Secure Japan 2008

ーIntensive Efforts for Enhancing Information Security Infrastructureー

Information Security Policy Council
June 19, 2008

Contents

Chapter 1: Action and Evaluation Based on Secure Japan 2007

Section 1: Background of action based on Secure Japan 2007

As dependence on IT increases in daily and socio-economic activities in Japan, information security has become an important issue in ensuring the safety and security of IT use. Under these circumstances, Secure Japan 2006 (hereinafter referred to as "SJ2006") was formulated in FY2006, as part of the efforts for the initial year of the First National Strategy on Information Security (hereinafter referred to as the "National Strategy"), a three-year plan for FY2006-FY2008. As a consequence, the following progress was made in this initial stage:

1) Emerging awareness about information security in the respective implementing bodies

2) Commencement of specific efforts by each implementing body

3) Establishment of information security promotion systems and a sustainable improvement structure

Based on this progress, the main issues in the following stage that began at the start of FY2007 were maintaining systems to promote the established information security measures by both the public and private sectors and achieving a stable promotion system for those measures, including improving insufficient measures. The efforts for information security in FY2007 were made in line with this direction.

Section 2: Priority Goals and Pillars of Effort in FY2007

In June FY2007 (the second year of the National Strategy), we developed an annual plan entitled "Secure Japan 2007" (hereinafter referred to as "SJ2007"), setting priorities for the government's information security measures.

SJ2007 aims to improve information security measures in the public and private sectors, adopting the following priorities: 1) maintaining and improving common awareness, since such awareness is generally infused into each public and private sector body; 2) continuously pursuing state-of-the-art technology, while giving consideration to the discussions at the Information Security Technology Strategy Expert Committee; 3) strengthening the strategic response capacity of the public sector, while maintaining a balance with the protection of human rights and the ensuring of transparency and legality in the public sector; and 4) maintaining and strengthening partnership and cooperation among international organizations. In keeping with these priorities, each body made progress in its efforts to implement measures.

Specifically, in continuation from FY2006, the competent ministries and agencies, including the Cabinet Secretariat, were to undertake a total of 159 projects by implementing specific measures 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 system, cooperation with concerned organizations, and establishment of a structure of continuous improvement)."

SJ2007 also specified the direction of the priority measures for FY2008, titled "Intensive Efforts for Enhancing Information Security Infrastructure," and listed a total of 24 specific measures such as "intensive efforts to develop and secure human resources engaged in information security," "intensive efforts for international collaboration in information security" and "comprehensive efforts to enhance the information security of e-Government."

Section 3: Evaluation of FY2007

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 SJ2007. "Evaluation, etc., of Information Security Policies in FY2007" (hereinafter referred to as the "Evaluation 2007") was formulated and reported to the Information Security Policy Council. This publication aims to draw out the directions suggested by the Evaluation 2007, identify the current conditions that predicate the formulation of the annual plan for FY2008, and evaluate the efforts made in FY2007. 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 FY2008.

This publication, based on these recognitions of the current situation, describes basic policies for FY2008 in Chapter 2, and outlines specific efforts to be addressed in FY2008 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 FY2009.

1. Evaluation/Analysis

[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).

The results of 159 specific measures to have been implemented within FY2007 in line with SJ2007 were classified and evaluated as follows:

A:	144 measures (90.6%, including 5 A' measures)
B^+:	1 measure (0.6%)
B:	12 measures (7.5 %)
C:	1 measure (0.6%)
-:	1 measure (0.6%)

○ A : Measures implemented as initially planned

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.

The measures that SJ2007 determined should be put into effect within FY2007 were started by each competent authority, and about 90% have progressed as initially scheduled. Of the remaining 10% of the measures (15 measures), which failed to progress as planned, seven were measures that required support from all ministries and agencies but had not been completed by some, such as the development of an information asset registry and shift to using "go.jp" as a domain name, six were measures that could not be completed within FY2007 despite being implemented, such as the conclusion of the Mutual Legal Assistance Treaty, one was a measure that failed to be promoted for reasons beyond the control of the government, including the revision of the criminal law, and one was a measure that was determined to be unnecessary in view of the outcomes of other measures.

The 144 measures rated as A were implemented as planned due to the efforts of the responsible officers at each ministry and agency, while the five measures rated as A' are connected with implementation by government agencies: namely, the "establishment of a PDCA cycle at each government agency," "establishment of a PDCA cycle for the whole government," "evaluation, etc. of the progress in implementing measures," "evaluation, etc. of information security management" and "enhancement of information security measures and implementation of cross-ministerial approaches." This implies that the issue is still one of insufficient systems and personnel, despite the continuous and strenuous efforts of the government to implement measures.

Some measures rated as A still require continuous efforts. These measures, and particularly those measures rated lower than A, will entail continuous and progressive efforts in FY2008, the final year of the National Strategy.

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

(a) Policy Field

(i) Central government/local governments

Based on the results of intensive inspections of web servers, etc. in FY2007, although it cannot necessarily be concluded that the government's measures have reached a sufficient level, it can be said that the level has been raised considerably, thanks to certain achievements being accomplished in a short period of time. This seems to be attributable in large part to the continuous and all-out efforts of government ministries and agencies, led by the competent departments, including the securing of necessary budgets and implementation of measures. Education centers and education tools have been developed, signifying the improvement of systems/infrastructure that will contribute to the development of human resources engaged in information security.

However, some issues have surfaced when looking at the systems currently in place. For example, there are only a few officers assigned to be in charge of the whole organization. Also, officers are often unable to acquire a sufficient level of expertise, since they are transferred from one position to another on a two- to three-year cycle, even though the positions require expertise. Moreover, some organizations do not always have a top-down decision-making structure in place with regard to information security measures. The upgrading of the level of measures is approaching the limit of response capacity, and thus further efforts are needed to enhance the systems.

Efforts have also been moving forward to promote e-Government/e-Local Governments, and it remains essential to take the perspective of information security into consideration when promoting such efforts.

(ii) Critical infrastructures

FY2007 saw the completion of the development of the CEPTOAR in all 10 fields, as well as the compilation of review policies for the establishment of the CEPTOAR Council (provisional name). In continuation from FY2006, cross-sectoral exercises were conducted for the second consecutive year, in cooperation between the public and private sectors, in the form of "functional exercises" that are closer to the actual responses. These factors would suggest that a framework/system is gradually being formed to promote information sharing and communication/coordination between public and private entities, while ensuring business continuity as an axis. It can also be said that awareness of the importance of measures has gradually been raised through these efforts by the public and private sectors. It is necessary to continue to make further efforts in the future by identifying the merits thereof, so that such efforts can proceed while fully respecting the initiatives of business operators.

(iii) Businesses

Measures/systems are being steadily upgraded in the business sector. Awareness of the importance of measures is also improving. This seems to be significantly affected by the fact that information leaks and system failures might cause a loss of trust and economic loss through re-investment in measures. A further increase in awareness of the importance of IT control following the enforcement of the Financial Instruments and Exchange Act (the Japanese version of the SOX Act) in FY2007 can also be listed as a contributing factor.

On the other hand, since there has been no noticeable change in the installation of anti-virus software, it is inferred that investment in information security measures tends to be made through management decisions by each entity based on comparison with economic losses.

It is also pointed out that the effect of information security measures is hard to observe. Furthermore, excessive investment in security may occur, since the minimum measures that would need to be taken are not clearly identified, and "precaution fatigue" is sometimes mentioned. In addition, concerns are raised that there is a gap in awareness between pioneering companies and small-sized companies.

Taking these conditions into account, it could be assumed that an equilibrium point is being reached in the promotion of efforts under the existing framework of measures. It is also possible that the security that can be assured under the current level of technology has reached its limit.

In order to further promote the efforts, it would be effective to define the merits of continuous measures, to clarify the minimum level that needs to be attained, and to promote efforts from the perspective of business continuity.

(iv) Individuals

Since support from other bodies in the area of individuals is more important than in other implementation fields, various efforts have been promoted under SJ2007 with a focus on dissemination and PR activities/information transmission concerning information security. For example, periodic upgrades of OSs and the installation/utilization of anti-virus software have gradually improved in recent years, with a resultant improvement in awareness of information security as a whole.

On the other hand, the level of awareness of new risks, such as bots, is still low, and the prospects of continuous improvement in awareness are not particularly encouraging. There is a generation or gender gap in awareness of the need for measures and in the progress in implementing measures.

From now on, in the area of individuals, it is necessary to continue to further efforts for dissemination and PR activities/information transmission, while reviewing the effectiveness of measures based on emerging changes, such as threats, etc. Eliminating the age/gender gap, in particular, is an important issue.

(v) Promoting information security technology strategy

In the area of technological development and R&D, a Beta version of the Secure VM (Virtual Machine) has been released, and efforts are progressing smoothly. Progress is also being made in the construction of a framework for technology/R&D in the field of information security involving the whole government. However, a full-fledged implementation of strategic efforts under such a framework has yet to happen, and effective promotion is required.

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

In response to the report of the Specialist Committee on Human Resources Development/Systematization of Qualifications[2], a range of efforts have been

[2] "The Report of the Specialist Committee on Human Resources Development/Systematization of Qualifications," Specialist Committee on Human Resources Development/Systematization of Qualifications, Information Security Policy Council (January 23, 2007)

made by both the public and private sectors in the field of human resources . As a result, it is fair to say that there has been much progress in the development of systems/foundations for developing and securing human resources, and awareness about human resources development has started to spread. However, the day has yet to come where the systems and foundations are solidly established and human resources development can be implemented in a self-sustainable manner. It will take time before many people can genuinely exercise their capacity as human resources engaged in information security. It is therefore fair to say that securing human resources that can meet the needs of society as a whole is still at an early stage.

(vii) Promotion of international partnership and cooperation

Japan has been actively involved in discussion processes through participating in international conferences and holding international conference workshops. In FY2007, in addition to these efforts, we have formulated the basic policies for international contribution to be initiated by Japan in the area of information security[3] and have started full-scale efforts for international cooperation and coordination. However, at present, we have just presented various policy suggestions towards international cooperation and coordination. It is thus important to take continuous action towards achieving the content of these suggestions.

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

Certain efforts have been made to improve the investigative capacity against new forms of crime and illegal conduct occurring in cyberspace, to facilitate system development and reduce mid- and long-term risks. With respect to reducing risks through the development of safety and security technology, the technology itself is still being developed, and it is necessary to continue and accelerate these efforts.

(b) Social Conditions

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

In the area of human resources, it is reasonable to conclude that there was progress in the development of systems/foundations for human resources in FY2007, through the active efforts of both the public and private sectors, and

[3] "Efforts for International Cooperation/Contribution of Japan in the Area of Information Security," Information Security Policy Council (October 3, 2007)

awareness of human resources development has penetrated the whole of society. However, the day has yet to come when the systems are solidly established and human resources development can be implemented in a self-sustainable manner. We are still groping for a specific method for human resources development, and it is thus fair to say that efforts remain at an early stage.

In the area of awareness, FY2006 saw an emerging awareness of the necessity of information security measures. In FY2007, awareness of information security-related threats and of the necessity of measures improved due to factors such as the promotion of the various efforts based on SJ2007, mass media reports (crucial information leaks, failures of fundamental IT systems, etc.), and the increasing amount of unauthorized computer access and network-based crimes. It is thought that awareness about information security is gradually increasing, although causes vary.

In the area of systems, this was the year in which a framework for the promotion of specific measures proceeded in a step-by-step manner. However, the response system for the implementation of government agency measures is thought to be reaching the limit of its response capacity under the existing system, even though strenuous efforts continue to be made for the promotion of measures. Thus, further efforts to enhance systems are required. In critical infrastructures, a framework/system is gradually being formed to promote information sharing and communication/coordination among public and private entities, while ensuring business continuity as an axis. Private companies have promoted efforts for the enhancement of measures and systems, including organizational responses, as represented by the continuous increase in the number of business operators that have acquired Information System Management Systems (ISMS).

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

There has been no significant change in physical aspects, but it is fair to say that there has been consistent investment made in the factors necessary to implement measures in a solid fashion. Government agencies have steadily promoted system measures, such as starting development of the Government Security Operation Coordination team (hereinafter referred to as the “GSOC”) and allocating the same level of budget as last year for system construction associated with compliance with the “Standards for Information Security Measures for the Central Government Computer Systems.” Since private companies had not made significant changes till FY2006 in terms of installing anti-virus software and comprehensive security software, it is inferred that investment in information security measures tends to be made through management decisions by each business entity based on comparison with economic losses. In the field of individuals, the overall level has been raised, but there is still a generation/gender gap and it is desirable to improve the implementation status, starting with the acquisition of necessary protective software.

It can be said that a variety of efforts have been making steady progress in terms of R&D/technology development. Owing to the results of these efforts, it is expected that the technological limit to ensure security will be extended and that measures will make substantial progress.

(iii) Circumstances (incidents/events, market, etc.)

With respect to circumstances, information leakages arising from computer viruses or file-sharing software have continued to occur,, and the amount of unauthorized computer access and Internet-based crimes has been on the rise in recent years. As IT has become increasingly integrated as an infrastructure in people's lives and socio-economic activities, we have continuously seen incidents where system failures caused by internal factors resulted in serious consequences.

From the viewpoint of changing risks, in addition to the traditional defacing of web sites or DoS attacks[4] on web servers, the stealing of critical information by sending malware[5] attached to e-mails to specific organizations and companies and threatening of companies by sending warnings of attacks have occurred at government agencies and companies. The aims of such acts have changed from crimes for pleasure to economic interests. At an individual level, "bot"[6] infections, which are hard to detect and whose damage is hard to determine, have continued to occur, resulting in unspecified damages.

Under these circumstances, while each entity has been making efforts of its own, the methods/objectives of attacks are constantly changing and their damage is hard to detect, meaning that risks to information security have not necessarily been reduced.

3. Overall Evaluation

[4] Attack to suspend or reduce the function of services by sending a large amount of illicit data or packets to servers or network devices via the network (Internet)

[5] A general term for programs such as computer viruses, worms, Trojan horses, bots, etc., that infect computers to be used for illicit acts

[6] A type of computer virus: a program that aims to manipulate a computer infected with the virus from outside via the network (Internet)

In FY2007, the efforts listed in SJ2007 have generally proceeded as planned, and the maximum effort was made to (1) maintain a system to promote information security measures in both the public and private sectors, and (2) stabilize the promotion of measures.

With respect to the status of efforts to implement measures, various indexes clearly indicate that there has been some progress. There have also been advances made in “upgrading the level of information security measures in the public and private sectors,” which has been prioritized when stabilizing the promotion of measures. With respect to measures by government agencies, in particular, the strenuous efforts of the relevant offices of government agencies based on the PDCA cycle have produced positive effects, and it is fair to say that certain improvements in conditions have been attained in a short period of time, even if things are still at a level requiring enhancement.

The following has been achieved in relation to the “four basic policies” listed in the National Strategy and set forth in SJ2007.

1) The common awareness of public and private entities associated with information security has been strengthened. For example, there has been improvement in the awareness of implementation bodies, such as government agencies, critical infrastructure operators, etc., and in awareness associated with human resources, which are the foundation of cross-sectoral information security.

2) In terms of technology, there has been progress in developing an environment where prioritized investment can be made in the field of information security by the government as a whole and in developing issue-solving types of technology, and state-of-the-art technology is being continuously pursued. In the future, it will be necessary to increase the level of the technological limit through such efforts.

3) With respect to enhancing the response capacity in the public sector, it is significant that a system is being built to prevent cyber attacks on government agencies and the occurrence of IT system failures in agencies, and to provide prompt and accurate responses to such incidents.

4) In terms of promoting cooperation and coordination, full-fledged international actions have been launched in response to the development of the national strategy for international coordination and contribution. At the same time, regarding cooperation/coordination among domestic public and private entities, even though the NISC is serving as a contact point, there has not yet been cross-sectoral communication among entities, and this is one of the issues for the

future.

Based on the above factors, the achievements attained through the efforts made in FY2007 can be summarized in the following four points: 1) maintenance/improvement of awareness of information security at each entity, 2) steady promotion of specific efforts in each field of implementation, 3) steady promotion of specific efforts covering the cross-sectoral field of information security infrastructure, and 4) maintenance and enhancement of information security promotion systems and promotion of policy management based on a sustainable improvement structure.

However, there exist some points where efforts are approaching their limit under the existing promotion systems or existing framework of measures, as can be seen in government agencies and private corporations. There are also some points where the existing technological level is reaching its limit, as can be seen in the area of technology.

As mentioned in the Evaluation of Information Security Policies of FY2006, there are policies to be taken continuously on a mid- and long-term basis, such as developing and ensuring human resources, policies that require accelerated efforts because full-fledged efforts are still an early stage, such as international cooperation/coordination, and policies to be taken promptly and intensively in a timely manner as urgent issues, such as enhancing the information security of e-Government.

Furthermore, since no drastic risk reduction has been achieved amidst the current situation, where existing information security issues are still present and new information security issues are emerging, the impact (outcome) of information security policies on society cannot be sufficiently assessed. Thus, it seems necessary to proceed with efforts to produce effects on society.

Active and intensive efforts are expected in the final year of the plan (FY2008), so that Japan can truly become a country with advanced information security through the efforts of these three years, based on the National Strategy.

Chapter 2: Basic Policy for Addressing Information Security in FY2008

Section 1: Issues in FY2008

Secure Japan 2008 (hereinafter referred to as “SJ2008”) sets out priority measures for the information security of the government of Japan in FY2008, the last fiscal year of the efforts under the National Strategy, based on the efforts and their evaluation results of FY2007.

Three major issues need to be addressed in FY2008, the final year of the three-year National Strategy. First, studies need to be conducted on a method that will bring about a breakthrough in the limitations of existing promotion systems, framework of measures and technological level. Second, some measures need to be put firmly in place: for instance, the development and ensuring of human resources, which requires mid- and long-term efforts; international cooperation/coordination, which requires an acceleration of efforts; and enhancing the information security of e-Government, which requires prompt and intensive efforts. Third, it is necessary to promote efforts so that information security policies can generate a social impact (outcome).

In terms of the first issue, it seems necessary to implement measures as planned for FY2008 while getting a more accurate grasp of the current situation, and at the same time to discuss drastic measures from a long-term standpoint. Currently, members of the review panel are holding various discussions for the formulation of the next National Strategy, with a view to the period from FY2009 onwards. It is necessary to discuss the measures from a long-term perspective so that they can be implemented on a full scale under the next plan.

The area related to the second issue is creating a foundation that is firm and strong enough to promote mainly the measures for information security. Japan can only truly become a country with advanced information security when there is a combination of promotion of the measures taken by implementing bodies and a firm and strong foundation. Efforts have been made by setting priority goals mainly in the implementation fields in FY2006 and FY2007. In addition to this, it is necessary in FY2008 to make intensive efforts towards enhancing the information security infrastructure.

With respect to the third issue, it is necessary to consider the time lag between the implementation of measures and the manifestation of their social impacts (outcomes). As described thus far, information security measures have produced steady outputs (progress in efforts), and it is therefore necessary to proactively continue the efforts while making revisions if there are problems regarding the feasibility and direction of measures. From this standpoint, the measures should continue to be upgraded in accordance with the PDCA cycle.

It can be said that a relatively large proportion of projects implemented before FY2007 have focused on developing the foundations for efforts, such as tools and systems − in other words, on building a platform for the manifestation of social impacts (outcomes). Examples of such projects are the development of the GSOC, discussions for the establishment of the CEPTOAR Council in the area of critical infrastructure, development of guidelines to cope with the Japanese version of SOX in the business sector, efforts for the establishment of a council for public and private partnerships in the area of human resources, and submission of various suggestions to international conferences. While using such a foundation for the efforts, it is also necessary, in the future, to proceed with efforts for a manifestation of the outcomes − the fruits of the efforts.

Section 2: Priorities of Information Security Measures in FY2007

The focal point of Japan’s information security measures in FY2008 is to continue efforts for a manifestation of substantial social impacts (outcomes) through “intensive efforts to enhance the information security infrastructure,” while considering responses to the limitations of existing promotion systems based on a long-term perspective, the frameworks for measures and the technological level. With respect to the four basic policies listed in the National Strategy, the following four efforts will be made: (1) continuous efforts to maintain/improve shared awareness between public and private entities, (2) efforts to somewhat overcome the limitations of existing technology through pursuing advanced technology, (3) continuous efforts to enhance the response capability of the public sector, such as efforts related to GSOC, and (4) efforts to enhance outputs through stronger cooperation/coordination of both domestic and international entities.

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

Information security measures in SJ2008, as in SJ2007, 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 FY2008, prioritizes the promotion of the following measures in government agencies, with the purpose of 1) upgrading the level of the Standards for Measures[7] 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 FY2009.

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

[7] "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)

that contractor deploy.

[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 FY2008.

Furthermore, based on knowledge and experience obtained through measures by government agencies, discussions will be held on the status of the Standards for Measures and revisions will be made based on the discussion results.

B) Establishment and Penetration of the PDCA Cycle

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

Each government agency will work for the thorough establishment and penetration of the PDCA cycle in the entire organization by, for example, taking initiatives to improve the measures based on the results of self-assessment and auditing of the implementation of information security measures.

Particularly, in FY2008, each government agency will make efforts to improve and enhance the implementation systems associated with information security auditing, to get an accurate understanding of the status of implementation of measures for all employees and information systems, and to raise employee awareness about security measures.

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

The Cabinet Secretariat will ensure the stabilization of 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 a full-scale evaluation and promote improvement in the information security measures at each government agency from the perspectives listed below. 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 the ISPC) and "The Best Form of Japanese Society and Evaluation of Measures" (decision made on February 2, 2007). At the same time, the Cabinet Secretariat will conduct discussions on the form of evaluation of government agencies after the period of the National Strategy, based on the knowledge and experience acquired through governmental measures in the past.

The implementation of routine evaluations will, in principle, be enforced based on a predetermined schedule and inspection items presented to each government agency by the Cabinet Secretariat, while taking the workload of each government agency into consideration, except for cases where an urgent evaluation is needed, 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)

With regard to evaluations of information security management at each government agency, the evaluation method and results of a pilot evaluation performed in FY2007 will be studied in an attempt to establish an effective evaluation method to facilitate improvements in information security measures.

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 continue to 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 continue to 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 continue to 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.

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 FY2008 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 FY2008 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 FY2008 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 revised with more emphasis on IT governance and operations, etc. 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. The Guidelines will be promoted to be utilized and prevailed throughout government agencies.

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, in FY2008 the Information-technology Promotion Agency (IPA) will start to provide support tools via the Internet for IT security evaluations and checking the suitability of the use of authentication products in the authentication system. At the same time, a function will be added to provide more detailed specifications of the authentication products that are already available.

Moreover, the use of said tools in government agencies, etc. will be promoted.

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 FY2008.

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

Continuously in FY2008, 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[8] 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

[8] 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, in principle.

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) Enhancement of method of ensuring the information security of e-Government at the planning/design stage (Security by Design: SBD) (Cabinet Secretariat, Ministry of Internal Affairs and Communications and relevant agencies)

It is absolutely essential to incorporate information security requirements appropriately into the operations and systems of e-Government that are currently under construction. Thus, discussions will be conducted on a method for planning and designing an information system that incorporates information security as a basic concept, and the outcome of the discussions will be reflected in government policies.

B) 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 as part of SBD with regard to the necessary technological and functional aspects for a common platform that will serve as the foundation for the operations and systems of the entire government, and for the establishment of next-generation e-Government.

C) 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 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. VM will enable intensively providing information security functions independent of the existing OS and applications environment. In FY2008, efforts will be made to improve the performance of Secure VM and expand its application environment, and at the same time, empirical experiments assuming government agencies use will be conducted and the issues involved in actual operation will be organized.

D) 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) was launched in FY2007 and will be continued on the basis of past achievements. 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.

E) 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 FY2008, in accordance with the development (installation) or renewal of each information system. The following measures will be taken for a smooth implementation.

1) In continuance from the previous year, each government agency will proceed with IPv6 adoption in FY2008 in line with the “e-Government Promotion Plan” (partially revised on August 24, 2007 by the Conference for Chief Information Officers (CIO)), using the “Guideline for e-Government IPv6 Systems” (released by the Ministry of Internal Affairs and Communications on March 30, 2007) as a reference.

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 FY2008.

F) 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)

In order to present requirements and regulations for the electronic authentication systems of government agencies, discussions will be held on the rough draft of the “Guidelines for Authentication in e-Government” (provisional name), which will then be compiled. Based on the results of the discussions, usage scenarios will be studied as part of SBD.

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

The Cabinet Secretariat will continue discussions on 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.

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

[Specific Measures]

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

With respect to domain names used by government agencies when sending messages and information to the general public, efforts had been made up until FY2007 to use domain names that authenticate the identity of government agencies, and such efforts will be widely disseminated to the general public in FY2008.

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)

[9] 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.

In order to prevent spoofing and falsifying of e-documents from government agencies, 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, issues will be extracted concerning the best forms of intra-government systems for performing e-signatures.

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

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

[Specific Measures]

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

Monitoring of e-Government recommended ciphers, study and research for ensuring safety and reliance of the e-Government recommended ciphers, and formulation of standards will all be conducted in FY2008.

B) Response to reduced safety of SHA-1 Hash function and RSA1024 public key encryption (Cabinet Secretariat, Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry and all government agencies)

1) The Cabinet Secretariat, Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry and all government agencies will promote efforts in accordance with the “Transition Guidelines concerning the SHA-1 Encryption Algorithm and RSA1024 Adopted by Government Agencies.”

2) The Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry will continuously monitor the safety of the SHA-1 and RSA1024 currently in use, as well as SHA-256 and RSA 2048, which will be in use subsequently. The Cabinet Secretariat will promptly provide each government agency with the necessary information.

C) Efforts for the safe use of ciphers in government agencies (Cabinet Secretariat, Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry)

The Cabinet Secretariat will compile guidelines for the transition of technology systems to maintain safety, as done in the case of SHA-1 and RSA1024, so that the necessary guidelines can be developed in the case where risks are likely to arise in the near future as a result of a drastic reduction in the safety of any of e-Government Recommended Ciphers list, other than SHA-1 and RSA1024. The Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry will promote the efforts to revise the e-Government Recommended Ciphers list.

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 FY2008. When procuring cryptographic modules, priority is given to the products certified by the relevant system as required.

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) Full-scale operation of the GSOC and enhancement of the analyzing capacity

(Cabinet Secretariat and all government agencies)

The GSOC, which started to be developed in FY2007, will come into full operation, with an aim to effectively prevent cyber attacks against government agencies and the occurrence of information leaks and system failures at government agencies, and rapidly and accurately respond to the occurrence of such incidents. Furthermore, efforts will be made to establish a cross-sectoral function ("Public-Private Partnership Scheme for Analysis Functions" (provisional name)) to analyze attacks, etc., in cooperation with related organizations both abroad and at home.

b) Research and study of the trend 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., following FY2007.

B) Supporting strengthening of emergency response capability of each government agency

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

Based on the state of operation of the GSOC, which will be in full operation in FY2008, the general trends and situations concerning cyber attacks against government agencies will be analyzed, and the results will be periodically provided to each agency. Efforts will also be made to enhance the system for the timely provision of information, including results of analysis of attack techniques that will be needed for individual measures.

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

In order to respond to advances in the cyber attack techniques that can be used in cyber terrorism and to increased threats linked to the hosting of the Toyako Summit and other events, the system for measures taken by the police against cyber terrorism will be strengthened and improved in FY2008, including enhancement of the information collection/analysis systems and provision of training within and outside the department, to maintain and improve the incident response capability and personnel skills for combating 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 for cyber attacks against information systems of Ministry of Defense, analysis equipment for network security will be studied and prototyped. Basic research will be performed on monitoring and analyzing technology against unauthorized computer access, cyber attacks and active protection technology, etc. continuously from FY2007.

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) Enhancement of education programs for government officials (Cabinet Secretariat and Ministry of Internal Affairs and Communications)

Based on the progress of deliberations conducted in FY2007, efforts will be made to improve the quality of integrated education programs for government officials (general employees, executive officers and personnel in charge of information security) and to expand the opportunities to participate in training sessions.

B) Deliberations concerning human resource development of government officials

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

Discussions will be continued concerning integrated education programs for the government to furnish government staff with 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)

Discussions will be continued 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)

Discussions will be continued 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) Implementation 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 FY2007, 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 furthermore 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)

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, BCP of ICT division, management of personal information concerning outsourcing) 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. Information security auditing will be promoted in line with the Guidelines for Information Security Auditing by Local Governments revised in FY2007. Specifically, internal auditors will be dispatched to those local governments where less progress has been made.

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 FY2006 to share information pertaining to information security among local governments. Support, such as necessary advice, will be continuously 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) Review of information security training for local government officials (Ministry of Internal Affairs and Communications)

Based on the guidelines concerning information security assurance at local governments, which were revised in September 2006, training will be reviewed, including the provision of courses in accordance with the authority/responsibility of each organizational system, and will continue to be offered for a wide range of local government officials.

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 FY2009, 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, hereinafter referred to as the "Action Plan"), and the following measures will be primarily promoted in FY2008.

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

Based on the "A Principle for Formulating of 'Safety Standards, Guidelines, etc.'[10] concerning Assurance of Information Security of Critical Infrastructures"[11], 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[12])

Based on the revision of the guidelines conducted in FY2007, confirmation/ verification of safety standards in critical infrastructures will be performed by around September 2008. Moreover, revisions of safety standards will be conducted on as-needed basis.

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

[10] "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.

[11] "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)

[12] "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))

The progress in verifying/validating and reviewing the “Safety Standards, etc.” for each critical infrastructure will be monitored and examined in FY2008, in cooperation with the competent authorities overseeing critical infrastructures.

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

Based on the results of studies in FY2007, the Cabinet Secretariat will conduct planning and preparation to implement studies on the dissemination of Safety Standards, etc. in each sector of critical infrastructure. These studies are scheduled to be implemented in early FY2009, with the cooperation of the relevant authorities overseeing critical infrastructures.

C) Review of the Principles (Cabinet Secretariat)

Based on the progress in reviewing the action plan and the outcome of interdependency analysis, the Cabinet Secretariat will conduct analysis/validation to shed light on the awareness of issues relating to information security measures, in cooperation with the agencies overseeing critical infrastructures and will launch an examination of those measures, such as revision of the guidelines, on an as-needed basis.

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)

a) Consideration for functions/requirements to be added to the information sharing system (Cabinet Secretariat)

The Cabinet Secretariat will consider the functions/requirements to be added to the information sharing system based on the progress in reviewing the Action Plan, the development of the CEPTOAR in each field and the deliberations conducted by the "Preparation Committee for Establishing the CEPTOAR Council (provisional name)" (to be described hereinafter).

b) Strengthening the partnerships with related organizations, etc. (Cabinet Secretariat)

The Cabinet Secretariat will strengthen its partnerships with information security-related authorities, government agencies dealing with incidents and relevant organizations, and will provide infrastructure operators with information that contributes to the measures taken by each in a timely and appropriate manner.

c) Consideration for reviewing the implementing items in the Action Plan concerning information exchange/information provision (Cabinet Secretariat)

Based on the progress in the review of the Action Plan and the deliberations conducted by the "Preparation Committee for Establishing the CEPTOAR Council (provisional name)" and studies on cross-sectoral exercises, the Cabinet Secretariat will consider reviewing the implementing items in the action plan concerning information exchange/provision, with the cooperation of the agencies overseeing critical infrastructures.

B) Implementation of CEPTOAR training (Cabinet Secretariat and agencies overseeing critical infrastructures)

Based on the progress in developing the CEPTOAR in each sector, the Cabinet Secretariat and agencies overseeing critical infrastructures will provide training opportunities, contributing to the maintenance and improvement of the information-sharing function of the CEPTOAR.

(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) Follow-ups on the map to grasp the characteristics of the CEPTOAR (Cabinet Secretariat)

Based on the progress in each CEPTOAR activity and consideration of the functions and requirements in FY2008, follow-ups on the map to grasp the characteristics of the CEPTOAR will be conducted by the end of FY2008.

B) Development of a support system to improve the reliability of the information systems used for critical infrastructures (Ministry of Economy, Trade and Industry)

In order to support the proactive efforts of critical infrastructure operators to improve the reliability of information systems, the IPA Software Engineering Center will develop a database from an expert/technical perspective, conduct macro-based quantity analysis and provide the CEPTOAR, etc. with the accumulated information. Support will also be provided for information system development/operations upon requests from critical infrastructure operators.

(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)

In cooperation with the "Study Group for Establishing the CEPTOAR Council (provisional name)," the competent authorities formulated the "Basic Concept for the CEPTOAR Council (provisional name)," based on which the "Preparation Committee for Establishing the CEPTOAR Council (provisional name)" will be set up in cooperation with various CEPTOARs in critical infrastructure sectors in around June 2008. Said Preparation Committee aims to establish the CEPTOAR Council (provisional name) within FY2008.

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 order to enhance the systems for communication/cooperation between the public and private sectors and to improve the response capacity in the event of an IT failure, interdependency analysis will be further refined based on the summary of the interdependency analyses conducted in FY2006 and FY2007, and by studying various issues, such as the "cross-sectoral connections of systems".

Thorough discussions will be held on the method of implementation, at the 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[13] (Cabinet Secretariat and agencies overseeing critical infrastructures)

In order to improve communication/coordination systems and the response capability of the public and private sectors in the event of an IT malfunction, the Cabinet Secretariat will select themes to be examined as research subjects based on various conditions, such as a specific type of assumed threat scenario, while considering the knowledge obtained from interdependency analyses, in cooperation with the agencies overseeing critical infrastructures, business entities and CEPTOARs in each critical infrastructure sector, etc., as was continued from FY2007. It will conduct cross-sectoral exercises using a suitable method (such as simulations and functional exercises) for each theme and will enhance the exercises.

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 FY2008, as in FY2007, supposing cyber attacks that may occur on the internet that connect each

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

critical infrastructures with focus on telecommunications operators.

C) Implementation of awareness-raising seminars for critical infrastructure operators (Ministry of Economy, Trade and Industry)

IPA or JPCERT/CC will host the "Critical Infrastructure Information Security Forum", aiming to provide critical infrastructure operators with information concerning advanced measures against IT failures both overseas and in Japan in FY2008.

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

[Specific Measures]

A) Review of the Action Plan (Cabinet Secretariat)

Based on the discussions at the Expert Committee on Critical Infrastructure, the Cabinet Secretariat will compile a review plan (draft for public comment) during 2008, in cooperation with the agencies overseeing critical infrastructures. To do this, discussions will be conducted with a view to compiling a rough draft in around September 2008.

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 FY2009, the government prioritizes the promotion of the following measures in FY2007.

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, in FY2008, the competent ministry will formulate guidelines for the management of information and information system that give consideration to existing legal systems, to be conducted by corporations, so that the information security measures of corporations can be implemented effectively.

The “Guidelines for Improving the Reliability of Information Systems” formulated in FY 2006 will be reviewed mainly in the area of IT governance and operations, based on studies on the current situation of measures taken by corporations to improve the reliability of information systems. The “Evaluation Index concerning Improvement of the Reliability of Information Systems” will also be reviewed in the same manner. Furthermore, dissemination activities will continue in order to recommend corporations to refer to said guidelines when developing and managing information systems.

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 carriers, efforts will be made to disseminate and promote domestic standardization and authentication of the Information Security Management Guidelines for Telecommunications (ISM-TG), the telecommunications service guidelines formulated in FY2006 by the Information Security Conference for Telecommunications (ISeCT) – which comprises telecommunications service providers and related organizations – while giving consideration to the progress in international standardization and in cooperating with the ISeCT.

B) Review of bidding conditions (Cabinet Secretariat, Ministry of Internal Affairs and Communications, 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 incorporating assessments of the level of information security measures of bidders into tender offers/acceptance.

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

In order to achieve a fair share of the burden of information security measures among small- and medium-sized enterprises and promote those measures, the competent ministry will draw up a standard format to verify the progress in the implementation of measures in FY2008 and will continue deliberations on the package of information security measures for small- and medium-sized enterprises.

D) Utilization and dissemination of “Information System Model Transaction/Contract (first edition)” and “Information System Model Transaction/Contract (supplemental edition)” (Ministry of Economy, Trade and Industry)

In order to visualize transactions between users and vendors and clarify the roles of stakeholders from the viewpoint of improving the reliability of information systems, the “Information System Model Transaction/Contract (first edition)” was published in April 2007. In response to the issues raised in this Contract, the “Information System Model Transaction/Contract (supplemental edition)” is scheduled to be formulated and published in early FY2008. This is a simple and transparent transaction model using the “Explanatory Note of Important Matters” concerning transactions using Packages, SaaS[14] and ASP[15], which account for the majority of transactions of small- and medium-sized enterprises, in particular. Efforts will be made to disseminate model transactions/contracts, including the establishment of a certificate system, in cooperation with related industrial associations.

E) Utilization and dissemination of the "SLA Guideline for SaaS" (Ministry of Economy, Trade and Industry)

With an aim to secure an appropriate transaction relationship when corporations use SaaS and to allow corporations to use the service more effectively, the METI will promote widespread use and dissemination, among both users and service providers, of the "SLA Guideline for SaaS," which sets forth the security levels to be agreed between users and providers, with an emphasis on the standpoint of ensuring information security.

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]

[14] Software as a Service

[15] Application Service Provider

A) Promotion of the use of third party evaluation

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

Discussions will be made on the promotion and dissemination of the guidelines for the use of assurance-based audit formulated in order to disseminate an assurance-based information security audit in which an auditor provides some assurance.

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

In FY2008, 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 promoting the utilization of support tools to determine the availability of authentication products for the systems. Japan Cryptographic Module Validation Program implemented by IPA will also be promoted.

B) Preferential tax treatment

a) 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 FY2008 through dissemination and PR activities of the tax system for strengthening the information infrastructure to increase industrial competitiveness that will be expanded and extended for two years in FY2008.

.

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

The Survey on Information Processing will investigate the usage of information security audit systems in companies, 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.

D) Promoting dissemination of the use of electronic signatures by corporations (Ministry of Internal Affairs and Communications, Ministry of Justice and Ministry of Economy, Trade and Industry)

Based on the results of discussions at the "Study Committee concerning Enforcement of the Electronic Signature and Authentication Law," measures to disseminate and accelerate the use of electronic signatures by corporations will be prepared.

E) Promotion of information security measures for ASP/SaaS (Ministry of Internal Affairs and Communications)

In order to contribute to the promotion of information security measures for ASP/SaaS, which is currently spreading in the form of ICT services that can be the basis to improve companies' productivity, the competent ministry will support industry efforts for activities promoting the dissemination, continuous revision and improvement of the "Guideline on Information Security Measures for ASP/SaaS" (January 30, 2008), which was formulated by the Study Group on Information Security Measures for ASP/SaaS.

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 FY2008.

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

In order to deepen understanding of information security among owners of small- and medium-sized enterprises and information system personnel, "Information Security Seminars" co-hosted by the IPA and the Japan Chamber of Commerce and Industry will be held throughout the country in FY2008, and local community-hosted seminars will be held on a trial basis to explore further developments. At the same time, dissemination and public relation activities will be conducted in coordination with IT business supporters.

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

Based on the report of the Human Resources Development WG of the Information Service and Software Subcommittee, Industrial Structure Council, the competent ministry will prepare a framework of common careers/skills in FY2008 that systematically organizes the skills needed for advanced IT human resources, including those engaged in information security, in an attempt to attain consistency of IT Skill Standards, Embedded Technology Skill Standards, Standards for Information System Users' skills and Information-Technology Engineers Examination.

D) 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.

E) Reform of the system of Information-Technology Engineers Examination (Ministry of Economy, Trade and Industry)

In order to enhance the development of advanced IT human resources, including those in information security, Information-Technology Engineers Examination, which measure skills in various information technology fields including information security, has been drastically reviewed. New examinations will be held in FY2009, while ensuring consistency with the framework of common careers/skills.

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)

Led by the Japan Computer Emergency Response Team Coordination Center (hereinafter referred to as the "JPCERT/CC"), efforts will be made in FY2008 to further streamline coordination in emergencies and ordinary times among overseas Computer Security Incident Response Teams (hereinafter referred to as "CSIRTs") and the domestic CSIRTs by using a shared system (already developed by FY2007) for those in need of specific information pertaining to threats/remedial measures, including the necessary analysis required.

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 FY2008.

C) Support for management of software vulnerabilities, etc. (Ministry of Economy, Trade and Industry)

In FY2008, the Ministry of Economy, Trade and Industry will commence operation of a system of information provisions at the IPA that allows vendors and users to quantitatively compare the seriousness of vulnerabilities, and will examine the enhancement of functions.

JPCERT/CC's activities to support and raise awareness of the importance of vulnerability management of software, etc. at user organizations will be enhanced. Specifically, JPCERT/CC will enhance the promotion, dissemination and improvement of various tools (partially developed in FY2007) and methods that will contribute to vulnerability management at organizations, including critical infrastructures.

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 FY2009, the government will intensively promote the following measures in FY2008.

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)

Efforts will be made to further promote information security education through information ethics education, for example, by hosting a forum to help children understand the importance of information ethics, including information security.

b) Research and development of programs to foster ICT media literacy[16] (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 programs 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 FY2006. The developed programs were made publicly available on July 2007 and are promoted to be widely disseminated to organizations engaged in fostering ICT media literacy. The efforts to disseminate these programs

[16] 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.

will continue in FY2008 and revisions will be made as necessary.

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

In FY2008, 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)

By using the "Criteria (checklist) for Teachers' Ability to Teach ICT," which include the ability to teach children to acquire basic knowledge on information security, the competent ministry will conduct a nationwide survey and improve teachers' ability to teach ICT, so that all teachers can 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)

"Internet Safety Classes" will be held throughout the country, continuously from FY2007, in an attempt to disseminate basic knowledge on information security among general users, and the "National Council for the Internet Safety Classes" will be organized to facilitate information sharing/coordination among private organizations that host said safety classes.

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 FY2007, in cooperation with telecommunications-related organizations.

c) Cyber Security College (National Police Agency)

Continuously from 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.

C) Developing young human resources engaged in advanced security (Ministry of Economy, Trade and Industry)

In FY2008, the competent ministry will run training camps for young people to improve their security awareness and find and develop competent security human resources, by providing practical lessons that invite front-line engineers in the industry as lecturers. Seminars will also be offered throughout the country to disseminate the results/contents of the lectures.

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 FY2008, 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 FY2007 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 crimes, etc., the competent agency will provide advice on basic remedial measures tailored to the problems that individual users might experience in FY2008, using Consultation Systems for Internet Safety and Security. Also, in order to prevent damage from crimes associated with dating websites, the competent agency will prepare leaflets targeting junior and senior high school students, which will then be distributed at municipal police stations and listed on the website of the National Policy Agency, thus implementing effective publicity and awareness-raising activities.

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

Starting from FY2008, each Bureau/Office of Telecommunications will commence operation of mobile vehicles for consultation about radio wave utilization environment, to provide citizens with a consultation service concerning the environment for radio wave use.

Dissemination and awareness-raising campaigns are planned during the designated Radio Wave Protection Period in June 2008, which includes encouragement to check a “technical conformity mark” through various media (national papers, local papers, industrial magazines, TV commercials, radio spots, advertisements on trains and buses, billboard screens, theater ads, distribution of posters or display on message boards of local governments/related organizations, distribution of leaflets, and notices in various PR magazines).

Furthermore, each Bureau/Office of Telecommunications will conduct dissemination and awareness-raising activities for stores selling radio communication devices during May-July and September-November 2008, and put banner advertisements for the “technical conformity mark” on news websites in June.

e) Campaign under a "Slogan for the Safe and Secure Use of Information and Communications" (Ministry of Economy, Trade and Industry)

The Council for the Promotion of Safe and Secure Information and Communication will promote improvement in the awareness of information and communications users, including beginners, by soliciting slogans concerning rules, manners and information security for using information and communications safely and securely, and posting award-winning posters, etc.

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 NISC (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 FY2008.

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 2008" will be posted on the English website of the National Information Security Center within FY2008.

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 FY2010 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[17] by FY2009, empirical experiments, which model the user environment, will continue in FY2008 to solve the issues associated with security assurance toward creating a ubiquitous environment by IPv6.

[17] 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.

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

In FY2008, the competent agencies will continue dissemination and awareness-raising regarding safety measures for wireless LAN through the guidelines for wireless LAN security, entitled "Guide for Safe Use of Wireless LAN," and also through the "Internet Safety Class."

D) Information collection/provision on malicious sites through proactive efforts (Ministry of Economy, Trade and Industry)

Recent illicit programs (malware) such as computer viruses are shifting from the traditional types sent out in bulk via e-mail to ones that are downloaded by users from websites or that remain invisible by entering clandestinely, exploiting the vulnerabilities of browsers, etc. In response to these illicit programs, it is increasingly necessary to proactively collect samples and information by using the same access methods as general users.

Thus, the competent ministry will operate an automatic system to gain access to Internet websites, collect/analyze malware, etc., and will accumulate the analyzed data and provide a wide range of general users with relevant information immediately.

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 FY2007.

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

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

[Specific Measures]

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

The ISPC, in cooperation with the Council for Science and Technology Policy, will 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 continuously from FY2008.

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 continuously from FY2007, 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 FY2007 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 continuously from 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 Backbone[18] by detecting and controlling abnormal traffic that would never occur in normal networking by FY2009, the competent agency will continue promoting research and development activities of the Next Generation Backbone in FY2007.

c) Research and development on detection of, recovery from and prevention of route hijacks[19] (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 FY2009, 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 a new-generation technology for information security (Ministry of Economy, Trade and Industry)

As information technology becomes a social infrastructure, information system incidents may impede the activities of the entire economy and bring risks to people’s lives and property. Hence, the competent ministry will conduct research and development of a new-generation technology for information security with the aim of reaching an ultimate solution, instead of managing symptoms.

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

[19] 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.

f) 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 conducted continuously from 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.

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

Discussions will be conducted continuously from 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.

h) Research and development of technology for a new-generation network infrastructure (Ministry of Internal Affairs and Communications)

The competent ministry will promote R&D of technology for a new-generation network infrastructure that can meet the varied and diverse needs of users and ensure optimal quality and security with ease and flexibility. In continuation from 2007, the ministry will develop fundamental dynamic network technology and conduct concept design for the new-generation network architecture in 2008.

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 be conducted 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 continuously from

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, 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.

In FY2008, efforts will be made to improve the performance of Secure VM and expand its application environment, and at the same time, empirical experiments assuming government agencies use will be conducted and the issues involved in actual operation will be organized.

c) Promotion of technical development, etc. toward the establishment of Digital Forensics[20] (National Police Agency)

Technical cooperation with private companies, etc will be promoted concerning Digital Forensics and development of technology regarding analysis of information technology will also be promoted in FY2008.

d) 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 FY2007. In FY2008, 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.

e) Promoting the advancement of critical communications in IP network systems (Ministry of Internal Affairs and Communications)

[20] 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.

In order to ensure critical communications in IP networks at times of disaster, the competent ministry will take necessary measures, conduct technology development and provide support by continuing studies from 2007, and will consider and organize the process for advancing critical communications by the end of 2008.

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 conducted continuously from 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.

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)

In cooperation between the Council for Science and Technology Policy (CSTP) and the Information Security Policy Council (ISPC), specific discussions will be conducted in FY2008 on more detailed themes, giving consideration to the project implementation period, project size, promotion system, budget and laws and regulations concerned.

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 FY2007.

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 FY2008 to create an environment where people can use IT safely and comfortably.

Moreover, the MEXT will make efforts toward the more efficient and effective dissemination and development of results obtained through the development and implementation of various education programs at each center, and will also support projects intended to elaborate and refine education materials.

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

Based on the report of the Human Resources Development WG of the Information Service and Software Subcommittee, Industrial Structure Council, the competent ministry will prepare a framework of common careers/skills in FY2008 that systematically organizes the skills needed for advanced IT human resources, including those engaged in information security, in an attempt to attain consistency of IT Skill Standards, Embedded Technology Skill Standards, Standards for Information System Users' skills and Information-Technology Engineers Examination.

C) 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 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.

D) 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 those in information security, Information-Technology Engineers Examination, which measure skills in various information technology fields including information security, has been drastically reviewed. New examinations will be held in FY2009, while ensuring consistency with the framework of common careers/skills.

E) 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 FY2008.

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 FY2008.

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, embodiment of the basic policies and specific measures formulated in FY2007 to strategically address international cooperation/contribution will be launched.

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 FY2008, 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) Establishment of an information security policy conference in Asia (Cabinet Secretariat, Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry)

In order to contribute to the establishment of a secure business environment in Asia, with which Japan has increasingly been enhancing its economic ties, and to the regional response for ensuring a stable network environment, the competent agencies will establish a new policy conference concerning information security between Japan and ASEAN countries, conduct policy dialogues at a senior official level, conduct policy research studies and dissemination/awareness-raising activities using international research institutions, etc., and discuss further the enhancement of cooperation between Japan and ASEAN based on the results of above efforts.

D) Enhancement of information-sharing system, etc. concerning network information security in Japan, China and Korea (Ministry of Internal Affairs and Communications)

Through the ICT Network and Information Security Working Group of Japan, China and Korea (established in 2004), the competent ministry will enhance information sharing on the basic policies, incident reports, security trends, etc. of each country and promote cooperation with related organizations, including the industry group of network operators .

E) 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 FY2008, to serve as an interface to facilitate effective and smooth cooperation with other countries.

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

In FY2008, 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.

G) 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 FY2008, in line with the progress of the revision work of the relevant guidelines by OECD.

H) 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 FY2008 and discussions will be deepened with other countries on occasions, such as policy dialogues, on an as needed basis.

I) Hosting of APT Training/Seminar (Ministry of Internal Affairs and Communications)

A training program titled "Construction of Information Security for Broadband Communications" will be offered in FY2008 through a special contribution by Japan to the Asia-Pacific Telecommunity (APT).

J) Support for enhancement of CSIRT systems overseas (Ministry of Economy, Trade and Industry)

The METI will provide support for the establishment of CSIRTs in the Asia-Pacific region, etc. through the JPCERT/CC. In FY2008, the ministry will provide support for the sharing of technologies and experience in incident response operations accumulated by the JPCERT/CC.

Since events attracting the world's attention, such as the Olympic Games and the G8 Summit meeting, will be taking place in Asia, the ministry will cooperate to improve the coordination capability of Asian countries to enable them to make fast and effective incident responses by further enhancing cooperation with CSRITs in other countries, through conducting incident response exercises in the Asia-Pacific region.

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 FY2007, 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) Promoting the sharing of early warning information in the Asia-Pacific region, etc. (Ministry of Economy, Trade and Industry)

In FY2008, the JPCERT/CC will install a system developed in FY2007 in the Asia-Pacific countries and will launch pilot operations with the purpose of establishing a common system for Internet observation from a fixed point in the Asia-Pacific region, while maintaining cooperation with related organizations in the region.

The ministry will promote the regional expansion of target delivery areas and interactive deliveries of the information on threats and information analysis concerning software vulnerabilities, etc., which JPCERT/CC is transmitting daily to each CSIRT in the Asia-Pacific region from FY2007.

C) 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.

D) Enhancement of information security management in the telecommunications business (Ministry of Internal Affairs and Communications)

With an aim to internationally standardizing the Guidelines for Information Security Management in the area of telecommunications, the competent agency proposed the Information Security Management Guideline for Telecommunications (ISM-TG) described in Chapter 3, Section 3, 1) to the International Telecommunications Union in FY2006 and FY2007, and they were then adopted as an international standard. In FY2008, efforts will be made for the adoption of this proposal as an International Organization for Standardization (ISO) international standard, thus contributing to enhancing the level of information security management on an international scale.

E) Promoting the creation of a secure business environment in the Asian region (Ministry of Economy, Trade and Industry)

The ministry will conduct joint research with Asian researchers, while utilizing Japan's knowledge and experience about methods for promoting the creation of a secure business environment in the Asian region.

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 FY2007 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)

The competent agency will reinforce and improve the system to appropriately respond to cyber crimes in FY2008: for example, by contracting out cyber patrol operations to the private sector.

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 collecting and analyzing information of crimes or illicit activities, etc. by illicit programs or file sharing software.

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 critical infrastructure operators will be conducted to increase awareness about measures against cyber terrorism on an as-needed basis in FY2008, in accordance with the characteristics of the operations of critical infrastructure operators. Efforts will also be made to contribute to emergency response activities in the event of the occurrence of cyber terrorism, by implementing joint exercises and by giving critical-infrastructure operators opportunities for participating in various types of drills, while respecting the intentions of critical infrastructure operators.

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

In FY2008, 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[21] (Ministry of Justice)

The competent agency will expedite the mutual provision of assistance by designating the investigative authority as the central authority through direct communication between central authorities, without going through diplomatic channels. Agreements on mutual investigation assistance have already come into force between Japan and the U.S. and between Japan and the ROK. An agreement on mutual investigation assistance was signed between Japan and China on December 1, 2007 and the competent agency will expedite the necessary procedures, such as early approval of the Japan-China agreement by the Diet, and work on concluding the ongoing negotiations on agreements on mutual investigation assistance with Hong Kong and the Russian Federation. The competent agency will also consider designating a "central authority" under the cyber crime convention, upon consultation with the relevant agencies.

h) Enhancement of the measures to prevent interference with important radio communications (Ministry of Internal Affairs and Communications)

・The competent agency will ensure the radio monitoring enhancement system, including the implementation of training, in preparation for the Toyako Summit,

[21] 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.

and will set up the Headquarters to Handle Interference with Important Radio Communications within the Ministry of Internal Affairs and Communications, thus taking all possible measures to respond to the occurrence of interference of important radio communications.

・In order to maintain order in radio wave use, remote control radio wave monitoring facilities will be renewed and their performance will be improved in FY2008, and 27 DEURAS sensor stations will be installed in areas where interference occurs frequently.

・Consideration will be conducted on the improvement of functions and performance of the uplink interference source identification system with pilot operation and the installation of radio source visualizing system (short burst wave compatible devices) into the system. Studies and research on broadband monitoring technology will also be conducted.

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

In FY2008, 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 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) Promotion of dissemination of Provider Liability Limitation Law to Limit Liability of Providers and related guidelines (Ministry of Internal Affairs and Communications)

As done previously, the Ministry of Internal Affairs and Communications will provide support for the dissemination of said Law and related guidelines through the websites of related trade organizations.

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 FY2008, 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 FY2008 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 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, as policy related measures, establish the Standards of Measures and PDCA cycle based thereon and implement the measures described in Chapter 3, Section 1 by, for example, formulating the system for the full-fledged operations of GSOC 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 NISC will continuously 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.

(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 FY2008, 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) Analysis of/recommendations on information security (Ministry of Economy, Trade and Industry)

An information security analysis laboratory will be set up in FY2008 as an information security analysis department of the IPA. The Laboratory will conduct studies to analyze threats, attacks, risks and remedial measures in the area of information security, from socio-economic and technological perspectives, and subsequently make recommendations.

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 FY2008.

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.[22] (Cabinet Secretariat)

The Cabinet Secretariat will announce the progress of the implementation of specific measures listed in SJ2008 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 government agencies (Cabinet Secretariat)

The 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.

C) Review of "Action Plan (Cabinet Secretariat) [Reprise]

Based on the discussions at the Expert Committee on Critical Infrastructure, the Cabinet Secretariat will compile a review plan (draft for public comment) during 2008, in cooperation with the agencies overseeing critical infrastructures. To do this, discussions will be conducted with a view to compiling a rough draft in around September 2008.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

[22] In this chapter, "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).

designed and carried out, even in the midst of implementing SJ2008.

(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.[23], 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.

The Ministry of Internal Affairs and Communications conducted deliberations in FY2006 and FY2007 concerning methods of evaluating the responses of telecommunications carriers to cyber attacks, as part of cyber attack response exercises in the telecommunications sector. These are listed in SJ2006, Chapter 2, Section 2-(4) and in SJ2007 Chapter 3, Section 2-(4). In FY2008, the use of the relevant evaluation criteria by telecommunications carriers in said exercises will be promoted and discussions will be held on improving the criteria.

[23] In this chapter, "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 Issues to Be Addressed Urgently in FY2009

~ Priorities for FY2009: "Development of Infrastructure towards Establishment of Systems to Promote Sustainable Information Security Measures" ~

Chapter 3 to Chapter 5 listed specific measures to be implemented in FY2008, the third and final year of the three-year National Strategy. These measures emphasize the "efforts for enhancing information security infrastructure" based on the efforts made in the previous two years, FY2006 and FY2007.

Through the development of the efforts of these three years – specifically, "Establishing the System for Information Security Measures in the Public and Private Sectors" in FY2006, "Upgrading of Information Security Measures in the Public and Private Sectors" in FY2007, and "Intensive Efforts for Enhancing Information Security Infrastructure" in FY2008, the final year – substantive benefits have been produced in the effort to achieve the objective of the National Strategy; that is, the "Establishment of a New Model of Public and Private Partnership." In specific terms, each implementing body (the central and local governments, critical infrastructures, corporations and individuals) is now aware of the necessity of information security measures, and systems for such measures have been developed. In addition, central and local governments, educational and research institutions, information-related operators, NPOs and media, which are the bodies that facilitate the understanding and solution of problems, have made various efforts to promote measures by implementing bodies, thus contributing to the improvement of the measures.

Based on the results of the efforts during these three years, the Information Security Policy Council has set up the "National Strategy Review Committee" to hold deliberations on the Next (Second) National Strategy on Information Security. This will be the mid-term plan for FY2009 and onwards. At the same time, as a result of assessment of the efforts in the last three years, issues that should be addressed have come to the surface.

Specifically, the last three years have merely developed the "(tentative) system/foundation to implement measures under the existing conditions/systems." In other words, it is hard to say that a sustainable framework has been sufficiently established to modify and improve measures flexibly in accordance with changes in technological innovations in IT and the social systems, while continuing to implement information security measures accurately with a view to the next five or more years.

For instance, government organizations have achieved some results in this short three-year period in terms of implementing measures based on the PDCA cycle using the Standards for Measures as a tool. Still, several responsible officers in each ministry or agency are trying to disseminate the measures throughout the organization, and there is room for improvements in the areas of dissemination and penetration among the organization and employees, efficiency of measures, and reduction of burdens. Some ministries and agencies have yet to develop a management system for the entire organization. Also, since such responsible officers are transferred to other sections on a two to three year rotational basis, the know-how and skills for implementing measures cannot be fully handed over, with the resultant issue that it is hard to maintain effective and efficient measures.

In critical infrastructures, too, each operator has been making efforts for information security measures. To further these efforts in the future, it is very important to increase the awareness of society as a whole about these efforts.

Under these circumstances, measures will be promoted in FY2009, with "Developing a Foundation for the Establishment of a System to Promote Sustainable Information Security Measures" as a priority issue to be urgently addressed, while bearing in mind the direction of the next National Strategy.

Section 1 Developing the Foundation for Establishing Systems to Promote Sustainable Information Security Measures by the Government

[Specific Measures]

A) Consideration for introduction of a management system for cross-organizational information security measures (Cabinet Secretariat)

It is necessary to gain the understanding of the entire organization and implement measures thoroughly, led by the department in charge of information security, in order to help information security measures be sustainably implemented by the organization as a whole. Discussions will be held on the system needed to achieve this objective and on the introduction of an effective management system.

B) Study on the state of objective scrutiny functions (Cabinet Secretariat)

Objective scrutiny functions (particularly the monitoring function and advisory function) are required to make the PDCA cycle of government organizations proactive and sustainable. Thus, the competent agency will discuss the state of scrutiny functions, such as ensuring objectivity, ensuring implementation capability, etc.

C) Promoting the methods of addressing the information security of e-Government at the planning and design stage (Security by Design: SBD)

It is absolutely essential to incorporate information security requirements appropriately into operations and systems for developing e-Government. Therefore, efforts will be made to promote methods of planning/designing information systems that incorporates information security as a basic concept (SBD), using opportunities such as the next cycle of the optimization plan for the establishment of e-Government.

D) Support for upgrading information security measures of small- and medium-sized ministries and agencies (Cabinet Secretariat and relevant ministries and agencies)

In order to upgrade the measures of small- and medium-sized ministries and agencies that do not have sufficient financial and personnel resources to promote information security measures, efforts will be promoted to provide expert knowledge and know-how efficiently.

E) Promoting use of the Guidelines for e-Government Authentication (Cabinet Secretariat)

With respect to electronic authentication, which is applied to the electronic administrative service of each ministry and agency based on its own discretion, the use of the Guidelines for e-Government Authentication (provisional) in government organizations will be promoted, based on the results of discussions conducted in FY2008, in order to organize and clarify the levels of authentication strength in accordance with the level of risks, while maintaining safety.

F) Efforts based on the “Guidelines for the Transition of the SHA-1 and RSA1024 Encryption Algorithms that are Used in Government Information Systems” (Cabinet Secretariat, Ministry of Internal Affairs and Communications and all government agencies)

A reduction in the safety of the SHA-1 and RSA1024 encryption algorithms has been reported. In order to ensure the safety and reliability of government information systems, efforts will be made to replace the encryption algorithms with safer ones in a timely manner, while considering the life cycle of the information system.

G) Priority on ensuring human resources in information security (Cabinet Secretariat and all government agencies)

In dealing with the chronic shortage of personnel associated with information security measures in government agencies, efforts will be made to secure experts and personnel in charge of the practical operations of information security measures – for example, allocating a Chief Information Security Advisor – who will serve as key players in the information security measures of each government agency.

H) Enrichment of education programs for government employees (Cabinet Secretariat and Ministry of Internal Affairs and Communications)

While giving consideration to the progress in discussions in FY2008, efforts will be made to improve the quality of integrated education programs for government employees (general employees, executive officers and officials in charge of information security measures) and to increase the number of attended lessons.

I) Enhancement of the emergency response capability of government organizations to cyber attacks (Cabinet Secretariat)

Based on the state of operations of the GSOC, which will commence full operations in FY2008, and the progress in the development of emergency response systems at each government agency, efforts will be made to strengthen cooperation between government agencies and related organizations in the public and private sectors, enhance communication systems in the event of emergencies, strengthen analysis and planning functions for attacks, and improve the overall emergency response capability against cyber attacks.

Section 2 Developing the Foundation for Establishing Systems to Promote Sustainable Information Security Measures in Areas of Implementation of Measures

A) Publicity and public hearing activities for the efforts of the entire critical infrastructure (Cabinet Secretariat)

Through enhancing publicity for efforts for the information security measures of critical infrastructure operators, the government will promote public understanding of the information security measures taken by those operators, as an indirect support for their information security activities.

B) Promoting studies on the implementation of information security measures by telecommunications operators (Ministry of Internal Affairs and Communications)

Discussions will be held about the information security measures to be implemented as preventive measures by telecommunications operators, in light of situations where the individual Internet users of bot-infected computers can become not only victims but also victimizers, unknowingly causing damage to others.

C) Promoting efforts to improve the level of information security measures taken by local governments (Ministry of Internal Affairs and Communications)

Efforts will be made for solid penetration into local governments (including small ones) of specific methods for analyzing risks of information assets, and of the prevention of information leakage associated with the outsourcing of information systems, which are scheduled to be discussed in FY2008. At the same time, information security monitoring will be facilitated to effectuate the PDCA cycle. Support will also be offered to the efforts of local governments to formulate the Business Continuity Plan (BCP) of ICT departments, in order to prevent suspension of business and to ensure early business recovery in times of disaster.

D) Promoting the continuous implementation of dissemination and enlightenment activities concerning the importance of information security measures for ICT service users (Ministry of Internal Affairs and Communications)

In response to the current situation, where methods of malware infection via the Internet are constantly becoming more advanced and sophisticated the competent ministry will promote the continuous implementation of dissemination and enlightenment activities for the information security measures recommended to be taken by users.

E) Promoting advanced R&D through industry-academia-government collaboration, in response to the advancement and sophistication of methods of malware infection (Ministry of Internal Affairs and Communications)

To deal with the current situation, where methods of malware infection via the Internet are becoming more malicious and the damage is becoming more localized, the ministry will enhance advanced R&D in order to promptly grasp the situation and establish appropriate remedial measures against system failures.

F) Enhancement of measures against spam e-mail messages (Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry)

Necessary measures will be taken in order to increase the effectiveness of measures against the increasing volume of spam e-mail messages, which are becoming more sophisticated and malicious, such as by developing the necessary systems and making operations against spam e-mail messages more advanced.

In cooperation with industrial associations such as the JEAG (Japan Email Anti-Abuse Group), a private organization founded mainly by major Internet service providers and mobile phone operators in Japan, the competent ministries will promote technology that is effective in stopping the transmission of spam e-mail messages, such as No.25 port blocking and sender ID authentication.

In order to block the increasing number of spam e-mail messages sent from overseas, the competent ministries will strengthen cooperation with foreign authorities that implement anti-spam measures and promote the introduction of international anti-spam measures in the private sector.

In addition, the competent ministers will continue to implement the “Project for Banning Unsolicited E-Mail” (February 2005 onwards), which provides information on spam e-mail messages to the Internet service providers concerned so that they can take the necessary measures, such as suspending service, etc.

G) Promoting the establishment of information security governance (Ministry of Economy, Trade and Industry)

In order to promote efforts to establish information security governance in corporations, efforts will be made to disseminate the guidelines, etc., that are scheduled to be formulated in FY2008. A support system for promoting information security measures will be developed, particularly for small- and medium-sized enterprises, in cooperation with related organizations such as the IPA.

H) Development of a system to ensure the dependability of embedded systems, etc. (Ministry of Economy, Trade and Industry)

The ministry will conduct studies on matters that developers should take into consideration to ensure the dependability of embedded systems, etc. Efforts will also be made for capability improvement/system development to conduct analysis and safety assessment of tamper-resistant technology, etc. at related institutions, with respect to the safety of LSI chips and IC cards, which are the core of embedded systems.

I) Promoting the creation of a secure business environment in Asia (Ministry of Economy, Trade and Industry)

Based on the research results of FY2008, the ministry will conduct studies on the further promotional measures to create a secure business environment in Asia.

J) Strengthening of systems associated with anti-cyber-terrorism measures (National Police Agency)

In order to respond to advances in cyber terrorism methods, the systems associated with anti-cyber-terrorism measures of the National Police Agency will be enhanced and developed, such as strengthening the information collection/analysis system and improving the incident response capability/technological capability of anti-cyber-terrorism personnel by implementing in-house and external training programs. Moreover, enlightenment activities will be performed to raise awareness of anti-cyber-terrorism measures on an as-needed basis, while giving consideration to the characteristics of the operations of critical infrastructure operators. Efforts will also be made to contribute to emergency response activities in the event of cyber terrorism incidents by implementing joint exercises and participating in various types of drills, while respecting the intentions of critical infrastructure operators.

K) Strengthening of systems associated with anti-cyber–crime measures (National Police Agency)

In order to respond appropriately to cyber crimes, which are growing increasingly complicated and sophisticated, efforts will be made to enhance/develop systems and enhance measures concerning digital forensics. In addition, the following activities will be promoted: cyber crime control, nationwide in-house and external training programs for police officers engaged in investigating cyber crime, dissemination and PR activities in relation to damage prevention, studies on the state of the public-private partnership, etc. International coordination/cooperation will be enhanced by, for example, holding a conference on technology for investigating cyber crimes in the Asia-Pacific Region.

L) Study on coordinating the information-sharing schemes and information exchange models of specialty fields (Cabinet Secretariat, Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry)

Planning appropriate responses to cyber attacks and IT failure, which have become increasingly advanced recently, requires information collection/correlation analysis utilizing diverse expertise and cooperation measures, in accordance with the objectives/functions of different information-sharing schemes.

To that end, the competent agencies will organize the roles and coordination of information-sharing schemes in each field, such as the system design field, virus analysis field and CSRIT/ISP field, and examine information coordination and information exchange models (coordination structure design) that are in line with the individual objectives and functions.

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

In order to deal with the localization of cyber attacks, sophistication and concealment of attack methods, and expansion of systems (control system, etc.) that may become attack targets, the competent ministry will promote enhancement of the capability for analyzing technologies and methods used for attacks and make efforts to improve the system for sharing malware samples, detection information, vulnerability-related information, and analysis technologies/tools among related organizations in industry, government and academia both within and outside the country.

Efforts will also be made to develop an appropriate information processing environment through activities such as providing support for incident responses, providing information concerning secure development and investigation methods for products to developers of IT products/systems, conducting dissemination and PR activities for intranet administrators, IT users, etc., and developing technical measures in tune with the needs of the time.