continuously be conducted to recommend the use of the "Guidelines for Improving the Reliability of Information System" as a reference when each company establishes and operates information systems. Furthermore, in order to contribute to the dissemination and promotion, "Evaluation Criteria for Improving Reliability of Information System (tentative)" will be established and evaluation tools will be provided within FY2007.

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

In order to contribute to the establishment and operation of information security systems in telecommunications services, efforts will be made for the dissemination and promotion,

including authentication, of the Information Security Management Guideline for Telecommunications (ISM-TG), which is the guideline in the telecommunications services formulated in FY2006 by the Information Security Conference for Telecommunications (ISeCT), which comprises telecommunications service providers and related organizations.

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

For government procurement of information system related products, discussions will be held among related government agencies with regard to the method of taking the assessment on the implementation level of information security of bidders into bidding conditions. Conclusion will be reached within FY2007.

C) Promotion of standardization for information service management, emphasizing information security control (Ministry of Economy, Trade and Industry)

In FY2007, JISQ 20000-1 (Information-technology Service Management, Part 1: Specification=ISO/IEC20000-1) and JISQ20000-2 (Information-technology Service Management, Part 2: Standards for Implementation=ISO/IEC20000-2) will be established as Japanese Industrial Standards to be used by information service providers in pursuit of improving quality of information services and customer satisfaction by planning, inspecting and continuously improving information service management with emphasis on information security control.

D) Promotion of information security measures in small- and medium-sized enterprises (Ministry of Economy, Trade and Industry)

In order to reduce the burden of information security measures on small- and medium-sized enterprises and promote it, discussions will start in FY2007 on the package of information security measures for small- and medium-sized enterprises and the standard format to verify implementation of the measures.

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

The information security measures intrinsically have functions different from those are necessary to accomplish original business and are to be implemented according to the risks pertaining to the business, and they have such characteristics that it is difficult to make them recognized visually, etc. Due to these characteristics, it is necessary to create an environment that enable businesses 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 the risk quantification method concerning information security (Ministry of Economy, Trade and Industry)

In order to improve the organization- and human-oriented management methods, research and development activities will continue to be implemented in FY2007, including quantification concerning information security in organizations, and measuring of cost efficiency involved in information security measures. Discussions will also be held on unique risks of offshore outsourcing.

B) Promotion of the use of third party evaluation

a) Promotion and 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 2007 on viable standards for the provision of high quality audit services to meet various needs, while seeking consistency with international standards.

In specific terms, in order to disseminate an assurance-based information security audit in which an auditor provides some assurance, discussions will be held on formulation of guidelines for the use of assurance-based audit.

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

In FY2007, Japan Information Technology Security Evaluation and Certification Scheme (JISEC) implemented by IPA will be promoted. At the same time, the use of the systems at the time of information system procurement will be expanded through such efforts as developing support tools to determine the availability of authentication products for the

systems. Japan Cryptographic Module Validation Program implemented by IPA will also be promoted.

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 2007 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 2007 through dissemination and PR activities of the tax system for strengthening the information infrastructure to increase industrial competitiveness.

D) Improvement of indices for companies (Cabinet Secretariat and Ministry of Economy, Trade and Industry)

Based on the "The Best Forms of Japanese Society and Policy Assessment from the Perspective of Information Security" (understanding made on February 2, 2007 by ISPC), several new surveys will be launched in FY2007, in addition to the usage of information security audit systems in companies, which was previously learned from the Survey on Information Processing. The surveys will investigate the compatibility assessment system for information security management systems in companies, use of system benchmarks for information security measures, confirmation of implementation of information security measures of business partners (including outsourcing and consignment), and introduction of the products accredited by ISO/IEC15408.

Also, in FY2007, based on the "Comparison with the Situation of Government Agencies" contained in the above-mentioned understanding, the Cabinet Secretariat will study methods of identifying what kind of data is lacking by comparing government indices with company indices and will gain an understanding of the situation as data becomes available, with the cooperation of government agencies.

3) Ensuring/Developing 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 made to maintain motivation of personnel engaged in implementing information security measures in each company.

[Specific Measures]

A) Support system for training projects for human resources engaged in telecommunications (Ministry of Internal Affairs and Communications)

Support will also be provided for training activities to develop human resources engaged in telecommunications, including security personnel who have professional knowledge and expertise in the area of information and telecommunications, continuously in FY2007.

B) Strengthening of functions of self-check tools for IT users in organizations (Ministry of Economy, Trade and Industry)

Indices to objectively measure the level of information security measures for IT users in organizations will be discussed and functions of self-check tools by using the indices will be strengthened within FY2007.

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 enterprises and information system personnel, “Information Security Seminars”, co-hosted by IPA and the Japan Chamber of Commerce and Industry will be held throughout the country in FY2007. Furthermore, discussions will be conducted on the dissemination and public relation activities in coordination with IT business supporters, as well as on the information collection/provision systems concerning the trend of information security related matters in other countries.

D) Establishment of a mechanism of objective evaluation for advanced IT human resources (Ministry of Economy, Trade and Industry)

Aiming to establish a mechanism to objectively evaluate human resources, a framework of common careers/skills will be developed in FY2007 to systematically identify the skills required for advanced IT human resources including those engaged in information security.

E) Setting up the Council for Industry-Academia-Government Collaboration (Ministry of

Economy, Trade and Industry)

In FY2007, the competent agency will set up the Council for Industry-Academia-Government Collaboration to counsel on the type of advanced IT human resources needed in the industry and the practical methods of developing advanced IT human resources in the industry and education field.

F) Support for faculty development (Ministry of Education, Culture, Sports, Science and Technology and Ministry of Economy, Trade and Industry)

In order to promote practical education in each information technology field, including information security, support will be provided to the efforts for faculty development (FD) of universities and so on will be supported to improve ability of teachers.

G) Reform of examination system for information processing engineers (Ministry of Economy, Trade and Industry)

In order to enhance the development of advanced IT human resources including information security field, the examination system for information processing engineers that measures skills in information technology field including information security will be drastically reviewed and a new examination system is scheduled to be launched in FY2008, upon ensuring consistency with the framework of common careers/skills.

H) Establishing a human resources development system for advanced telecommunications (Ministry of Internal Affairs and Communications)

In order to develop the human resources playing an important role in information strategies of corporations and in creating new businesses, practical Project Based Learning (PBL) materials in ICT management sector, including telecommunications security, will be developed in FY2007.

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 between related organizations and enhance a coordinated response system to rapidly respond to computer viruses or vulnerabilities, etc, with proactive cooperation of industries engaged in information-related businesses.

[Specific Measures]

A) Enhancement of coordination scheme among emergency response teams of organizations (Ministry of Economy, Trade and Industry)

In order to provide information on threats and response measures directly to the possible target organization of attacks, discussions led by the Japan Computer Emergency Response Team Coordination Center (hereinafter referred to as "JPCERT/CC") will be undertaken in FY2007 on enhancement of capability to analyze related information obtained from Computer Security Incident Response Teams (hereinafter referred to as "CSIRTs") within and outside the country, and on improvement of coordination among CSIRTs within organizations.

B) 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 information security issues that are becoming more sophisticated day by day 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 JPCERT/CC in FY 2007.

Specifically, discussions will be held on enhancement of information gathering concerning information security issues, mechanisms to effectively and efficiently transmit gathered information and strengthening of international cooperation, etc.

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

In order to ensure the safety of websites, the competent agency will commence deliberations in FY 2007 on guidelines regarding security requirements to be presented by the consigners to the developers (consignees) when creating web applications.

D) Development of evaluation criteria for the degree of importance and priority of vulnerabilities of software, etc. (Ministry of Economy, Trade and Industry)

The Ministry of Economy, Trade and Industry will develop a framework of information provisions that allows vendors and users to quantitatively compare the seriousness of vulnerability in IPA and JPCERT/CC under internationally consistent standards and to make decisions on the degree of importance and priority of measures. The Ministry will also install support tools for decision making on priorities of measures in accordance with the environment of each user, and the operation is scheduled to start in FY2007.

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 2007.

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 and diversified 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 elementary and secondary education and inter-generation information security education.

[Specific Measures]

A) Promotion of information security education from elementary and secondary education

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

The competent agency will conduct discussions on the effective instruction methods for information morals, etc., including information security, compile examples of instructions, and create a website to widely introduce them for dissemination among teachers. Also, targeting teachers' consultants and teachers, the competent agency will hold forums to disseminate instructions on information morals, etc. including information security, in an attempt to further promote information security education.

b) Research and development of methods to foster ICT media literacy[9] (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 conducted research and development activities on new methods to foster ICT media literacy, such as the development of instruction manuals and teaching materials on comprehensive literacy required for the use of ICT media in FY 2006. The developed programs will be made publicly available and be widely disseminated to organizations engaged in fostering ICT media literacy in FY2007 and onwards.

[9] 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 and posters for "information security measures" (Ministry of Economy, Trade and Industry)

In FY 2007, in order to contribute to reducing the damage by computer viruses or hacking, the IPA will solicit slogans and posters for raising awareness on information security measures from students of primary, middle and high schools and publicize the winners' works.

d) Improving teaching abilities for information security (Ministry of Education, Culture, Sports, Science and Technology)

In light of the fact that "the ability to educate students and pupils on information security" is listed in the checklist on teaching abilities for ICT, which was compiled in FY2006, the competent agency will conduct a national survey within 2007 and will improve teaching abilities for ICT to enable all teachers to provide guidance on information security.

B) Promotion of cross-generational information security education

a) Promotion of nation-wide information security education (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 2007 by continually holding such classes throughout the country.

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

A course of lectures on safe and secure use of the Internet, primarily targeting guardians and teachers, will be conducted on a national scale continuously from FY 2006, in cooperation with telecommunications-related organizations. Furthermore, holding of international cooperative events, etc. will be considered.

c) Cyber Security College (National Police Agency)

In FY2007, in order to raise awareness/knowledge of information security, lectures and seminars on the current situation of cyber crimes and cyber crime cases will be held, targeting educators, local government employees, general users of the Internet, etc.

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 public awareness of information security, given the reality of rapidly advancing and complicated 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 2007, through such approaches as "*@police*", "Information Security Website for the Public", "Antiphishing Japan", and the "Council for Promoting Measures against Phishing", etc., as well as through the "CHECK PC! Campaign", envisioning cooperation with activities conducted by related companies and organizations, etc.

These efforts will focus not only on IT beginners, but also on active users with less benefit in information security.

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 continuously from FY 2006 through such approaches as disclosure of the occurrences of unauthorized computer access and the progress of research and development for access control functions.

c) Promotion of measures to prevent damage from improper Internet use (National Police Agency)

In order to prevent damage from cyber crime, etc., the competent agency will provide advice on the basic measures tailored for the problems individual users might experience, using consultation systems for safety and security of the Internet, continuously from FY2006.

In order to prevent damage from cyber crime, the competent agency will effectively implement PR and enlightenment/information collection activities by, for example, actively receiving information pertaining to cyber crime.

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 in which people are able to purchase and use radio equipments safely, the competent agency will implement dissemination and PR activities continuously from FY2006 to encourage people to check the “label to verify the compliance with technology standards”, which is attached to radio equipments, through the use of mass media, posters and the 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 people's awareness of information security, the competent agencies will undertake nation-wide PR and education activities, based on the concept of the “Information Security Day”, which is held on February 2 every year.

The competent agencies will also award individuals and organizations with prominent contributions and achievements in information security.

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

a) Continuous issuance of e-mail magazine of the National Information Security Center (Cabinet Secretariat)

In order to rouse public opinion and provide information pertaining to information security on a daily basis, the competent agency will continue to issue e-mail magazines on an approximately monthly basis in FY 2007.

b) Announcement of award of the information security promotion category of the Information Promotion Contribution Award (Ministry of Internal Affairs and

Communications, Ministry of Economy, Trade and Industry)

During the Information Month in FY2007, an "Information Promotion Contribution Award (category of information security promotion)" will be announced to recognize individuals and companies, etc. with outstanding contributions to ensuring information security.

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, the English version of "Secure Japan 2007" will be posted on the English website of the National Information Security Center (NISC).

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 stop cyber attacks (Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry)

Trials and discussions, including the technical and practical aspects, will be carried out with an aim to establish a comprehensive framework by FY 2010 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 stop spam mails and cyber attacks from entering through bot-infected computers without imposing an excessive burden on individual users.

Also planned is an information exchange with related overseas organizations on Japan's commitment will be carried out as necessary.

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[10] by FY 2009, empirical experiments, which model the user environment, will continue in FY 2007 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 2007, the competent agencies will further promote dissemination of the guidelines entitled “For Safe Use of Wireless LAN” and at the same time, improve the contents of pamphlets and handouts concerning the safe use of wireless LAN, such as the pamphlet on the “Internet Safety Class”, which serves as a tool for PR and enlightenment activities for general users.

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

Chapter 4: 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, developing and ensuring human resources engaged in information security, promotion of international partnership and cooperation, crime control, and protection and redemption of rights and benefits.

Section 1: Promotion of Strategy concerning Information Security Technology

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

In FY2007, the ISPC, in cooperation with the Council for Science and Technology Policy, will start assessing the implementation progress of R&D and technology development relating to the information security of Japan through cooperation among 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 implement full-scale assessments (1:ex-ante, 2:mid-term, and 3:ex-post) on the effects of investment in R&D and technology development relating to information security technologies in FY 2007, and results will be promptly made available for public.

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

The competent agencies will continue discussions in FY 2007 on policies to allow the government to 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 make 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, Ministry of Internal Affairs and Communications, Ministry of Education, Culture, Sports, Science and Technology, Ministry of Economy, Trade and Industry, and Ministry of Defense)

In relation to the mid- and long-term objectives that are directly linked with the strengthening of IT as an infrastructure, the competent agencies will commence discussions on the measures for intensive investment of public research funds within FY2007.

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[11] by

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

detecting and controlling abnormal traffic that would never occur in normal networking, the competent agency will continue promoting research and development activities of the Next Generation Backbone in FY 2007.

c) Research and development on detection of, recovery from and prevention of route hijacks[12] (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 prevention of route hijacks by FY 2009, the competent agency will continue promoting research and development activities on the detection of, recovery from and prevention of route hijacks in FY2007.

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

Based on the five-year plan commenced in FY2006, in order to further improve information security, the competent agency will undertake the research and development on comprehensive technologies that ensure the security of information, including technologies to ensure 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 the information with regard to disaster prevention and disaster alleviation without being disconnected even in case of a large-scale disaster.

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

The competent agency will promote research and development activities continuously from FY2006 on the next generation access control technology, authentication technology and software technology that are not bound to conventional technologies founded on the existing information systems as basis technology that is essential to realize high reliability society.

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 promote research and development on information security technologies continuously from FY 2006 with the purpose of enabling the owner/controller of information to determine whether it discloses or not and the scope of disclosure by

[12] 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.

himself/herself, and ensuring the disclosure precisely in accordance with the decision.

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

Based on the premise that incidents happen, the competent agency will conduct research and development activities continuously form 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 information leakage, rather than simply protecting information or system.

h) Research on the risk quantification method concerning information security (Ministry of Economy, Trade and Industry) [Reprise]

In order to improve the organization- and human-oriented management methods, research and development activities will continue to be conducted in FY2007, including quantification concerning information security in organizations, and measurment of cost efficiency with regard to information security measures. Discussions will also be held on unique risks of offshore outsourcing.

i) Research and development of technologies for measures against information leakage (Ministry of Internal Affairs and Communications)

Aiming to develop technologies to minimize the damage resulting from information leakage caused by the use of file sharing software, etc., which is difficult to prevent with the self-effort of the individual users, by the end of FY2009, research and development activities will be launched in FY2007 concerning detection of information leakage, automated suspending of leaked information from circulating via networks and enabling advanced and simplified method of managing chain of custody of information, etc.

j) Research and development for advancement of safety verification of telecommunications components (Ministry of Internal Affairs and Communications)

Discussions will commence in FY2007 on required technologies for improving the accuracy of security verification of telecommunications components, such as functions and equipments, etc. which compose the information network.

k) Research and development of dynamic network technology (Ministry of Internal Affairs and Communications)

Basic designs and prototyping will be conducted on elementary technology for dynamic network technology in FY2007, in view of building the fundamental technologies necessary

to create an environment in the next generation network which consists of various networks and terminals by FY2010. In the next generation network, an optimal communications environment is always provided through automated recovery function from network malfunctions and any person has an access without any limitation to the information accumulated on the network.

l) Promotion of ensuring security functions of communications terminals responding to the advancement of IP communications (Ministry of Internal Affairs and Communications)

Along with the advancement of IP communications it is expected that information security functions will be made available by coordinating communications terminals and networks, and thus directions will be determined in FY2007 for the modality of basic functions of communications terminals essential for the use of IP network and the promotion measures necessary for ensuring required functions.

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, Ministry of Internal Affairs and Communications, Ministry of Education, Culture, Sports, Science and Technology, Ministry of Economy, Trade and Industry and Ministry of Defense)

With regard to R&D and technology development with short-term goals, such as improvement of existing technologies and development of operational technologies, etc., analysis will commence to understand the progress of efforts made by the public and private sectors, and to improve coordination of the investment portfolio to avoid under-investment or excess investment in various areas in FY2007.

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 Virtual Machine (VM) will be promoted in FY 2007, 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) [Reprise]

After discussions on establishing evaluation criteria for the quality of the OS security that supports the information systems of E-Government, and the efforts made to establish all the necessary evaluation items and criteria usable for system procurement in FY2006, a technological survey will be conducted in FY 2007 on the system installation of the OS, etc. towards full-fledged launch of E-Government.

d) Promotion of technical development, etc. toward the establishment of Digital Forensics[13] (National Police Agency)

Technical cooperation with private companies, etc will be promoted toward the establishment of Digital Forensics and development of technology regarding analysis of information technology will also be promoted in FY2007.

e) Development and evaluation of information system with high level of assurance (Ministry of Defense and Ministry of Economy, Trade and Industry)

The Ministry of Defense will promote research on information systems and evaluation methodology satisfying the Evaluation Assurance Level 6 (EAL6) based on ISO/IEC15408(evaluation criteria for IT security), continuously from FY2006. In FY2007, evaluation tests will continue using the samples produced thus far. Joint research with IPA will also be conducted on the items related to the application of security evaluation technologies acquired by the Ministry of Defense to the new international evaluation criteria.

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 critical communications in times of disaster, etc., under an all-IP networking environment, a survey of domestic and overseas operation methods will be conducted in FY2007, with an aim to establish operation technologies for critical communications correspondent to IP networks, etc., by 2008.

g) Survey on the latest trends in information security-related products/services (Cabinet Secretariat, Ministry of Economy, Trade and Industry)

Discussions will be conducted in FY2007 on the methods of examining products and services with excellent information security technology, etc., as well as on methods of

[13] 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.

disseminating the results of the survey and related information to government agencies, local governments and business entities that own and operate critical infrastructures.

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

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

Leaving the area in which technology development is being undertaken in the private sector to the initiatives of the private sector, analysis will be launched within FY2007 on 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.

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

In FY 2007, the competent agency will promote 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)

Specific discussions will start on themes suitable for the Grand Challenge under cooperation between the Council for Science and Technology Policy (CSTP) and ISPC.

Section 2: Developing/Ensuring 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 2007.

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

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

[Specific Measures]

A) Progressive education program for IT specialist training (Ministry of Education, Culture, Sports, Science and Technology)

The competent agency will support establishing centers to develop and facilitate advanced IT human resource development programs in cooperation between industry and academia in FY 2007 to create an environment where people can use IT safely and comfortably.

B) Enhancement of functions of self-check tools for IT users in organizations (Ministry of Economics, Trade and Industry) [Reprise]

Indices to objectively measure the level of information security measures for IT users in organizations will be considered and functions of self-check tools utilizing the indices will be enhanced within FY2007.

C) Establishment of a mechanism of objective evaluation of advanced IT human resources (Ministry of Economy, Trade and Industry) [Reprise]

Aiming to establish a mechanism to objectively evaluate human resources, a framework of common careers/skills will be developed in FY2007 to systematically identify the skills required for advanced IT human resources, including those engaged in information security.

D) setting up the council for industry-academia-government collaboration (Ministry of Economy, Trade and Industry) [Re-listing]

In FY2007, the competent agency will set up the Council for Industry-Academia-Government Collaboration to conduct deliberations on the type of advanced IT human resources needed in the industry and the methods of developing advanced IT human resources in the practical field in industry and education.

E) Support for faculty development (Ministry of Education, Culture, Sports, Science and Technology and Ministry of Economy, Trade and Industry) [Reprise]

In order to promote practical education in each information sector, including information security, support will be provided to the efforts for faculty development (FD) of universities, etc. to improve ability of teachers.

F) Reform of examination system for information processing engineers (Ministry of Economy, Trade and Industry) [Reprise]

In order to enhance the development of advanced IT human resources, including human resources engaged in information security, the examination system for information processing engineers that measures skills in information sectors including information security will be drastically reviewed and a new examination system is scheduled to be launched in FY2008, upon ensuring consistency with the framework of common careers/skills.

G) Support system for training projects for human resources engaged in telecommunications (Ministry of Internal Affairs and Communications) [Reprise]

Support will also be provided for training activities to develop human resources engaged in telecommunications, including security personnel who have professional knowledge and expertise in the area of information and telecommunications, continuously in FY2007.

H) Establishing a human resources development system for advanced telecommunications (Ministry of Internal Affairs and Communications) [Reprise]

In order to develop the human resources playing an important role in information strategies of corporations and in creating new businesses, practical Project Based Learning (PBL) materials in ICT management sector, including telecommunications security, will be developed in FY2007.

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.

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 2007.

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

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 development of an environment on an international scale through cultivation of culture and the improvement of literacy at an international level.

[Specific Measures]

A) Deliberations on international cooperation/contribution (Cabinet Secretariat and all government agencies)

In order to clarify specific items to be addressed internationally, to identify partners for cooperation in realizing an "information security advanced nation" and to develop a Japanese Model to actively send messages within and outside the county, discussions will be held on basic policies and specific measures in FY2007 to strategically address international cooperation/contribution with the concerted efforts of the whole government.

B) 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 facilitate cooperation within multinational frameworks, such as G8 OECD and APEC, in FY 2007, 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.

Furthermore, policy dialogues with related government agencies in other countries will be strengthened thorough discussions on information security at the cross-sectoral bilateral policy dialogue.

C) 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 as the function of POC in Japan, which will be made internationally recognized in FY 2007, to serve as an interface to facilitate effective and smooth cooperation with other countries.

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

In FY 2007, 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.

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", the competent agency will contribute to the development of an environment in which awareness can be shared both nationally and internationally in FY2007, in line with the progress of the revision work of the relevant guidelines by OECD.

F) Efforts for improving international awareness/literacy (Cabinet Secretariat, Ministry of Internal Affairs and Telecommunications, and Ministry of Economy, Trade and Industry)

Deliberations will be conducted on the measures to improve international awareness/literacy for information security in FY2007 and discussions will be deepened with other countries on occasions, such as policy dialogues, on an as needed basis.

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 publicizing and dissemination of Best Practices (Cabinet Secretariat and all government agencies)

In order to make contributions as the world's most IT-advanced nation, in FY 2007, 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 that each country encounter, 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 CSIRTs in the Asia Pacific region will be supported. In specific terms, in FY 2007, in cooperation with APCERT (a forum of CSIRT in the region) accumulated incident response technologies and experiences of JPCERT/CC will be shared relevant organizations in the region, and through the promotion of incident response exercises which will be implemented with cooperation between overseas CSIRTs and relevant domestic organizations in the Asia-Pacific region, etc., enhancement of the capability of these organizations will be attempted.

C) Promotion of sharing of information of Internet observation from fixed-point in the Asia-Pacific region, etc. (Ministry of Economy, Trade and Industry)

JPCERT/CC will start deliberations in FY2007 on the establishment of an information sharing system of Internet Traffic Monitoring in the Asia-Pacific region, etc.

D) Strengthening capability to analyze attack methods and promotion of information sharing on analysis results (Ministry of Economy, Trade and Industry)

In order to formulate effective protective measures against attacks, examinations will be conducted on the framework to analyze technologies and methods used by perpetrators, as well as the trends, etc., and to share the analysis results among security-related organizations throughout the world.

Specifically, in FY2007, IPA and JPCERT/CC will consider the improvement of the capability to analyze attack methods and best practices, etc. to globally and safely share the analysis results.

E) 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 proposed the Information Security Management Guidelines for Telecommunications (ISM-TG) described in Chapter 3, Section 3, 1) to the International Telecommunications Union in FY2006. Efforts will also be made to have it adopted as an international standard in FY2007, thus contributing to enhancing the international level of information security management.

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

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 FY2007.

1) Development of infrastructure to control cyber crimes and to protect and redeem rights and benefits

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

[Specific Measures]

A) Strengthening of countermeasures against cyber crime

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

In order to appropriately respond to diversifying and more complicated cyber crimes, the competent agency will actively carry out inter-/intra-department training in FY 2007 for police officers who are engaged in cyber crime investigations throughout the country.

b) Strengthening and improvement of the system for taking countermeasures against cyber crime (National Police Agency)

In FY2007, the competent agency will strengthen and improve the investigation system to take countermeasures against increasingly diversified and complicated cyber crimes that are perpetrated across prefectural borders irrespective of geographic constraints.

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

In order to respond to increasingly diversified and complicated modus operandi, such as unauthorized computer access, and toward enforcement of a new legal framework following the conclusion of Convention on Cybercrime, the competent agency will improve and strengthen equipments and applications in FY2007 for analyzing access records, for conducting on-site investigations and operation tests on computer viruses, and for recovery of electromagnetic records, etc.

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

In light of the advancement of information processing in recent years, and in order to appropriately respond to cyber crimes, the competent agency will promote a legal framework for the conclusion of cyber crime 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, currently under deliberation)

e) Strengthening public-private collaboration against cyber terrorism on critical infrastructures (National Police Agency)

Enlightenment activities for business entities of critical infrastructures will be conducted to increase awareness about measures against cyber terrorism on an as needed basis in FY2007, in accordance with the characteristics of the operation of business entities engaged in critical infrastructures.

f) Promotion of international cooperation for cyber crime control (National Police Agency)

In FY 2007, information will be effectively exchanged with law enforcement organizations of the countries with impact on Japan's cyber crime situation. Also, participation in international frameworks related to cyber crime measures, such as the G8 High-Tech Crime Subgroup meeting and ICPO, will be promoted, and establishment of a multilateral cooperative relationship will be promoted by holding the cyber crime conference on the investigative technology in the Asia-Oceania region, etc.

g) Promoting promptness of international investigative assistance using a Central Authority System[14] (Ministry of Justice)

The competent agency will expedite mutual provision of assistance by designating investigative/judicial authority as a central authority through direct communication between

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

the central authorities without going through diplomatic channels. Agreement on mutual investigation assistance has already entered into force between Japan and the US and between Japan and ROK. The competent agency will work on the conclusion of similar bilateral agreements in FY 2007, with Hong Kong, China and Russia. The competent agency will also consider designation of a "central authority" under the cyber crime convention, upon consultation with relevant agencies.

h) Enhancement of the measures against interference of critical radio communications services (Ministry of Internal Affairs and Communications)

There have been incidents that threaten people's lives and properties caused by the degradation or suspension of system functions, due to interference and intervention against critical radio communications infrastructures, such as aviation radio or emergency radio. There is also concern about system malfunctions due to intended manipulation of critical radio communications infrastructures, and therefore, enhancement of measures that immediately eliminate such incidents is becoming more important.

Thus, the competent agency will improve and enhance radio wave monitoring providing an appropriate response to declarations/consultations of interference and intervention against critical radio communications, and facilitate rapid elimination of interference and intervention, based on the "Three-Year Plan for Strengthening Radio Monitoring" continuously from FY2006. In addition, the competent agency will enhance radio wave monitoring by developing a system to conduct a thorough investigation to clarify the cause of interferences or other interventions from April 2007.

i) Promotion of concentration and systematization of knowledge on Digital Forensics (National Police Agency)

In FY2007, the competent agency will promote concentration and systematization of knowledge on analysis of information technology to establish a criminal case, and at the same time, efforts for the establishment of Digital Forensics will be promoted, including the promotion of enhancement of collaboration with related domestic organizations through holding of digital forensics conferences, etc.

B) Development of infrastructure for protection and redemption of rights and benefit in cyberspace

a) Studies on infrastructure for protection and redemption of rights and benefit in cyberspace (Cabinet Secretariat)

In order to facilitate the development of infrastructure for protection and redemption of rights and benefit in cyberspace, research and studies will be implemented in FY2007 on

the best means of response to infringement of rights and benefit in cyberspace and the necessity of measures including legal measures against information leakage/illicit acquisition of information and the necessity of an environment which allows easy authentication, taking overseas situations into account. The result of the research and studies will be announced and necessary approach will be made to related agencies based on the results.

b) Promotion of dissemination of Provider Liability Limitation Law to Limit Liability of Providers and related guidelines (Ministry of Internal Affairs and Communications)

In order to provide users with relief against infringement of rights and benefit in cyberspace, the competent ministry will promote the dissemination of the Law on Restrictions on the Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identity Information of the Sender Information (Provider Liability Limitation Law). Specifically, the relevant law will be disseminated to users through PR and enlightenment activities, etc., and support will be given to telecommunications-related industrial groups for the dissemination activities of related guidelines.

2) Development and dissemination of technologies to improve 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 under the approval of all the concerned parties in communications as well as other technology to improve safety and reliability in cyberspace contexts.

[Specific Measures]

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

In FY2007, the competent agency will promote joint research on the detection of symptoms of cyber attacks by analyzing the logs of firewalls, etc., in cooperation with universities.

Chapter 5: Policy Promotion System and Structure of Continuous Improvement

The government will comprehensively implement major policies described in the previous chapter in FY 2007 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 the person with appropriate skill 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 plays a core role in promoting the information security measures of the entire government, will continuously be ensured, and its high-level human resources will be actively utilized to mobilize the expert knowledge of the public and private sectors.

Under this system, the competent agency will implement the measures described in Chapter 3, Section 1, as policy related measures, in order to make a full-fledged launch of the Standards of Measures and PDCA cycle based thereon and to strengthen the emergency response capability of the entire government. Besides response to the Standards of Measures and response to emergency, efforts will be made to respond to various needs to implement the information security measures of government agencies, such as measures to enhance information security in E-Government, etc. As measures for critical infrastructures, the measures listed in the Chapter 3, Section 2 will be implemented in accordance with the action plans concerning information security measures.

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. The competent agency will also expand the functions to conduct examination/consideration for various trends of basic information necessary to promote information security measures.

B) Improvement of information security consulting functions to promote information security measures of government agencies (Cabinet Secretariat)

In order to support the promotion of the information security measures of government agencies, the National Information Security Center (NISC) will improve information security consulting functions by the experts of the Center, with the purpose of responding to various needs including the response related to Standards for Measures, emergency response, and response for enhancing information security of E-Government.

C) Discussions on the best forms of response measures of the government against potentially grave risks, etc. (Cabinet Secretariat)

In order to respond specifically to potentially grave risks (for example, troubles that may occur in the future, such as Y2K issues) and issues that are hard to resolve under the current government systems (such as those without clear jurisdiction), the Cabinet Secretariat will consider the possible measures of the government, aiming to reach a conclusion by the end of FY2007.

(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)

In FY2007, the competent agencies will continue to strengthen the framework for their own information security measures, and also continue implementing, 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.

B) Deliberations toward the establishment of information security analysis department (tentative name) (Ministry of Economy, Trade and Industry)

In order to widely collect and analyze relevant data and results of both domestic and foreign research activities of information security, the competent agency will conduct deliberations on the establishment of an information security analysis department within related domestic organizations in FY2007.

Section 2: Partnerships with Other Related Organizations

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 each organization, and to promote information security measures for the entire government in an integrated form, by increasing cooperation in proposing and implementing various measures in FY2007.

Particularly in terms of 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 continuously in FY2007 and onwards. 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 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, etc.[15] (Cabinet Secretariat)

The Cabinet Office will announce the progress of the implementation of specific measures listed in Secure Japan 2007 twice a year and the evaluation, etc. will be conducted at the end of the fiscal year.

B) Discussions on a milestone toward strengthening information security measures of

[15] In this measure, "Evaluations, supplementary study and analysis, etc. in line with evaluation criteria" are expressed as "evaluations, etc.", consistent with the definition in the "Operational Policies for Evaluations based on Evaluation Criteria" of the "Evaluations, etc.", toward Realization of Secure Japan and Promotion of Reasonable and Continuous Improvements" (decision made on February 2, 2007 by the Information Security Policy Council).

government agencies (Cabinet Secretariat)

In the first quarter of FY2007, a schedule for routine evaluation, evaluation criteria and the concept of evaluation criteria concerning the measures to improve the government's information security will be formulated as a milestone in FY2008 for the realization of the National Strategy.

C) Review of "Action Plan on Information Security Measures for Critical Infrastructures" (Cabinet Secretariat) [Reprise]

In FY2007, studies/findings will be conducted on the progress of the improvement of information security in critical infrastructures, in preparation for the review of "Action Plan on Information Security Measures for Critical Infrastructures". In so doing, discussions will also be made on ensuring and coordination of consistency with other related cross-ministerial approaches, such as responses to disasters, etc. Also, discussions on the modality of the public-private partnership will continue.

(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 2007.

(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)

Based on the evaluation criteria developed in FY2006, with a view to visualize the path to realization of the National Strategy (Realization of Secure Japan), the competent agencies will promote the use of criteria for evaluating the degree of dissemination of information security measures for each implementing body (government agencies, local governments, critical infrastructure, corporations and individuals) in the government and international organizations and will consider the revision of the relevant evaluation criteria in response to the evaluation results, etc. Also, with respect to evaluations, etc.[16], the whole process of the evaluations, etc. will be smoothly promoted, while the Cabinet Secretariat enhances the functions of survey responsibilities, since supplementary surveys will be implemented when appropriate.

In the meantime, in order to contribute to the establishment of the above-mentioned evaluation criteria, the Ministry of Internal Affairs and Communications conducted deliberations in FY2006 concerning evaluation criteria for the response of telecommunications carriers against cyber attacks, as part of cyber attack response exercises in the telecommunications sector, which is listed in SJ2006, Chapter 2, Section 2-(4). In FY2007, the use of the relevant evaluation criteria by telecommunications carriers will be promoted and discussions will be held on the improvement of the relevant evaluation criteria in response to evaluation results, etc.

[16] In this measure, "Evaluations, supplementary study and analysis, etc. in line with evaluation criteria" are expressed as "evaluations, etc.", consistent with the definition in the "Operational Policies for Evaluations based on Evaluation Criteria" of the "Evaluations, etc.", toward Realization of Secure Japan and Promotion of Reasonable and Continuous Improvements" (decision made on February 2, 2007 by the Information Security Policy Council).

Chapter 6: Direction of Priority Measures for FY 2008

~ Priorities in FY 2008 "Intensive Efforts for Enhancing Information Security Infrastructure: Focusing on Developing and Ensuring Human Resources Engaged in Information Security, Adoption of Information Secruity Measures on an International Scale, and Enhancement of Information Security of E-Government" ~

Specific measures to be implemented in FY2007, the second year of the three-year plan, are listed in Chapter 3 through Chapter 5. These are the continuation of the efforts of FY2006, focusing on **"raising the level of information security measures in the public and private sectors".** With the actions taken over these two years, each implementation body is expected to reach a certain level of improvement toward achieving the objectives of the National Strategy for information security measures.

However, as mentioned in Chapter 2, Section 3, information security measures cover many areas in which it takes time for efforts to show results (1). There are some areas in which measures are still at the incipient stage, although implemented (2) and some areas in which timely and rapid response is required as an urgent priority (3).

From these viewpoints, as presented in Chapter 1 and Chapter2, establishment /enhancement of information security infrastructure, specifically developing/ensuring human resources engaged in information security, is an issue of urgency in many aspects, and needs to be pursued intensively beyond the single year of 2007. Furthermore, international efforts with regard to information security measures, represented by the promotion of international partnership/cooperation, as mentioned in Chapter 1, are still at the first step and further acceleration is necessary from FY2007 onward. In addition, efforts for information security enhancement for E-Government infrastructure should be implemented appropriately at the required time, while giving due consideration to the schedule of developing various systems that compose E-Government.

With these factors as background, in FY2008, the last year of the National Strategy, measures in line with the direction of past efforts will continue to be intensively implemented, focusing on the **"intensive efforts for enhancing information security infrastructure"**; particularly in accordance with the directions described below.

Section 1: Intensive Efforts for Developing/Ensuring Human Resources Engaged in Information Security

Developing/ensuring human resources engaged in information security in Japan will require steady implementation in line with various recommendations listed in the report of the Specialist

Committee on Human Resources Development/Systematization of Qualifications. It cannot be said that these issues will be fully solved in one short year of FY2007. Thus, efforts will be continuously and intensively made in the relevant areas in FY2008, the last year of the National Strategy.

[Specific Measures]

A) Improvement of a cross sectoral support and comprehensive system for human resource development (Cabinet Secretariat, Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

In order to effectively promote improvement of the quality and expansion of the quantity of human resources including information security field throughout Japan, the competent agencies will develop a cross sectoral human resource development support system that is managed by the organization running various educational programs including qualification systems and thus promote supporting comprehensive human resources developing/ensuring.

B) Progressive education program for IT specialist training (Ministry of Education, Culture, Sports, Science and Technology)

The competent agency will support development of the center to develop/implement programs aiming for developing advanced security specialists, and will promote dissemination/launch of the achievements of educational materials, etc., which are obtained through the development/implementation of the programs, to other universities, etc.

C) Focusing on ensuring human resources engaged in information security in government agencies (all government agencies)

In light of the chronic shortage of human resources engaged in information security in government agencies, all government agencies will exert efforts to ensure personnel serving as a core of information security in each agency.

D) Improvement of educational programs for government employees (Cabinet Secretariat and Ministry of Internal Affairs and Communications)

In response to the result of discussions made in FY2007, efforts will be made to improve the quality of the government's integrated educational programs for government employees (general employees, officers and officials responsible for information security measures) and expand the number of lectures and seminars, etc.

E) Further promotion of awareness/ability of network users concerning information security (Ministry of Internal Affairs and Communications)

The competent agency will promote efforts for further improvement of awareness of network beginners with little experience in information security and will make efforts to enhance the response capability of users to security risks from using websites, etc., so that they can appropriately and independently respond to the security threats they face.

F) Formulation and distribution of educational materials to teach easy and practical information security measures (Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

In order to develop literacy and an environment where teachers, students and pupils of primary, junior high and high schools can use the Internet safely, the competent agencies will promote the use of educational materials in lessons provided at individual schools, reflecting the latest trends in information security.

G) Promotion of information security measures in small- and medium-sized enterprises (Ministry of Economy, Trade and Industry)

With the aim of reducing the burden and promoting the information security measures of small- and medium-sized enterprises, and in order to streamline the tasks of personnel responsible for information security measures for small- and medium-sized enterprises, the competent agency will promote the formulation of a package of information security measures for small- and medium-sized enterprises and a standard format to confirm the progress of implementation of measures.

H) Dissemination of assurance-based information security audit (Ministry of Economy, Trade and Industry)

In order to disseminate an assurance-based information security audit in which an auditor provides some assurance, guidelines for assurance-based audits, etc. will be formulated and discussions will be held on the method of dissemination.

I) Strengthening of systems, etc. concerning the measures against cyber terrorism (National Police Agency)

In order to respond to advanced methods and increased thereats of cyber terrorism, on the occasion, for example, of hosting the 2008 Summit, the competent agency will promote strengthening of countermeasures against cyber terrorism taken by the police, such as providing training within and outside the department to improve response capabilities and technical ability of personnel coping with cyber terrorism, and conduct enlightenment activities for business entities of critical infrastructures, on an as needed basis, to increase awareness of measures against cyber terrorism, in accordance with the characteristics of

operations of each business.

J) Strengthening/improvement of a system to control cyber crime and improvement of the level of skills (National Police Agency)

In order to promote countermeasures against increasingly diversified and complicated cyber crimes, using Digital Forensics, the competent agency will make efforts to strengthen/improve its investigative capabilities and also will promote training within and outside of the department for police officers being engaged in investigating cyber crime throughout Japan, concerning Digital Forensics, etc.

Section 2: Intensive Efforts for International Collaboration in Information Security

Regarding the efforts for international collaboration in information security measures, represented by international partnership/cooperation, the government will consider basic concepts as well as specific measures for strategic commitment to international cooperation/contribution in FY2007. In FY2008, full-scale action will be taken based on these measures with it's speed accelerated.

[Specific Measures]

A) Enhancement of counter service functions at the National Information Security Center (Cabinet Secretariat)

Since IT infrastructure stays connected to the world for 24hours a day/365 days a year, the Cabinet Secretariat will establish a system to rapidly/appropriately respond to information and communication concerning the information security issues of government agencies throughout the world within FY2008.

B) Promotion of international strategy to be formulated in FY2007 (Cabinet Secretariat)

The Cabinet Secretariat will strategically promote activities with regard to international relationship concerning information security in FY2008, in line with the basic concepts and specific measures to be formulated in FY2007, in order to actively distribute information to the world, including Japan, and to make a strategic commitment to international cooperation/contribution as a whole government.

C) Hosting international conferences on information security measures (Cabinet Secretariat and concerning agencies)

The competent agencies will work toward hosting international conferences that provide

opportunities for policy officers and experts in information security from public and private sector to share their knowledge and experience in FY2008.

D) Improvement and international implementation of organizational management measures/related guidelines (Ministry of Economy, Trade and Industry)

The competent agency will make efforts to improve organizational management measures/related guidelines, such as measures for information system management in the context of information security, and to distribute information to the world as well as domestically.

In order to contribute to improving information security measures of corporations in Asia-Pacific countries, the contents of information security benchmarks will be introduced to those countries.

E) Enhancement of international response systems for CSIRTs and related organizations and advancement of information coordination (Ministry of Economy, Trade and Industry)

In order to promptly share information among concerned parties, and to ensure a smooth response to the ever evolving information security issues, such as computer viruses, illegal access, vulnerability, etc., "computer security early-warning systems" by IPA and JPCERT/CC, etc. will be enhanced within 2008. Specifically discussions will be conducted on various issues such as enhancement of information gathering concerning information security issues, framework for effectively/efficiently distributing collected information, and strengthening efforts for international coordination, etc.

Particularly, the structure of CSIRTs in the Asia-Pacific region, etc., will be strengthened. Furthermore, the scope of coordination will be expanded and its level will be advanced, by building a system that enable sharing the data of Internet Traffic Monitoring with CSIRTs and visualization of the data, and sharing information on analysis of malware, etc.

F) Establishment of information security analysis departments (tentative) (Ministry Economy, Trade and Industry)

In cooperation with organizations in other countries, the competent agency plans to establish information security analysis departments (tentative) in related domestic organizations, in order to collect and analyze relevant data and the results of domestic and international research activities on a wide scale.

G) Improvement of information collection and analysis functions concerning information security (Ministry Internal Affairs and Communications)

In view of cooperation with both domestic and international related organizations, the

competent agency will promote collection/management of information pertaining to information security, research activities on analysis/measures at the Information Security Research Center of NICT. Information analysis and sharing with concerned organizations at Telecom ISAC Japan (Information Sharing and Analysis Center) will also be promoted.

H) Promotion of international coordination/cooperation through the Conference of the G8 Ministers of Justice and Interior (National Police Agency)

The competent agency will make efforts to accelerate the speed of the implementation of measures against cyber crime by, for example, deepening common awareness about the situations surrounding cyber crimes with concerned countries, on the occasion of the Conference of the G8 Ministers of Justice and Interior to be held in Japan in 2008.

I) Strengthening of international coordination/cooperation concerning Digital Forensics in the Asia-Oceania region (National Police Agency)

In order to strengthen international coordination/cooperation on Digital Forensics in the Asia-Oceania region, the competent agency will strengthen the information sharing functions for Digital Forensics through, for example, expansion of the participants of the cyber crime conference on the investigative technology in the Asia-Oceania region.

Section 3: Comprehensive Approaches to the Enhancement of Information Security of E-Government

Currently, various measures for E-Government are underway by competent agencies, in line with the "Priority Policy Program 2006" (decision made on July 26, 2006 by IT Strategy Headquarters) and the "E-Government Promotion Plan" (decision made on August 31, 2006 by CIO Liaison Committee). Inter-agency operations are to be carried out in an integrated manner through centralized systems, and discussions are to be conducted on integration and sharing of the common systems of the government agencies in an attempt to ensure overall optimization. In FY2008, verifications will be performed from the point of view of information security on these issues, and comprehensive efforts will be made to strengthen information security in E-Government.

Furthermore, it is necessary for e-local governments to implement measures to enhance information security, in accordance with the efforts of the government agencies.

[Specific Measures]

A) Enhancement of measures to ensure information security of E-Government from the stages of planning and designing (Security by design) (Cabinet Secretariat, Ministry of Internal Affairs and Communications, and relevant government agencies)

It is essential to appropriately integrate the information security requirements into the various operations and systems of E-Government that are under construction. The competent agencies will enhance measures to plan and design the systems that incorporate information security as a basic concept.

B) Promotion of verification of information risks associated with E-Government and promoting standardization of its methods (Cabinet Secretariat and relevant agencies)

In order to strengthen the information security of E-Government, the competent agencies will consider method of verification and installation of information security measures to be installed in government agencies in accordance with the actual environment of each agencies and promote standardization of its operation through the verification of information security risks by examining vulnerabilities using simulated attacks and by analyzing IT malfunctions occurred in and outside the government agencies.

C) Consideration on cryptography policy toward maintenance/improvement of information security (Cabinet Secretariat, Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

In order to ensure safety and reliability of information systems, the competent agencies will consider modality of safe encryption measures that will be carried out and the systematic promotion of those based on the results of discussions made by government agencies in FY2007.

D) Steady operation of GSOC and strengthening it's analyzing function

The Cabinet Secretariat will work toward the steady operation of GSOC, which is under development in FY2007. Furthermore, the Secretariat will analyze the general tendencies and situation of cyber attacks on government agencies, based on the operations of GSOC. The Secretariat will also regularly provide the analysis results to each government agency, and make efforts to enhance the system to provide the information necessary for implementing individual measures at the appropriate timing, such as analysis results of attack methods. The Secretariat will also establish a cross-sectoral analysis function on attacks (Analytical Scheme for Public-Private Cooperation (tentative)), in cooperation with domestic and international related organizations.

E) Discussion of the method of promotion of the use of encryption in local governments (Ministry of Internal Affairs and Communications)

Along with the efforts made by government agencies, the competent agency will

consider effective means to promote the use of information security measures, such as use of encryption, which have not been fully implemented by local governments. In order to improve information security in local areas, discussions will be conducted on public-private cooperation and the ways of dissemination/enlightenment to the general public at the local level.