Secure Japan 2009

- All Entities Should Assume
They May Be Subject to Accidents -

June 22, 2009
Information Security Policy Council

Table of Contents

Chapter 1: Measures and Assessment Based on the First National Strategy on Information Security (FY2006 - 2008)

Section 1: Assessment of the National Strategy and Previous Annual Strategies, and Their Relationships with This Plan

The “First National Strategy on Information Security” (called the “First National Strategy” hereinafter), established by the Information Security Policy Council on February 2, 2006 aiming at accomplishing a “Secure Japan” (“a nation with truly advanced information security”) completed its strategic term at the end of FY2008. Subsequently, the “Second National Strategy on Information Security” (called the “Second National Strategy”) was established by the Information Security Policy Council on February 3, 2009 to continue development of the previous strategy and activities from FY2009.

As the overview of the measures in the First National Strategy describes in chapter 1 of the Second National Strategy, the objective of the strategy was to launch Japanese information security policies and “promote awareness” for all organizations. In order to accomplish a “Secure Japan” as advocated by the strategy, an annual strategy “Secure Japan 200x” has been formulated since FY2006 to promote specific measures to develop an infrastructure for information security through stages such as “establishment of the system” -> “raising of standards” -> “intensive efforts.”

- In FY2006, the “establishment of a system for information security measures in the public and private sectors” was launched as the first step towards a “Secure Japan.” 133 specific measures and 26 measures to indicate the direction of priority measures for FY2007 were listed. Approximately 87% of the measures were implemented as initially planned, and the rest were estimated to be achievable in the mid- to long-term. Consequently, the first steps resulted in the following developments.
    1) Emerging Awareness of Information Security in the Respective Organizations
    2) Application of Specific Measures by Each Organization
    3) Establishment of Information Security Promotion Systems and a Sustainable Improvement Structure

- In FY2007, aiming at “raising the standard of information security measures in the public and private sectors”, efforts were focused on stabilizing the systems for promoting information security measures in the public and private sectors, such as maintaining the information security measure promotion systems and raising the

standard where measures were not sufficient. 159 specific measures and 24 measures to indicate the direction of priority measures for FY2008 were listed. Approximately 91% of the measures were implemented as initially planned, and the rest were estimated to be achievable in the mid- to long-term. Consequently, the following developments were achieved.

1) Maintained or reinforced awareness of information security in the respective organizations
2) Application of specific measures in each implementation field
3) Application of specific measures in cross-sectoral information security infrastructures
4) Promotion of policy enforcement based on maintenance and reinforcement of information security promotion systems, and sustainable improvement structure

- In FY2008, as preparation for “intensive efforts for enhancing information security infrastructure”, activities were focused on “information security human resource development and assignment”, “international collaboration in information security”, and “information security reinforcement of e-Government.” 157 specific measures and 21 measures to indicate the direction of priority measures for FY2009 were listed. Approximately 89% of the measures were implemented as initially planned, and the rest were estimated to be achievable in the mid- to long-term. The consequent achievement includes certain improvements, the prospect of sustainable activities, and the establishment of a common platform towards the four key policies defined in the First National Strategy: “development of common awareness in the public and private sectors”, “pursuit of state-of-the-art technologies”, “reinforcement of public responses”, and “promotion of partnership and cooperation.”

Following the First National Strategy, annual plans for specific measures will be developed and its implementation status will be assessed with consideration to changes in social circumstances and published during the course of the Second National Strategy. The result of the assessment will be reflected to the following annual plan as part of the annual PDCA cycle. An additional overall assessment of the First National Strategy (FY2006 - 2008) was also carried out in FY2008 as it was the final year of the First National Strategy and published by the National Information Security Center (called “NISC” hereinafter) on May 8, 2009 as the “Assessment of Information Security Policies in 2008.”

Secure Japan 2009 (called “SJ2009” hereinafter) is to set the direction for measures

based on these assessments, especially the assessment over three years of the First National Strategy.

Section 2: Measures and Assessment over Three Years of the First National Strategy (FY2006 - 2008)

The assessment of the First National Strategy was carried out by measuring the degree of achievement of the “social profile of Japan in 2009” (called the “2009 profile” hereinafter) drawn up in “The Best Forms of Japanese Society and Policy Assessment from the Perspective of Information Security” formulated in the 10th Information Security Policy Council on February 2, 2007.

(1) Assessment, Analysis, and Issues of Social Changes Caused by Implemented Measures

[1] Government Agencies and Local Governments

The following describes examples of the “2009 profile” and the degree of achievements.

- With regard to “establishment of the standards for measures and of the PDCA cycle through assessment and recommendations based on the standards”, government agencies' measures have become up-to-date and appropriate thanks to timely reviews of the standards and measures for information security (called “Standards for Measures” hereinafter). Also, the measure application status of basic items such as terminals, servers, etc. has significantly improved due to the progress in establishing the basic PDCA cycle through assessments and recommendations in government agencies.

- With regard to “launch of common activities among government agencies towards reinforcement of mid- to long-term security measures”, activities such as the study for implementing an e-Government and promotion of safe encryption deployment in government agencies have been launched.

- With regard to “strategic deployment and development of specialist human resources”, each government agency is taking measures as described in the

"Action Plans for Human Resource Development/Securement in IT" formulated based on the "Guidelines for Human Resource Development/Securement in IT at Administrative Agencies"[1]. Also the quality of the government's standard training programs were improved and the opportunities to participate in such programs expanded.

- With regard to "progress of information security measures in incorporated administrative agencies being almost in line with those of government agencies", development and review of information security policies based on the Standards for Measures is in progress.

- With regard to "measures against cyber attacks on government agencies", implementation and subsequent operations of the GSOC[2] reinforced the defense against cyber attacks across government agencies.

As a summary of the above statuses, the initial target indicated as the "2009 profile" is generally achieved though not perfect yet.

[2] Critical Infrastructure

The following objectives are proposed as the "2009 profile."

- Establishment of the "safety standards" to clarify the standard of information security measures in each field; subsequently all parties in charge of critical infrastructures must carry out a self assessment to verify if their own information security measures are sufficient.

- Establishment of a communication and information exchange system between public and private sectors. Implementation of a framework to share information concerning information security measures for critical infrastructures such as CEPTOARs[3] and CEPTOAR-Council[4] and establish information sharing, communications, and liaison systems for IT-malfunctions.

---

1 Formulated by the government agency chief information officer (CIO) conference on April 13, 2007.

2 Abbreviation for Government Security Operation Coordination team. The monitoring and immediate response team for government agency information security.

3 CEPTOAR: Capability for Engineering of Protection, Technical Operation, Analysis and Response

4 The private organization for voluntary information sharing formed by CEPTOARs.

- Clarification of possible threats to each critical infrastructure, analysis of mutual dependencies such as which critical infrastructures may be affected as a result of an IT-malfunction in a certain critical infrastructure, and establishment of measures with consideration to such mutual dependencies.

- Establishment of continuous efforts towards improvement in information security measures such as annual cross-sectoral exercise for a critical infrastructure failure in collaboration with public and private sector organizations on a specific scenario assumed based on possible disasters.

In order to achieve the “2009 profile”, four pillars to bear measures were identified in the “Action Plan on Information Security Measures for Critical Infrastructures” (called the “First Action Plan” hereinafter) formulated by the Information Security Policy Council on December 13, 2005, under close liaison between public and private sectors to reinforce information security measures for critical infrastructures. 38 specific measures have been taken in three years of the First Action Plan.

Application of these 38 specific measures had completed by the end of FY2008; therefore, it is considered that the basis of liaison among concerned organizations has been established, and the ground to foster awareness and mutual recognition of their contributions towards information security has been cultivated among all concerned parties.

On the other hand, spread of and dependency on IT is increasing even while such measures are being applied. Therefore, the groundwork for functional recovery in the event of an IT-malfunction is also important to protect the daily lives of citizens and socio-economic activities from serious disruption in addition to preventive measures. In other words, balanced pre-disaster measures and post-disaster measures should be in place. Consequently, appropriate reviews and spread of policies, safety standards, etc. will continue to be an issue for contributing towards steady improvement.

Also, the importance of sharing disaster information and the knowledge attained from experience in other business sectors and other business operators is being recognized. Determining how the concerned organizations can fulfill their expected roles including the efficient use of CEPTOARs and CEPTOAR-Council will become an issue in the future.

Resolving these issues will require thorough understanding of diverse

efforts by critical infrastructure operators and encourage mutual understanding between operators and sectors to foster smooth cooperation and mutual recognition among concerned organizations.

[3] Enterprises

There have been numerous measures taken to target “the global leader position of security measure implementation” as described in the “2009 profile.”

Enterprises have been conducting autonomous efforts to prevent loss of trust due to information security incidents and to protect confidential information which would affect their competitiveness since the number of “critical information leakage” incidents did not show any sign of decrease. Also, awareness of business continuity has increased and more enterprises are developing their BCP (business continuity plan).

The government has been supporting such business activities by developing and acknowledging various certification schemes and guidelines.

As a result of such efforts for information security improvement, the number of enterprises certified for information security management systems (ISMS), the ratio of enterprises which have developed information security policies, and the ratio of enterprises which have implemented technical measures are increasing. This suggests that efforts towards establishment of a PDCA cycle are in progress.

On the other hand, 40% of enterprises still consider the benefit of information security measures is limited only to information security improvement. Therefore, in order to raise the standard of information security, it is crucial to establish an environment where application of information security measures is valued and helps improve the enterprise's value and competitiveness in the market.

As a summary of the above statuses, while progress has been made in the application of information security measures in enterprises, especially in the establishment of the PDCA cycle, it is difficult to claim to have attained “the global leader position of security measure implementation” in all measures. While efforts to raise the standard of information security should continue, it is also necessary to consider how to encourage small and medium enterprises

which are having difficulty in applying measures due to shortage of resources, as shown by the measure application statuses by the scale of organizations.

[4] Individuals

The government and non-profit organizations have made efforts in active PR and dissemination activities targeted at individuals in order to achieve “reduction in people with concerns about using IT.”

In addition to such efforts, the numerous media reports on information leakage incidents including private information helped raise the awareness of information security on the individual level and improve the application status of information security measures.

On the other hand, more than 40% of individuals still have concerns in using IT because the number of information leakage incidents shows no sign of decrease, and individual's awareness of new threats is lagging. Further efforts to raise the standard of information security are required to achieve the target “reduction in people with concerns about using IT.”

There are difficult problems in achieving this target. It is hard to make individuals recognize new threats and more than 20% of individuals have not applied even the basic measures which have long been pointed out.

Also it must be examined if there are any efficient measures other than raising the standard of individual's awareness in order to achieve security while the diversity of Internet usage is expected to increase.

Besides more efficient PR and dissemination activities, it is necessary to develop services to prevent information security incidents without depending on individuals' awareness as well as means to achieve security in increasingly diverse Internet usage.

[5] Promotion of Information Security Technological Strategy

After three years of the First National Strategy, some areas show recognition of the importance of information security technology development and efforts to maintain the environment for it. Specifically, many technology development projects were undertaken to solve issues such as cyber attacks using bots, as well as R&D for the development of advanced information

security technology for detection, recovery, and prevention of route highjack and development of a safe environment using virtual machine technologies.

Meanwhile, management of organizations and personnel did not show satisfactory advancement. This issue must be addressed in the future. “Effective implementation system of research and technological development” and “grand challenge” type research and technological development, formulated in FY2007 require further progress.

New issues have also arisen due to social changes that surround information security as IT usage has expanded in the past three years. The following issues must be added as subjects of research and technological development.

- People's dependency on IT increases as the functionality of information devices and the diversity of network services rapidly expand. This is highly likely to result in significant expansion of the range of information security concerns.

- As the generation structure changes in an aging society, it becomes more important to design and develop services and products from the viewpoint of ease of use and mitigation of information security risks due to a user's mistakes and errors.

- The existing security measures are becoming insufficient while the speed of discovering new vulnerabilities and development of attack methods are increasing.

Therefore, three priorities, “prioritization and maintenance of diversity of information security technology development”, “promotion of 'grand challenge' type research and technological development”, and “system formulation and preparation of ground for efficient research and technological development systems” must be addressed in the future while keeping an eye on these new issues.

[6] Information Security Human Resource Development and Assignment

In three years of the First National Strategy, certain results were achieved in

the systematization of information security qualifications and training as stated in the “Expert Committee on Human Resources Development/Systematization of Qualifications” report, and policies were established concerning various types of information security human resources.

On the other hand, knowledge and skills in information security are not yet shared among the entire human resources who require such knowledge and skills including management and information system personnel. In addition, it has become clear that further efforts are required before the effect of information security human resource development becomes apparent and the social needs for such resources is fulfilled.

Meanwhile, some information security personnel voiced their concerns that they could not clearly visualize their career path. Therefore, measures are required to satisfy the needs of information security human resources themselves as well as to satisfy the demand from where such resources are needed.

[7] Promotion of International Partnership and Cooperation

Measures were applied to achieve the following targets in the three years of the First National Strategy.

- Regular information sharing and exchange concerning information security projects between concerned parties overseas

- Dissemination of the information security status and efforts in Japan to other nations through active information disclosure

- Various efforts for information security issues in Japan are regarded as a best practice model for other countries

When NISC was founded, the organization was unknown to the world and PR was not easy. However, thanks to active and continuous attendance at international meetings and PR efforts, its presence is more widely recognized and the frequency of information exchange has been significantly improved.

Specifically, the number of attendance at international meetings concerning information security strategies has been rapidly increasing every year and the

NISC has also been participating in a wide range of activities in Asia-Pacific, Oceania and other regions. As a result, regular information sharing and exchange with government agencies in these regions has been taking place.

Also, the information security status and efforts are sufficiently acknowledged by other nations through international meetings and other bilateral and regional activities. For example, the NISC is now receiving attendance requests for international meetings in European, American, and Asian regions, and collaboration requests for liaison reinforcement.

In order for Japanese information security strategies to be regarded as the best practice and deployed as a model in other countries, there has to be a mechanism in the given country to apply a model to their own practice, in addition to our continuous dissemination. The Cabinet Secretariat held the ASEAN Japan Information Security Policy Meeting in cooperation with the Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry in order to continuously and efficiently disseminate the best practice of information security in Japan and to prepare the environment from where both Japan and ASEAN countries can benefit. However, such activities are still at an early stage and an assessment of the strategy's effectiveness must be carried out on a mid- to long-term scale. Meanwhile attempts for standardization of strategies and creation of a best practice collection have been continuing through international organizations. How to effectively take advantage of such an opportunity requires further consideration.

As a summary of the above, targets set in the “2009 profile” have been mostly achieved except for some parts.

[8] Crime Control and Protection and Redemption of Rights and Interests

Throughout three years of the First National Strategy, continued activities for crime control and protection and redemption of rights and interests have achieved certain progress. On the other hand, IT itself and social circumstances of the users have been rapidly changing. As a result, in reality, the efforts are concentrated on establishing a foundation to control current cybercrimes and restrict the damage within a certain range, and are inevitably monotonous.

Also, careful consideration is required for legislation matters since it may

affect an individual's rights and interests. It will be inevitable to allow a certain period of time before reaching a conclusion through examination of the existing laws and analysis of the social circumstances.

(2) Summary

Overall, certain improvement has been achieved in subjective and objective confidence in the use of IT. For example, improved recognition of the importance of information security in organizations, progress in establishing the system for continuous assessment and improvement using the PDCA cycle, and definite progress in the application status of various measures. Also, efforts to implement a concrete model of the “ideal profile” of public and private sector cooperation were undertaken. This involved preparation of the framework and foundation for public and private sector cooperation for information security as part of establishing a safe IT environment. From now on, it is necessary to promote organizations' autonomous efforts and continuous improvement in order to further establish subjective and objective confidence in IT and a safe IT environment with awareness to changes in the surrounding environment based on the established framework and foundation.

The first remaining issue is to plan long term measures from the newly established framework and execute them. The second is to support organizations whose efforts fell short due to shortage of resources in every field, and the third is to continue applying measures at a rational level while flexibly dealing with environmental changes.

With regard to the first issue, continuous examination is necessary on fields which require actions in the new framework, and implement the determined actions as specific measures.

The second issue addresses organizations which are having difficulty in applying measures due to shortage of resources in addition to the lack of investment in information security due to the worsening economic situation. These organizations represent the major determiner of the overall standard of information security. Therefore, it is necessary to support organizations with insufficient resources in order to maintain information security standards in Japan.

With regard to the third issue, continuous efforts are required until social

effects appear. However, the efforts must be corrected or altered according to the social circumstances to avoid these activities become self serving or inertia. Also, these activities must be continued at a rational level.

Chapter 2: Basic Policies for Addressing Information Security in FY2009

Section 1: Directions in FY2009 to 2011

Three years of the Second National Strategy will continue efforts in the First National Strategy, reinforce measures where the efforts during the First National Strategy fell short, and take fresh actions according to the developed policies to reinforce resistance of the “Accidents Assumed Society” based on the assessment of the three years of the First National Strategy rather than the assessment of the FY2008 alone. Also, circumstantial changes which may have occurred after the development of the Second National Strategy, such as the current economic situation, must be taken into consideration. Efforts must aim at “establishment of strong 'individuals' and 'society'” where IT is truly managed in addition to building a “safe IT environment” with the above considerations to achieve the following objectives.

(1) Foundation to Reinforce Resistance of the “Accidents Assumed Society”

The focus of the Second National Strategy is to reinforce resistance of the “Accidents Assumed Society” with an assumption that disasters may occur, rather than the previous activities focused on preventative measures aiming at no accidents. Readiness to disasters must be one of the items which should be actively addressed from FY2009 with consideration to the fact that IT-malfunctions that may affect people's lives and socio-economic activities have already been occurring now and then.

(2) Rationally Proven Approach

The First National Strategy prioritized preparing the foundation of information security measures around government agencies and concentrated the activities on it. As a result, while it managed to implement the system, it failed to reach social agreement on how far each effort should be practiced. Therefore, issues on cost-effectiveness and durability of measures remained. For that reason, the three years of the Second National Strategy emphasizes on activities for implementing practical information security measures rather than measures that negatively affect convenience while trying to balance the costs and effect.

(3) Counteractions to the Current Economic Circumstances

In order to climb out of the current economic situation described as “once in a hundred years” or “three years for complete recovery”, strategies to make use of IT to propel economic growth have been announced following the formulation of the “New Strategy for the Digital Era: Three-Year Emergency Plan” by the Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society (called the “IT Strategic HQ” hereinafter) on April 9, 2009. These prove that IT is recognized as the foundation to support development of every area, and it is essential to take information security measures to make the IT environment safe for citizens. Even in the IT promotion by the emergency economic measures, information security measures must not be put off, but included without fail.

Section 2: Three-Year Action Flow - Growing Steps -

In order to achieve the target of the Second National Strategy, “establishment of strong 'individual' and 'society' in the IT age”, the first requirement is to reinforce the resistance of the “Accidents Assumed Society.” The targets of these three years' activities are to innovate the nation's awareness, promote activities in the society as a whole, make Japan a “matured and advanced nation in information security” where every organization is able to take consistent information security measures before and after an accident, and to maintain these statuses. Therefore, the “individuals” and “society” will grow stronger through the following processes.

Year 1 (FY2009): The time of “awareness.” Every organization will recognize this is an “Accidents Assumed Society” first, then start information security improvement activities based on this recognition. A review of the counteractions after an accident will be carried out using the systems and tools prepared in the three years of the First National Strategy.

Year 2 (FY2010): The time of “cooperation.” Every organization will examine their own activities and discuss the possibilities of liaison or task sharing with another organization with related activities; so that they can start working in cooperation to create an environment where the society takes consistent actions as a whole.

Year 3 (FY2011): The time of “maturity.” Every organization will take the necessary actions to fit into an “Accidents Assumed Society.” They will also concentrate on measures whose implementation has fallen behind to make use of the prepared information security foundation reasonably and efficiently, and finalize the three-year activities.

Section 3: Issues in FY2009 and Priorities of Information Security Policies

SJ2009 is the first annual plan based on the Second National Strategy, and it dictates priorities in Japanese information security policies in 2009 and 2010.

FY2009 focuses on planning and execution of various measures towards building an “Accidents Assumed Society” along the growth image described in section 2. Also, based on the direction indicated in section 1, the government will plan and implement various measures on a basic concept where every organization will be reminded of the need for rationality in information security measures, and inclusion without fail of the necessary information security measures even in an urgent IT investment.

(1) Formation of a Common Understanding among Public and Private Sectors on New Concepts

The government will form and establish a common understanding among public and private sectors on new concepts, such as an “Accidents Assumed Society” and a “rationally proven approach” to prepare the necessary environment for encouraging autonomous and lasting efforts. Especially for critical infrastructures, the common understanding among organizations should be formed urgently for how to maintain the services and how to swiftly recover from an IT-malfunction, since their stoppage, decline, or unavailability will greatly affect people's lives and socio-economic activities. Additional efforts include training and PR activities linked to human resource development and assignment, examination of the barometer and method of assessing information security measures, and establishment of a system for information sharing among various organizations.

(2) Promotion of e-Government

The emergency plan and various strategies for economic growth are expected to accelerate efforts concerning the e-Government, which aims to improve people’s

convenience, in all sections of the government. In order to make this e-Government useful and safe, information security measures must be embedded in an appropriate manner, specifically, information security measures must be considered from the planning and design stage of the information systems.

(3) Information Security Human Resource Development and Assignment

In order to steadily and continuously promote various policies, a human infrastructure will be prepared by developing and assigning human resources with knowledge and skills in information security and developing a system for implementing information security measures in an organization. Specifically, efforts will be made to enrich training programs and PR activities concerning information security for various types of organizations, review and promote the information security qualification system through “visualization of skills”, and develop human resources to support unskilled users and raise the standard of information security measures.

(4) Promotion of International Liaison and Cooperation

A safe and secure information security infrastructure should be prepared to support Japanese enterprises' economic activities across the border. Also, accelerate international liaison and cooperation concerning information security to improve continuity of a society with increasing IT dependency by taking efficient countermeasures in the event of a cross border IT-malfunction. With regard to the economical aspect, public and private sector cooperation and international liaison should be established and specific measures should be mutually agreed especially in the Asian region where many Japanese enterprises have extended their business. Also, with regard to social continuity, reinforce the liaison through active dissemination of Japanese efforts in international meetings concerning critical information infrastructure protection policies and security policies. In addition, as a cross-sectoral activity, actively apply international best practice to help Japanese information security policies reach the global top level.

(5) Promotion of Information Security Technological Strategy

A technological strategy should be actively promoted by ensuring progress in mid- to long-term R&D such as the “grand challenge” type R&D in order to contribute the truly required information security technology towards building a “secure IT environment.” Specifically, based on the understanding that technological development is the true strength of Japan, actively recognize the needs, propel the establishment and review of the framework for connecting the

needs with the specific operations for implementation and avoid such technological R&D activities being left as a formality.

Chapter 3: Important Policies for the FY2009[5]

The Second National Strategy inherits the framework of the First National Strategy which classifies organizations subject to information security measures into four areas; government agencies and local governments, critical infrastructure, enterprises, and individuals. SJ2009 also dictates specific policies according to the characteristics of these four areas.

In order to promote formation of the common understanding among organizations on the degree of risks where information security measures are required and their objectives, and to maintain continuous and rigid information security efforts by public and private sectors, it is necessary to take appropriate actions in each area and to build a foundation which serves society as a whole. Therefore, the government is required to comprehensively address the following measures with clear mid- to long-term strategies, from the perspectives of promotion of information security strategies, development and assignment of information security human resources, promotion of international liaison and cooperation, crime control, and protection and redemption of rights and interests.

Section 1: Promotion of Measures in the Four Areas and Objectives of the Policy

(1) Four Areas Subject to Measures

[1] Government Agencies and Local Governments

[Government agencies]

The government will prioritize the following policies in the FY2009 in order to maintain the Standard for Measures determined during the First National Strategy and the assessment and recommendation framework based on the Standard for Measures while implementing information security measures which can be a model for domestic and overseas organizations, and to achieve the necessary information security level for running the administration safe and securely as well as providing services worthy of citizens' confidence.

[5] With regard to the approach to information providers (organization to whom information such as individuals' private information is entrusted), the Second National Strategy takes closely related sections from the existing policy structures (four areas and four cross-sectoral fields subject to measures) of the First National Strategy for convenience.

(a) Establishment of a System for Active Information Security Efforts in Every Government Agency

1) Reinforcement of Management in Each Process of the PDCA Cycle

Each government agency will establish a system which is able to responsibly conduct information security efforts in the given organization in order to establish an information security governance. The system will be placed directly under the chief information security officer and in the information system project management office (PMO) or an equivalent department. Also, assign a chief information security adviser with specialist knowledge to assist the chief information security officer with required staff members, and establish a system to reflect the specialist instructions and advice swiftly and definitely to the entire organization.

In order to clarify their explanatory responsibility concerning information security measures to win citizens' confidence to the administration, government agencies will develop an "Information Security Annual Report" (Information Security Report) which describes their concept of information security, objectives, plans, their results and assessment concerning information security measures, and an assessment on whether the PDCA cycle is effectively functioning in the given agency using objective indicators such as numerical representation. This task will involve the chief information security adviser to maintain objectivity of the information security report. Also, actively take advantage of external audit systems where possible. The prepared information security report will be published and disclosed on occasions such as the "Information Security Measures Promotion Council" established under the Information Security Policy Council.

A guideline for creating information security reports will be developed to ensure the balance of measures in each government agency, as well as further improvement. The information security report will also be quantitatively assessed and the result will be reported to the Information Security Policy Council. In addition, a council will be established for chief information security advisers of each government agency to compare and assess the information security reports, share the knowledge and experience, and to exchange feedback.

The Standards for Measures will be reviewed annually to reflect technological and environmental changes and maintain information security measures in government agencies up-to-date and appropriate.

As for information security measures concerning systems which handle confidential information (classified management information) held in government agencies, the government agencies will be responsible for applying measures based on the standard concerning classified management information dictated in the "Basic Policy Concerning the Enhancement of the Counter Intelligence Functions"[6] while following the PDCA cycle based on the Standards for Measures. The Counter Intelligence Center will take the initiative in establishing a multi-layered check mechanism for the implementation status in collaboration with the Cabinet Secretariat and concerned government agencies.

[Specific Measures]

A) Establishment of the Information Security Governance (All Government Agencies)

a) Each government agency will develop policies to prepare a system where information security measures are conducted responsibly in the given agency under the chief information security officer.

6 Determined by the Counter Intelligence Promotion Council on August 9, 2007.

b) Each government agency will assign a chief information security adviser with specialist knowledge to assist the chief information security officer, and secure staff members as necessary.

B) Establishment and Spread of the PDCA Cycle

a) Establishment and Spread of the PDCA Cycle at Each Government Agency (All Government Agencies)

Each government agency will thoroughly establish and spread the PDCA cycle in the entire organization to improve its own measures based on the result of the self-assessment and audit on its information security efforts.

b) Establishment and Spread of the PDCA Cycle in the Entire Government (Cabinet Secretariat and All Government Agencies)

The Cabinet Secretariat will objectively assess and compare the progress of activities at government agencies through measure implementation status reports and point audits on critical items based on the Standards for Measures, make recommendations to improve the measures taken at government agencies and the Standards for Measures, and also ensure the establishment and spread of the PDCA cycle in the entire government by preparing an environment for the required system at government agencies.

The implementation of routine assessments will, in principle, be executed based on a predetermined schedule and inspection items presented to each government agency by the Cabinet Secretariat taking the workload of each government agency into consideration, except for urgent cases.

The result of assessments will be published to promote effective measures within the government, fulfill explanatory obligation to the citizens, and to maintain information security.

c) Development of Guidelines for Information Security Reports (Cabinet Secretariat and All Government Agencies)

The Cabinet Secretariat will develop a guideline for creating information security reports for government agencies and study a method for a quantitative assessment of information security reports submitted by government agencies.

Also where possible, government agencies will create a trial version of the information security report and disclose on an occasion such as the Information Security Measure Promotion Meeting.

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

Based on the changes in the technology and environment, the Standards for Measures will also be reviewed in FY2009.

E) Support for Efforts based on the Standard for Measures and Promotion of Effective Operations

a) Distribution of Information Security Related Information (Cabinet Secretariat)

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

b) Efforts to Solve Common Issues among Government Agencies on Information Security Measures (Cabinet Secretariat and All Government Agencies)

The Cabinet Secretariat will continue to address common operational issues in information security measures and provide opportunities to examine and share the measures in collaboration with government agencies.

c) More Efficient Self-assessments and Audits at Government Agencies (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 operational efficiency associated with training, self-assessments and audits, and present the result of the study to each government agency.

d) Centralized Management of Information Systems at Government Agencies (Cabinet Secretariat, Ministry of Internal Affairs and Communications and All Government Agencies)

In order for each government agency to understand and implement the information security measures required for the information systems, each government agency will record the information handled by each information system and items subject to information security measures including the classification of the given information in the information asset registry compiled by each government agency.

F) Response to Information Leakage Caused by Computer Viruses and the Like (All Government Agencies)

In order to prevent information leakage caused by viruses and the like that infect computers via file-sharing software and so forth, each government agency must implement strict information management continuously in FY2009 based on the Standards for Measures to control take-out of internal information and the use of private computers for office work.

G) Ensuring Information Security Standards at Contractors

a) Use of the Conformity Assessment Scheme for Information Security Management System (Cabinet Secretariat and All Government Agencies)

In order to verify information security standards of outsourcing candidate contractors continuously in FY2009, the information security management conformity assessment system and information security benchmark will be used where necessary as part of the selection process in government procurement.

b) Use of Information Security Audit System (Cabinet Secretariat and All Government Agencies)

In order to appropriately assess and verify information security standards of contractors, an information security auditing system based on management standards compliant with international standards, will be used continuously in FY2009 where necessary.

c) Deployment and Establishment of the “Guidelines for Improving Reliability of Information Systems” (Cabinet Secretariat and Ministry of Economy, Trade and Industry)

The government will promote the deployment and establishment of the “Guidelines for Improving Reliability of Information Systems Second Version” which dictates the method to improve reliability of all information systems from all aspects such as process management including development and operation, technology and organization. The document has been enhanced in FY2009 with articles on IT governance and operations.

H) Development and Distribution of a Verification Tool for PDCA Cycles (Ministry of Economy, Trade and Industry)

The government will support verification of information security PDCA cycles applied for information systems at government agencies in FY2009. For example, the Information-Technology Promotion Agency (called the “IPA” hereinafter) will launch development of a tool which supports verification of security requirements on information system component devices. The tool is scheduled to

be distributed in FY2010.

I) Information Security Measures for Systems Handling Specially Controlled Secrets (Cabinet Secretariat and Concerned Government Agencies)

The Cabinet Secretariat will work on establishing a multi-layered checking system to review the state of implementation of the handling standard of Specially Controlled Secrets provided in the Counterintelligence Policy in collaboration with government agencies concerned and reach agreement on the general outline.

2) Human Resource Development and Assignment in Government Agencies and Raising of Personnel Awareness

The government will examine and verify information security related tasks in government agencies and summarize the skills required for the personnel involved in these tasks.

Based on the identified skills, each government agency will create specific plans for training and assignment of internal human resources involved in information security measures to compile the "Guidelines for Human Resource Development/Securement in IT" in accordance with the "Guidelines for Human Resource Development/Securement in IT at Administrative Agencies."

Also, each government agency will actively employ private sector security specialists in strategic outsourcing to secure the chief information security adviser and support staff by making use of systems such as fixed-term contract.

Each government agency will promote awareness of information security for all officials including management in collaboration with the Personnel and Information System Departments such as including information security in staff training as well as promoting public and private sectors personnel exchange system.

[Specific Measures]

A) Enhancement of Training Programs for Government Officials (Cabinet Secretariat and Ministry of Internal Affairs and Communications)

The Cabinet Secretariat and the Ministry of Internal Affairs and Communications will improve the quality of the government's standard training programs for government officials (general staff, management, and staff in charge of information security measures).

B) Examination of Information Security Related Tasks (Cabinet Secretariat)

The Cabinet Secretariat will examine and verify information security related tasks in government agencies and summarize the skills required for the human resources involved in these tasks.

C) Execution of the Guidelines for Human Resource Development/Securement in

IT (Cabinet Secretariat, Ministry of Internal Affairs and Communications, and All Government Agencies)

In order to develop and assign human resources with knowledge and capability including information security to contribute towards the safe and secure use of information systems, each government agency will take actions as described in the "Guidelines for Human Resource Development/Securement in IT" formulated based on the "Guidelines for Human Resource Development/Securement in IT at Administrative Agencies."

D) Employment of Private Sector Specialists (All Government Agencies)

Each government agency will actively employ private sector security specialists in strategic outsourcing to secure the chief information security adviser and support staff by making use of systems such as fixed-term contract.

E) Human Resource Development for Government Officials (All Government Agencies)

Each government agency will promote awareness of information security for all officials including management in collaboration with the Personnel and Information System Departments such as by including information security in staff training as well as promoting public and private sectors personnel exchange system.

3) Budgeting for Timely Information Security Measures

Since information security measures must be applied in a timely manner, each government agency will have to make the best possible prediction and draw up maintenance contracts which allow appropriate measures to be applied at an appropriate time. They should effort to use the budget efficiently in collaboration with the Account and Information Systems Departments, as well as to consider taking advantage of the "result-oriented"[7] approach.

[Specific Measures]

A) Budgeting Approach (All Government Agencies)

Each government agency will make the best possible prediction on information security measures, prepare for the measures, and draw up maintenance contracts which will allow appropriate measures to be applied at an appropriate time. In such a case, they should consider the "result-oriented" approach to focus on the definite result, and work in collaboration with the Accounting and Information Systems Departments to complete the process without delay.

[7] An approach to clarify the position, set a quantitative target, and carry out a post-project assessment in order to effectively use the limited financial resources. In the case of budgeting, the approach is focused on the successful project result such as by adding flexibility according to the characteristics of the project.

4) Reinforcement of Information Security Measures for Information Systems under Outsourced Operations or Management

With regard to information systems whose operations or management is outsourced to an external organization, each government agency must ensure that these external organizations comply with the government agency's information security policy by exchanging appropriate contracts based on the Standards for Measures, and verify if the systems are operated properly.

[Specific Measures]

A) Reinforcement of Information Security Measures for Information Systems under Outsourced Operations or Management (All Government Agencies)

Each government agency will ensure the security of information systems whose operations or management is outsourced to an external organization in accordance with the Standards for Measures ("1.2.5.1 Outsourcing" in the version 4).

5) Implementation of a Mechanism to Accumulate and Apply Technical Knowledge

In order to take advantage of technical and specialist knowledge and experiences in information security, the government will implement a mechanism to make collective use of the knowledge and experiences of researchers and practitioners in associated incorporated administrative agencies and information security related organizations.

[Specific Measures]

A) Reinforcement of Liaison with Information Security Related Incorporated Administrative Agencies (Cabinet Secretariat, Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

The Cabinet Secretariat will reinforce liaison with incorporated administrative agencies such as the National Institute of Information and Communications Technology (NICT), National Institute of Advanced Industrial Science and Technology (AIST), and IPA as well as information security related organizations by holding periodical communication meetings in order to accumulate and make use of the knowledge and experiences of their researchers and practitioners.

6) Consistency with the Laws and Regulations Concerning the Information Security

The government will carry out the necessary adjustments to maintain consistency between information security related laws and regulations including the document management legislation currently under consideration, and the Standards for Measures.

[Specific Measures]

A) Consistency with the Laws and Regulations Concerning the Information Security (Cabinet Secretariat)

The Cabinet Secretariat will carry out the necessary adjustment to maintain consistency between information security related laws and regulations, and the Standards for Measures.

(b) Establishment of a Mechanism to Appropriately Integrate Information Security Measures into Information Systems in the Entire Government

When various information systems are implemented in government agencies, total costs should be controlled, and convenience and flexibility should be achieved, as well as various requirements such as information security should be fulfilled. Therefore, the government should implement a combined approach with consideration to integration of information security measures in the planning and design phase (Security by Design) and optimization of business and systems in addition to implementation and operation of the information system. In such a case, a method to promote reduction of TCO (Total Cost of Ownership: Total costs for implementation, maintenance, and management of a system) for the entire government should be studied.

Also, various information to determine the necessary information security measures should be presented and referenced at procurement of information systems and materials.

[Specific Measures]

A) Method to Integrate Information Security Measures in the Planning and Design Phase (Cabinet Secretariat, Ministry of Internal Affairs and Communications, and Concerned Government Agencies)

With regard to integration of information security measures in the planning and design phase (Security by Design), the government will study the form of cooperation between supplier and purchaser, as well as the method for developing and assuring an information system with consideration to security based on the Standards for Measures in FY2009.

B) Reinforcement of Liaison between the Cabinet Secretariat and Government Agency Deputy Chief Information Officers (CIO) (Cabinet Secretariat and Ministry of Internal Affairs and Communications)

The Cabinet Secretariat, Deputy CIOs, and chief information security advisers will continue to liaise for ensuring security in information systems in government agencies in FY2009.

C) Utilization of Highly Safe and Reliable IT Products (Cabinet Secretariat and All Government Agencies)

The government will continue to prioritize products approved by Japan

Information Technology Security Evaluation and Certification Scheme (JISEC)[8] as dictated in the Standards for Measures when procuring IT products in order to implement highly safe and reliable information systems in FY2009.

D) Support for System Selection and Procurement with Consideration to Information Security (Cabinet Secretariat and Ministry of Economy, Trade and Industry)

In order to assist government agencies in practical and efficient procurement of IT systems, the IPA will continue to examine products which are certified by an IT security assessment or a certification system, and promote the use of them in government agencies.

E) Clarification of the Applicable Range of Third Party Certificate System at Procurement of Information Systems (Cabinet Secretariat and Ministry of Economy, Trade and Industry)

In order to improve information security at procurement of information systems for the government, the government will clarify cases where “critical security requirements” are specified as one of the procurement criteria which dictates whether or not the system should be certified by an “IT Security Assessment and Certificate System” or “Encryption Module Test and Certification System” as described in the Standards for Measures. The government will also reflect the results to the measures to be taken by government agencies in FY2009.

F) Assessment and Improvement of Next Generation OS Environments to Achieve Advanced Security Functions (Cabinet Secretariat, Cabinet Office, Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

The development of “Secure VM” prototype was completed in FY2008. The government will carry out a trial in the Cabinet Secretariat and a proving test on the assumption of its use in government agencies to summarize issues in actual operation. Also, the government will effort to improve performance and expand the deployment environment of Secure VM through cooperation among industry, academia and government.

[8] "Japan Information Technology Security Evaluation and Certification Scheme" (JISEC) is a system where security functions and the targeted security assurance level of IT products and systems are assessed by a third party based on the international standards ISO/IEC 15408, the results are officially verified and publicized in principle.

(c) Improvement of Convenience and Security Level of e-Government

In order to improve the convenience of administrative services, efficiency of administrative operations and the security level, the government will study the form of system security for e-Government. The study will include the implementation method of the user interface which should provide improved convenience and security for the users, and should also be cost-effective.

[Specific Measures]

A) Convenience of e-Government and Improvement of the Security Level (Cabinet Secretariat, Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

The government will examine the strategy including implementation of e-Government in order to improve the convenience of administrative services, efficiency of administrative operations, and the security level, with consideration to the discussions in the Study Committee for the Creation of e-Government Guidelines in FY2009.

B) Development and Use of the Electronic Authentication Guidelines (Cabinet Secretariat, Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

In order to present requirements and regulations for electronic authentication systems in government agencies, the government will continue to study the rough plan for the “Electronic Authentication Guidelines” (provisional name) before its development.

(d) Reinforcement of Business Continuity and Emergency Response in Government Agencies

Currently government agencies' business continuity plan assumes metropolitan earthquakes based on the “Policy Framework for Tokyo Metropolitan Earthquakes” compiled by the Central Disaster Prevention Council in September 2005. However, continuity must also be secured in the event of other disasters and malfunctions. Government agencies will decide on the necessity and priority of measures in the event of information system disasters and malfunctions, and develop the business continuity plan for required items. Also, government agencies will study the backup system for critical systems at government agencies and the information on them with a governmental cross-sectoral approach.

In order to reinforce emergency response and recovery, the GSOC which started its full scale operations in FY2008 will take initiative to form a close liaison with government agencies and concerned organizations in Japan and overseas. Establishing an emergency communication system and strengthening analysis and measure planning functions against attacks will improve the entire government's emergency response and recovery capability against cyber attacks as well as strengthen the Japanese security.

[Specific Measures]

A) Development of Business Continuity Plan (All Government Agencies)

Each government agency will study the necessity and priority of response in the event of an IT system disaster or malfunction, and develop a business continuity plan for necessary items in order to ensure continuity of the services.

B) Investigation of the Current Status of Backup for Critical Systems and Information (Cabinet Secretariat and Ministry of Internal Affairs and Communications)

The Cabinet Secretariat and the Ministry of Internal Affairs and Communications will investigate the current status of the backup system for critical systems and information in government agencies and study a governmental cross-sectoral approach.

C) Reinforcement of Cross-Sectoral Problem Solving Functions against Cyber Attacks in Government Agencies

a) Reinforcement of the GSOC's Analysis Capability (Cabinet Secretariat and All Government Agencies)

The GSOC, which started its full scale operations in FY2008, will reinforce liaison with concerned organizations to improve its analysis capability on cyber attacks against government agencies.

b) Research and Study of the Latest Technological Trend Concerning Information Assurance (Ministry of Defense)

The government will continue its efforts in FY2008 to investigate the latest technological trend in cyber attacks as well as defense against cyber attacks, and study a centralized defense system for assuring information on information systems.

D) Reinforcement of Emergency Response and Recovery Capability of Government Agencies

a) Reinforcement of Emergency Response and Recovery Capability of Government Agencies (Cabinet Secretariat)

Based on the operational status of the GSOC which started its full operations, the government will continue its efforts in FY2008 to analyze general trends and circumstances of cyber attacks. The government will periodically provide the analysis results to government agencies and will also provide the analysis results of the attack method which are required for individual measures whenever appropriate.

b) Study of Analysis and Response to Cyber Attacks (Ministry of Defense)

In order to further enhance analysis and response capability against cyber attacks on information systems of the Ministry of Defense, the government will study and create a trial product of a network security analysis device and continue its efforts in FY2008 to study the basics of illegal access monitoring and analysis technology, cyber attack analysis technology, and active defense technology.

E) Reinforcement of Measures against Cyber Terrorism (National Police Agency and Ministry of Justice)

The government will prepare a system to catch an early warning of terrorism in the cyber space, strengthen international liaison for information exchange, and make continuous efforts to collect and analyze information concerning attackers and methods in order to reinforce measures against cyber terrorism[9].

(e) Promotion of Information Security Measures for Incorporated Administrative Agencies

In order to promote information security measures in incorporated administrative agencies, government agencies supervising incorporated administrative agencies will explicitly include items concerning information security measures in the mid-term objectives and establish a system where the incorporated administrative agencies systematically apply the information security measures. Each incorporated administrative agency will establish a PDCA cycle for its own information security measures based on a series of measures taken by government agencies including the Standards for Measures, according to its operation characteristics and measure application status. Government agencies supervising incorporated administrative agencies will establish an effective communication system available even in an emergency situation.

[Specific Measures]

A) Development of Information Security Policies in Incorporated Administrative Agencies (Cabinet Secretariat and Government Agencies Supervising Incorporated Administrative Agencies)

Each government agency will request the incorporated administrative agencies under its jurisdiction to develop and review latter's information security policies with reference to the Standards for Measures, and will provide necessary support.

B) Preparation of an Environment for Improvement of Information Security Measures in Incorporated Administrative Agencies (Cabinet Secretariat)

The government will prepare an environment to improve information security

[9] An electronic attack on the backbone system of a critical infrastructure, or a serious failure of the backbone system of a critical infrastructure that is likely to have been caused by an electronic attack.

measures such as providing information necessary to develop and review information security policies in incorporated administrative agencies.

C) Inclusion of Information Security Measures in the Mid-term Objectives (Government Agencies Supervising Incorporated Administrative Agencies)

Each government agency will explicitly include items concerning information security measures in its mid-term objectives in order to promote information security measures in incorporated administrative agencies under its jurisdiction.

D) Implementation of the PDCA Cycle in Incorporated Administrative Agencies (Government Agencies Supervising Incorporated Administrative Agencies)

Each government agency will support the independent administrative agencies under its jurisdiction to establish a PDCA cycle for their own information security measures based on a series of measures taken by government agencies including the Standards for Measures, according to their operation characteristics and measure application status.

E) Preparation of an Emergency Communication System (Cabinet Secretariat and Government Agencies Supervising Incorporated Administrative Agencies)

Each government agency will prepare an effective communication system available even in an emergency situation with the incorporated administrative agencies under its jurisdiction, and verify its effectiveness.

(f) Promotion of Other Individual Information Measures

1) Support for IPv6 in the Government Agencies' Information Systems

In order to take initiative in the countermeasures for IPv4 exhaustion, the government will systematically take measures for supporting IPv6 at a development (implementation) or update of information systems. Support for IPv6 in information systems with direct communication with the outside such as the e-Government is planned to be implemented by FY2010 in principle. The government will address security issues in the transition from IPv4 to IPv6 appropriately.

[Specific Measures]

A) Support for IPv6 in e-Government Systems (Cabinet Secretariat, Ministry of Internal Affairs and Communications and All Government Agencies)

The use of IPv6 in e-Government is beneficial in security reinforcement such as prevention of illegal use of e-Government services and information leakage, interactive communications, and implementation of inter-government agency systems. Also, since IPv4 addresses are expected to exhaust in 2010 at the earliest,

the government will continue to take initiative and implement support for IPv6 in information communication devices and software at the time of development (implementation) or update of information systems. The government will also address security issues in the transition from IPv4 to IPv6. The following measures will be taken for smooth implementation.

a) Each government agency will continue to advance support for IPv6 in information systems according to the "Program for Promoting e-Government", partly revised by the Conference for Chief Information Officers (CIO) on December 25, 2008, and by referring to "the guideline for the introduction of IPv6 network in e-government systems" formulated by the Ministry of Internal Affairs and Communications on March 30, 2007.

b) In order for the general public to access services such as e-applications using IPv6, Internet service providers must also provide IPv6 connection services to individual users. The Ministry of Internal Affairs and Communications will continue to publish information on the availability of IPv6 connection services by the Internet service providers on its website.

2) Prevention of Government Agency Spoofing

Malicious third parties must be prevented from spoofing government agencies or their staff and causing damage to the public at large and private sectors. The government will take actions such as the use of domain names which guarantee government legitimacy on mail servers and web servers, and deployment of the electronic certificate by adding an electronic signature on e-mails transmitted from government agencies.

[Specific Measures]

A) Prevention of Spoofing Concerning E-mails Transmitted from Government Agencies (Cabinet Secretariat, Ministry of Internal Affairs and Communications, and All Government Agencies)

The government will deploy the sender domain authentication technology such as SPF (Sender Policy Framework) to prevent malicious third parties from spoofing government agencies or their staff and causing damage to the public at large and private sectors.

B) Use of Domain Names which Guarantee Government Legitimacy (Ministry of Internal Affairs and Communications and All Government Agencies)

Government agencies will continue to use domain names which guarantee government legitimacy ("go.jp" domain names in organizational type JP domain names, and domain names reserved for administrative use among JP domain names for general use) when transmitting information to the public in principle

and widely inform these measures to the public.

3) Promotion of Safe Encryption for Government Agencies

In order to ensure safety and reliability of the e-government, the government will continuously monitor and investigate safety of the encryption currently in use among government agencies. Also, the concerned organizations will carry out necessary tasks for revising the "e-Government Recommended Ciphers List" in FY2013 with consideration to technological trends and international efforts. In addition, based on the experiences gained through the development of the "Migration Plan of Cryptographic Algorithm SHA-1 and RSA1024 in Information Systems of Government Agencies"[10], the government will promote swift migration to a safe encryption algorithm from that whose safety level has been jeopardized.

[Specific Measures]

A) Promotion of Safe Encryption for Government Agencies (Cabinet Secretariat, Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry, and All Government Agencies)

a) The Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry will monitor, investigate, and study the safety and reliability of the recommended encryption for the e-Government, and create the standards in FY2009.

b) The Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry will also make preparations for revising the "e-Government Recommended Ciphers List."

c) The Cabinet Secretariat, Ministry of Internal Affairs and Communications, and all government agencies will promote efforts in accordance with the "Migration Plan of Cryptographic Algorithm SHA-1 and RSA1024 in Information Systems of Government Agencies." Also, based on the experiences gained through the development of the "Migration Plan of Cryptographic Algorithm SHA-1 and RSA1024 in Information Systems of Government Agencies", the cabinet secretariat will promote swift migration to a safe encryption algorithm from that whose safety level has been jeopardized.

B) Promotion of Safer and More Reliable Encryption Modules (Cabinet Secretariat, Ministry of Economy, Trade and Industry and All Government Agencies)

In order to promote the use of safer encryption modules, the government will practice the "Encryption Module Test and Certification System" formulated by the IPA and prioritize products certified by this system when procuring an

[10] Formulated by the Information Security Policy Council on April 22, 2008.

encryption module where necessary.

[Local Governments]

Each local government will aim at applying the desired information security measures over a wide administrative area. The government will promote the following prioritized measures.

(a) Promotion of Rational and Autonomous Information Security Measures in Local Governments Including Small Local Governments

The government will promote the application of desired information security measures in all local governments including small local governments. Specifically, the government will promote the risk analysis of information assets which are subject to measures and audit, examination of information security policy development, review of guidelines in preparation for an audit, and spread of the guidelines to contribute towards development of a business continuity plan[11]. With regard to human resources, a joint workshop and local seminars should be organized to improve ability of the staff that is in charge of these measures.

[Specific Measures]

A) Dissemination and Enlightenment for the Improvement of Information Security Level in Local Governments (Ministry of Internal Affairs and Communications)

In order to promote development of a business continuity plan for the information department, establishment of an information asset registry, and risk analysis activities in local governments, the government will hold information security seminars at several locations in Japan and encourage the practice of the “Guidelines for Risk Analysis and Assessment of Information Security Assets in Local Governments.”

The government will also review guidelines for information security policies, and send a business continuity plan development adviser from the ICT department to interested local governments.

[11] "Guidelines for ICT Business Continuity Plan (BCP) of Local Governments" formulated by the Ministry of Internal Affairs and Communications in August 2008.

(b) Support for Liaison between Local Governments for Application of Information Security Measures

With consideration to the limited resources available to invest in information security measures at local governments, the government will support liaisons between multiple local governments for efficient application of measures. Objectives of the support are introduction of the best practice to local governments and creation of a model case. Also, the government will hold workshops and study groups to improve awareness and understanding among the management of local governments, and consider sending of an adviser for approaches such as mutual audit.

[Specific Measures]

A) Dissemination and Enlightenment for the Improvement of Information Security Level in Local Governments (Ministry of Internal Affairs and Communications)

The government will invite the best practice and model case of information security among multiple organizations.

Also, the government will support the sending of an internal audit adviser to promote mutual audit.

(c) Strengthening of Organizations Assisting Local Governments in the Application of Measures

In order to promote application of measures, it is effective to strengthen organizations that assist local governments in their efforts. Therefore, while developing a cooperation system with every organization in possession of knowledge concerning information security by offering joint workshops for public and private sectors and NPOs, the government will reinforce the support system for autonomous organizations using a portal web site inside the LGWAN (Local Government Wide Area Network).

[Specific Measures]

A) Dissemination and Enlightenment for the Improvement of Information Security Level in Local Governments (Ministry of Internal Affairs and Communications)

The government will support operations by publishing explanations on information security in a portal web site inside the LGWAN (Local Government Wide Area Network).

(d) Promotion of Measures over a Wide Administrative Area of Local Governments

The government will promote application of information security measures over a wide administrative area of local governments with consideration to individual relationships between organizations under the national administration and local governments. For instance, when implementing an IT infrastructure at schools, the government may encourage application of information security measures, communicate effective measures through the municipal educational board, and improve awareness of the municipal educational board by

introducing the best practice.

[Specific Measures]

A) Dissemination and Enlightenment for the Improvement of Information Security Level in Local Governments (Cabinet Secretariat, Ministry of Internal Affairs and Communications, and Ministry of Education, Culture, Sports, Science and Technology)

The government will liaise first with the Ministry of Internal Affairs and Communications, and concerned government agencies since the number of information security incidents is relatively high in educational sectors. The government will analyze the existing information security measures and application status, and set specific measures for the future. Also, the government will disseminate and enlighten approaches to information security in meetings of local autonomous bodies' staff in charge of information education.

(e) Promotion of Best Practice Sharing among Local Governments and between Local Governments and Government Agencies

In order to promote the application of information security measures among approximately 1,800 local governments, it is effective to share the best practice among them. Therefore, the government will promote information sharing among local governments using a portal site inside the LGWAN (Local Government Wide Area Network). Also, the government will hold review meetings and discussions to provide opportunities for various levels from management to field engineers in local governments to share the best practice.

The government will also consider the method of sharing the best practice between local governments and government agencies since it will be equally effective.

[Specific Measures]

A) Dissemination and Enlightenment for the Improvement of Information Security Level in Local Governments (Ministry of Internal Affairs and Communications)

The government will promote the use of the portal site inside the LGWAN (Local Government Wide Area Network) by inviting the best practice of information security and enrich the site with many information security incident articles.

(f) Support for Training of Local Governments' Information Security Personnel

Since promotion activities by the local government are effective in human resource development of local information security personnel, the government will develop an environment to support local governments. Specifically, the government will create and provide references which can be used in seminars to encourage local governments to hold educational seminars on information security. Also, the government will promote training of tutors to further endorse human resource development.

[Specific Measures]

A) Enrichment of Information Security Training for Local Government Employees (Ministry of Internal Affairs and Communications)

The government will enrich the e-Learning contents to enable all local government employees to learn without restrictions of time and location.

[2] Critical Infrastructure

The concerned organization related to the information security measures for critical infrastructure will aim at preventing IT-malfunctions from severely affecting people's lives and socio-economic activities in accordance with the “Second Action Plan on Information Security Measures for Critical Infrastructure” (called the “Second Action Plan” hereinafter) formulated by the Information Security Policy Council on February 3, 2009. They should take appropriate action according to their roles to maintain critical infrastructure services and ensure a swift recovery from IT-malfunction. The following measures are prioritized in FY2009.

(a) Preparation and spread of the “Safety Standards”

The government will review the positioning of the policy and clarity of the contents of the policy formulated in the First Action Plan including supplementary contents concerning business continuity. While promoting efforts that will contribute to the improvement of the safety standards with consideration to maintaining consistency with the PDCA cycle of the critical infrastructure providers, the government will also make efforts to encourage and spread advanced individual measures.

[Specific Measures]

A) Continuous Improvement of Policies (Cabinet Secretariat)

The government will analyze and verify policies in the first half of FY2009 in collaboration with government agencies in charge of critical infrastructures. “A Principle for Formulating 'Safety Standards, Guidelines, etc.' concerning Assurance of Information Security of Critical Infrastructures (Version 3)” (provisional name) should be decided by October 2009. In addition, the government will continue to analyze and verify these guidelines in order to reflect new knowledge and experience as social trends change, and will prepare for publication of a supplementary version after 2010 if necessary.

B) Continuous Improvement of Safety Standards

a) Continuous Improvement of Safety Standards (Government Agencies in

Charge of Critical Infrastructures)

The government will analyze and verify the safety standard of all critical infrastructures by the end of FY2009 based on “A Principle for Formulating 'Safety Standards, Guidelines, etc.' concerning Assurance of Information Security of Critical Infrastructures (Version 3)” and characteristics of each critical infrastructure. Also, the Safety Standards will be revised as necessary.

b) Reinforcement of Information Security Management in Telecommunications Services (Ministry of Internal Affairs and Communications)

In order to contribute towards the implementation and operation of telecommunication carriers’ information security systems, the government will continue to make efforts to establish and spread national standards and certification systems in liaison with national standardization organizations, concerning the Information Security Management Guidelines for Telecommunications (ISM-TG) formulated in FY2006 by telecommunication vendors and concerned organizations, with consideration to international standardization.

c) Safety and Reliability Assurance for IP Network Compliant Telecommunication Systems (Ministry of Internal Affairs and Communications)

In order to ensure stability of ICT services as the IP network increases, the government will take necessary safety and reliability measures such as definition of analysis methods for highly technical incidents from the perspective of network facilities and operations and management by the end of FY2009.

d) Continuous Management and Verification of the Safety Standard Improvement Status (Cabinet Secretariat)

The government will verify the status of analysis, verification, revision, and action plans of critical infrastructure “Safety Standards” and publish the results within FY2009 in collaboration with government agencies in charge of critical infrastructures.

C) Spread of Safety Standards (Cabinet Secretariat and Government Agencies in Charge of Critical Infrastructures)

The government will make efforts to spread the security standards of critical infrastructures, investigate the dissemination status at the beginning of FY2009 in collaboration with government agencies in charge of critical infrastructures, and

publish the results by October 2009.

The government will also plan and prepare for investigations in the next fiscal year.

(b) Reinforcement of Information Sharing System

The government will organize the information which is shared among concerned organizations including CEPTOARs and CEPTOAR-Council established in the First Action Plan. Also the government will prepare the environment required for providing and communicating information, and encourage autonomous activities of the CEPTOARs and CEPTOAR-Council.

[Specific Measures]

A) Organization of Information Subject to Sharing (Cabinet Secretariat)

The government will organize information on IT-malfunctions subject to sharing and the sharing method from the perspective of disaster prevention, damage minimization, swift recovery, and recurrence prevention.

B) Enrichment of Information Supply and Communication

a) Review of Information Sharing Rules (Government Agencies in Charge of Critical Infrastructures)

There are information sharing rules for information supply from government agencies in charge of critical infrastructures to CEPTOARs, and information sharing rules for information communication from critical infrastructure vendors to government agencies in charge of critical infrastructures. The government will confirm the consistency of these rules against “Implementation Details Concerning Information Supply and Communication in the 'Second Action Plan on Information Security Measures for Critical Infrastructure'” (called the “Implementation Details” hereinafter), and revise the information sharing rules as necessary.

Also, the government will advice CEPTOARs to check information sharing rules within the CEPTOAR to maintain consistency with the “Implementation Details” and will confirm the status of this task.

b) Review of the “Implementation Details” Concerning Information Supply and Communication in the Second Action Plan (Cabinet Secretariat)

The government will review the Implementation Details based on their operational status and the progress of the “organization of information subject to sharing.”

c) Preparation of a Support System for Improving Reliability of the Information System for Critical Infrastructures (Ministry of Economy, Trade and Industry)

In order to support the proactive efforts of critical infrastructure vendors to improve reliability of information systems, the IPA Software Engineering Center will in continuation from FY2008 develop a database from an expert/technical perspective, conduct macro-based quantitative analysis and provide the accumulated information to the CEPTOARs. Support will also be provided for development and operations of information systems upon request from critical infrastructure vendors.

d) Implementation of CEPTOAR Training (Cabinet Secretariat and Government Agencies in Charge of Critical Infrastructures)

The government will provide opportunities to confirm the information communication function to maintain and improve the information sharing system between CEPTOARs in collaboration with government agencies in charge of critical infrastructures.

C) Reinforcement of CEPTOARs (Cabinet Secretariat and Government Agencies in Charge of Critical Infrastructures)

In order to encourage CEPTOARs growth, the government will summarize the functions and activity status of each CEPTOAR to share the information with each CEPTOAR in collaboration with government agencies in charge of critical infrastructures. The summary of functions and activity status of each CEPTOAR will be published around the end of FY2009.

D) Support for the CEPTOAR-Council (Cabinet Secretariat)

The Cabinet Secretariat will act as the administrative office to support the activities of CEPTOAR-Council.

(c) Common Threat Analysis

Dependency analysis was carried out in the First Action Plan to understand which IT-malfunction would affect which critical infrastructure. The government will continue the analysis and study possible common threats among the critical infrastructures.

[Specific Measures]

A) Common Threat Analysis (Cabinet Secretariat)

The government will analyze threats which may be common among critical infrastructures in conjunction with the dependency analysis on prioritized subjects. The government will also investigate trends of concerned domestic

studies and existing IT-malfunction cases. Subjects of the above analysis and investigation will be determined by a questionnaire to critical infrastructure vendors.

The government will request cooperation from government agencies responsible for critical infrastructures, CEPTOARs, and critical infrastructure vendors and will consider liaising with research organizations to improve the effectiveness.

The results of the analysis and investigation will be summarized into a report and published where possible.

(d) Cross-sectoral Exercise

The government will conduct a cross-sectoral infrastructure exercise assuming an IT-malfunction with the collaboration of government agencies in charge of critical infrastructures, critical infrastructure vendors, and CEPTOARs for those critical infrastructures, based on knowledge and experience on cross-sectoral exercise methods obtained in the First Action Plan.

[Specific Measures]

A) Cross-sectoral Exercise (Cabinet Secretariat and Government Agencies in Charge of Critical Infrastructures)

In collaboration with government agencies in charge of critical infrastructures, CEPTOARs, critical infrastructure vendors, the government will examine a exercise scenario on the assumption of a specific IT-malfunction and carry out a cross-sectoral exercise to extract issues and systematize knowledge and experience for exercises.

The knowledge and experience gained will be shared among the concerned parties and published where possible.

B) Reinforcement of Response to Cyber Attacks in Telecommunications (Ministry of Internal Affairs and Communications)

In order to develop human resources with advanced ICT skills who are able to reinforce and mediate the liaison system between the concerned vendors and government in the event of an emergency, the government will continue to promote cyber attack response exercises carried out by telecommunication vendors on the assumption of an inter-infrastructure Internet cyber attack in liaison with Telecom-ISAC Japan which is formed by telecommunication vendors and manufacturers.

C) Information Security International Conference (Cabinet Secretariat and the

Concerned Government Agencies)

The government will start a campaign for inviting the International Watch and Warning Network (IWWN) Conference which will be attended by experts from critical infrastructure protection teams, emergency response teams, and law enforcement agencies all over the world in preparation for participation in the global scale cyber exercise “Cyber Storm III.”

(e) Adaptation to Environmental Changes

In order to swiftly adjust information security measures according to changes in social and technological environments, the government will make efforts to improve its capability of sensing such changes which were not assumed at the time of developing the Second Action Plan. If such changes cannot be dealt with using the framework of the Second Action Plan, the cabinet secretariat will study an alternative system.

[Specific Measures]

A) PR and Public Hearing Activities

a) Promotion of PR and Public Hearing Activities (Cabinet Secretariat)

The government will implement and operate a web site dedicated to PR and public hearing for information security measures.

The government will make good use of seminars and lectures to actively publicize the “Second Action Plan” and measures based on the plan.

b) Implementation of Awareness-Raising Seminars for Critical Infrastructure Vendors (Ministry of Economy, Trade and Industry)

In order to provide information concerning domestic and overseas advanced measures against IT-malfunction, the IPA or the General Incorporated Association Japan Computer Emergency Response Team Coordination Center (called “JPCERT/CC” hereinafter) will hold the “Critical Infrastructure Information Security Forum” in FY2009.

B) Enhancement of Risk Communications

a) Enhancement of Risk Communication (Cabinet Secretariat, Government Agencies in Charge of Critical Infrastructures)

The government will prepare an environment for risk communication between critical infrastructure vendors, the concerned organizations, and government agencies in charge of critical infrastructures, in collaboration with government agencies in charge of critical infrastructures.

b) Measures to Reduce Vulnerabilities in Software and Information Systems

(Ministry of Economy, Trade and Industry)

If vulnerability is found after the software product or information system is on the market or on operation, both the developer and user will incur cost for repair. On the other hand, if measures are not appropriately applied, it might become target of attacks such as illegal access which might cause even more serious damage. In order to minimize such costs and risks, JPCERT/CC will publicize information security issues to consider at different stages such as design, programming, and pre-shipping tests of software products in the form of practical guides and seminars to software developers. Activities such as holding secure coding seminars and spreading coding standards among actual developers will take place in FY2009 concerning languages which are widely used for embedded software that is not easy to rectify once on the market.

c) Prioritized Supply of Software Vulnerability Related Information to Critical Infrastructure Vendors, and Support for Information Security Related Information Management (Ministry of Economy, Trade and Industry)

The government will provide vulnerability related information on pre-release software, information security threats which are likely to require measures from critical infrastructure vendors, and countermeasures to CEPTOARs or critical infrastructure vendors through JPCERT/CC as an early warning based on prior agreement.

Also, the government will provide information concerning implementation and operations of Computer Security Emergency Response Team (called the “CSIRT” hereinafter) for critical infrastructure, and a tool to help efficient management of numerous information security related information items, and will enhance the service that distributes vulnerability information in a format that can be automatically loaded to the management tool.

In addition, the JPCERT/CC will support countermeasures against information security incidents such as coordination of actions against the attacker, and analysis of the attack method upon request from critical infrastructure vendors.

d) Supply of Information Concerning Vulnerabilities in the Control System in the Critical Infrastructure Operation (Ministry of Economy, Trade and Industry)

The government will supply collected information concerning vulnerability risk mitigation for control systems used in the operation of a critical infrastructure and measures against threats to the concerned vendors. The government will also start investigating specifications of a test tool which will enable assessment of control systems in a near-live environment.

e) Implementation of a Liaison System for Measures against Vulnerabilities in Control Systems (Ministry of Economy, Trade and Industry)

The number of potential threats to control system products is expected to rise as the number of implementations of standard protocols (TCP/IP, Ethernet, etc.) and general products rises. On the other hand, measures and best practice are still in the development phase. Therefore, development and implementation engineers are expected to suffer from an increasing burden of collecting and assessing information. For that reason, the government plans to use the "Control System Vendor Security Information Sharing Task Force", set up in FY2008, with JPCERT/CC as the administrative office to launch its full scale operations. Activities such as collecting information concerning security measures on control systems and information sharing will contribute towards smooth measure application against threats to vulnerabilities in control systems.

C) Promotion of International Liaison (Cabinet Secretariat)

The government will collect the best practice from overseas as well as investigate activities of international organizations concerning information security policies and standardization.

Also, the government will gather information concerning international threats and vulnerability information and will provide it to the concerned organizations.

[3] Enterprises

Targeting the global leader position of security measure implementation in enterprises, the government will prioritize the following policies in FY2009.

(a) Establishment of Information Security Governance as "Part of Corporate Management"

In order to position information security governance as part of business management, the government will promote PR activities to management and develop a rational information security governance process model. While reinforcing a system to raise awareness of the management, the government will encourage the spread of concrete measures by further developing and improving Information Security Management System (ISMS) compliance assessment, information security audit, IT security assessment and certification, encryption module test and certification systems, information security reporting model, information security measures benchmarking tool, etc. Also, the government will specify the information security measure application level as assessed by using the systems above or the results of a third party assessment as one of the supplier tender conditions where necessary. In addition, the government will examine a useful cost effectiveness assessment method to prevent information security governance from becoming an excessive burden for enterprises. In order to position information security governance as "part of corporate management", there are issues which should be adjusted in line with the concerning laws and regulations. Therefore,

the government will also analyze and organize the concerning laws and regulations, and summarize them in guidelines.

[Specific Measures]

A) Promotion of Establishment of Information Security Governance (Ministry of Economy, Trade and Industry)

In order to promote establishment of information security governance in enterprises, the government will formulate and publicize the “Information Security Governance Implementation Guidance” and “Information Security Measure Guidance for Outsourcing” and promote international standardization for deployment in international business liaisons.

The government will continue to encourage enterprises to deploy guidelines and assessment indices formulated in the “Guidelines for Improving Reliability of Information Systems Second Version” which was revised in FY2008 to emphasize issues such as IT governance and operations, and the “Evaluation Index concerning Improvement of the Reliability of Information Systems.”

B) Promotion of Information Security Audit System (Ministry of Economy, Trade and Industry)

The assurance based information security audit which grants a certain guarantee on comments made by an auditor on the information security of the audited subject should be more widely deployed. The government will promote the assurance base audit by supporting development of management standards and audit policies focused on the industry and business type.

C) Streamlining Third Party Assessment and Promotion of High Quality Information Security Related Products (Ministry of Economy, Trade and Industry)

The government will promote the IT security assessment and certificate systems by IPA and encourage the use of these systems at information system procurement in FY2009. The government will also promote deployment of the encryption module test and certification system by IPA.

D) Deployment and Establishment of “Information System Model Transaction/Contract” (Ministry of Economy, Trade and Industry)

The government published the “Information System Model Transaction/Contract (Version 1)” in April 2007 in order to improve reliability of information systems by clarifying the transaction between the user and vendor, as well as the roles of each party. The government subsequently developed a simple

and transparent transaction model, the “Information System Model Transaction/Contract (Supplemental Edition)” in April 2008, based on the “Explanatory Note of Important Matters” especially for transactions when using SaaS[12] or ASP[13], packages widely used by small and medium enterprises. The government will liaise with both the users and vendors in organizations in the concerned industries in order to encourage the use of these model transactions/contracts.

E) Distribution of “Information Security Measure Benchmark System” (Ministry of Economy, Trade and Industry)

The IPA will continue to provide the “Information Security Measure Benchmark System.”

F) Improvement of Indices for Enterprises (Ministry of Economy, Trade and Industry)

The government will carry out the “Survey on Information Processing” to investigate the usage of information security audit systems, the information security management system compliance assessment and the use of information security measure benchmarks in enterprises, the confirmation status of information security measures at counterparties (including outsourcing and consignment), and the implementation status of ISO/IEC15408 certified products in enterprises.

G) Review of Tender Conditions (Cabinet Secretariat, Ministry of Internal Affairs and Communications, Ministry of Finance, Ministry of Economy, Trade and Industry, and All Government Agencies)

With regard to government procurement of IT systems, the concerned government agencies will examine the method of incorporating tenders' information security application status such as the results of ISMS, information security audit, information security level assessment into consideration.

H) Promotion of Electronic Signature in Enterprises (Ministry of Internal Affairs and Communications, Ministry of Justice, and Ministry of Economy, Trade and Industry)

Based on the results of the “Study Committee Concerning Enforcement of the Electronic Signature and Authentication Law”, the government will study

[12] Software as a Service

[13] Application Service Provider

methods of promoting the use of electronic signatures in enterprises.

(b) Promotion of Products and Services which Contribute to the Improvement of Information Security at Enterprises

The government will prepare an environment to assist enterprises to understand and select the necessary information security measures. The government will continue its efforts in the First National Strategy to promote studies on the practical use of quantitative assessment of information security related risks in enterprises, and the use of IT security assessment and certification systems.

However, in order to promote the supply of products and services which contribute to the improvement of the information security, reinforcement on the part of the assisted organization must not be overlooked. Therefore, the government will encourage the use of SaaS and ASP to facilitate the measures, reinforcement of anti-spam measures, encryption and authentication technologies, and security assessment systems for an NGN/IPv6 transition environment. Also, promotion of products and services should take their total cost of ownership into consideration as well.

[Specific Measures]

A) Support for Management of Software Vulnerabilities (Ministry of Economy, Trade and Industry)

The IPA launched the operation of a mechanism where vendors and users quantitatively compare the severity of vulnerabilities under internationally confirmed standards and provide such information which would contribute towards determining the importance and priority of measures. The IPA will continue the operation and enhance the function.

Also, the JPCERT/CC's efforts to emphasize the importance of vulnerability management of software at user organizations and support activities will be reinforced. Specifically, the government will encourage and improve various tools and methods for vulnerability management of organizations including critical infrastructure, and will enhance the service that distributes vulnerability information in a format that can be automatically loaded to the management tool in order to reduce costs in user organizations.

B) Measures to Reduce Vulnerabilities in Software and Information Systems (Ministry of Economy, Trade and Industry) [Reprise: Refer to Chapter 3, Section 1 (1) [2] (e) B) b)]

If vulnerability is found after the software product or information system is on the market or on operation, both the developer and user will incur cost for repair. On the other hand, if measures are not appropriately applied, it might become target of attacks such as illegal access which might cause even more serious damage. In order to minimize such costs and risks, JPCERT/CC will publicize information security issues to consider at different stages such as design,

programming, and pre-shipping tests of software products in the form of practical guides and seminars to software developers. Activities such as holding secure coding seminars and spreading coding standards among actual developers will take place in FY2009 concerning languages which are widely used for embedded software that is not easy to rectify once on the market.

C) Safety Improvement in Corporate Web Sites (Ministry of Economy, Trade and Industry)

In order to contribute towards early detection and remedy of web application vulnerabilities, the government will continue to provide to the administrator of corporate web sites the “log analysis type web site vulnerability check tool” (iLogScanner) which analyzes the log to check for any trace of external attacks, and will take appropriate action against new attack patterns as necessary.

D) Safety Improvement for Embedded Software (Ministry of Economy, Trade and Industry)

The government will continue to provide vulnerability check tools for TCP/IP and SIP which are protocols used by developers of embedded devices and electric household information appliances, and will take the appropriate action against newly discovered vulnerabilities.

E) Deployment of the “Policies for Information Disclosure Concerning Safety and Reliability of Data Centers” (Ministry of Internal Affairs and Communications)

Demand for Data Centers as the foundation of corporate activities is increasing rapidly in recent years due to their superior quality and lower environmental load. The trend of comparing, evaluating, and selecting a Data Center is apparent. In response, the government will classify mandatory and optional items for information disclosure concerning safety and reliability of a Data Center to standardize and add disclosure items. The government will also promote the use of the “Policies for Information Disclosure Concerning Safety and Reliability of Data Centers (Version 1)” formulated and published in February 2009, that clarifies information disclosure items concerning the building, facility, and security of Data Centers to assist the users to compare, evaluate, and select the Data Center.

F) Streamlining Third Party Assessment and Promotion of High Quality Information Security Related Products (Ministry of Economy, Trade and

Industry) [Reprise: Refer to Chapter 3, Section 1 (1) [3] (a) C)]

The government will promote the IT security assessment and certificate systems by IPA and encourage the use of these systems at information system procurement in FY2009. The government will also promote deployment of the encryption module test and certification system by IPA.

G) Preparation of a Security Assessment System for System LSI (Ministry of Economy, Trade and Industry)

The government will prepare the system required for ISO/IEC15408 compliance security assessment within Japan to assess system LSIs used on IC cards by FY2011.

H) Establishment of the Common Quality Indicator for Reliability Assessment (Ministry of Economy, Trade and Industry)

Quality management using quantitative data is effective in improving the success rate of system development projects and improving information system reliability. Organizations in concerned industries are formulating quality indicators and accumulating quantitative data. The government will establish and distribute common rules to enable sharing quality indicators and quantitative data to further promote quality management using quantitative data.

I) Deployment and Establishment of the “SLA Guideline for SaaS” (Ministry of Economy, Trade and Industry)

In order to assist enterprises to ensure appropriate transactions when using SaaS and to use SaaS more effectively, the government will promote the use of the “SLA Guidelines for SaaS” among SaaS users and providers. The document was formulated and published in January 2008 and describes guidelines concerning the service level where users and service providers should agree on from the viewpoint of information security.

J) Deployment of the “Certification System for Information Disclosure Concerning Safety and Reliability of ASP and SaaS” (Ministry of Internal Affairs and Communications)

In order to assist enterprises to compare, evaluate, and select ASP or SaaS services, the government will publicize and make use of the privately operated certification system for information disclosure concerning safety and reliability of ASP and SaaS based on the “Guidelines for Information Disclosure Concerning Safety and Reliability of ASP and SaaS.”

K) Establishment and Development of the “Guidelines for Information Disclosure concerning ASP/SaaS Security and Reliability for Medical Information” (Ministry of Internal Affairs and Communications)

The importance of medical information requires high safety standards. Therefore, it is important to promote appropriate and safe handling of medical information in ASP and SaaS services. The government will develop the “Guidelines for Information Disclosure concerning ASP/SaaS Security and Reliability for Medical Information” to indicate requirements to the ASP and SaaS vendors such as the responsibilities when handling medical information and the approach to agreement, as well as promote the use of the “Guidelines for Information Disclosure concerning ASP/SaaS Security and Reliability for Medical Information” among ASP and SaaS users and vendors who handle medical information.

L) Development of Systems to Facilitate Information Security Measures (Ministry of Economy, Trade and Industry)

The government will develop a system which will serve as the foundation of Software as a Service (SaaS) on the Internet to allow small and medium enterprises to improve operational efficiency inexpensively and easily, and applications such as security management which runs on the system.

M) Enhancement of Anti-Spam Measures (Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

In order to take measures against growing spam e-mails which are increasingly skillful and malicious, the government will steadily enforce the Act on Regulation of Transmission of Specified Electronic Mail, to which an opt-in system has been introduced under a change in the law in 2008, and the Act on Specified Commercial Transactions.

The government will also promote implementation of effective technologies for preventing spam e-mail transmission such as port 25 blocking and sender domain authentication in collaboration with industrial associations such as the JEAG (Japan Email Anti-Abuse Group) founded under an initiative of major Internet service providers and mobile phone service providers in Japan.

However, a large part of spam e-mails received in Japan are transmitted from overseas. The government will also reinforce liaison with overseas authorities in charge of spam e-mail measures as well as promote international spam e-mail measures in private sectors.

In addition, the government will continue to promote the “Project for Eliminating Unsolicited E-mail” (since February 2005) which notifies information on illegal spam e-mail to the Internet service provider which was used to transmit such e-mail and requests them to take an action such as suspension of services.

N) Development of a System to Secure Dependability of Embedded Systems (Ministry of Economy, Trade and Industry)

The government will study the items which developers should take into consideration in order to secure dependability of embedded systems. Also, the government will encourage concerned organizations to improve their ability to analyze and assess safety, such as the anti-tampering technology of LSI chips and IC cards which are the core of embedded systems, and to prepare the system for such tasks.

O) Promotion of Electronic Signature in Enterprises (Ministry of Internal Affairs and Communications, Ministry of Justice, and Ministry of Economy, Trade and Industry) [Reprise: Refer to Chapter 3, Section 1 (1) [3] (a) H)]

Based on the results of the “Study Committee Concerning Enforcement of the Electronic Signature and Authentication Law”, the government will examine methods of promoting the use of electronic signatures in enterprises.

P) Implementation of a Security Assessment System in NGN/IPv6 Environments (Ministry of Internal Affairs and Communications)

The government will extract specific security threats and vulnerabilities in the NGN/IPv6 transition process, assess the importance, and develop a security assessment system for NGN/IPv6 environments in pursuit of measures.

Q) Clarification of Legality of Reverse Engineering of Software and the Like for Safety Purposes (Ministry of Education, Culture, Sports, Science and Technology)

In response to the report from the Subdivision on Copyrights within the Council for Cultural Affairs, the government will take action swiftly to clarify the legality of reverse engineering for the purpose of information security.

R) Preferential Tax Treatment for Investment in Corporate Information Systems with Advanced Information Security (Ministry of Economy, Trade and Industry, and Ministry of Internal Affairs and Communications)

The information infrastructure reinforcement tax system was extended for two years and enhanced by the tax system reform in FY2008. The government will continue its efforts to spread the system and promote investment into information systems with high standard information security.

S) Establishment of an Agreement Method for Non-functional Requirements[14] (Ministry of Economy, Trade and Industry)

The government will develop an appropriate agreement method between users and vendors on non-functional requirements including reliability, performance, and security in order to improve dependability of information systems, and liaise with concerned industries to promote its deployment.

(c) Development and Assignment of Information Security Human Resources in Enterprises

Development and assignment of information security human resources are essential in enterprises as well as improving awareness of information security measures in management. The government will widely promote PR and dissemination by holding seminars on human resource development. In terms of measures, it is essential to foster and maintain human resources who can flexibly handle environmental changes such as new IT services, or human resources who are capable of making decisions based on a broad view of the entire enterprise management. In such a case, it is also important to consider the career path the information security human resource can aim for. Therefore, the government will encourage development of a common career skill framework to establish skill standards as an objective human resource assessment mechanism by the joint effort of public and private sectors. The government will also promote the use of the Information-Technology Engineers Examination, and frameworks and qualification tests concerning human resource development in private sectors which are compliant with the above mentioned common career skill framework. In addition, the government will also prepare a system to establish curriculums for advanced information security human resource development, teacher training, and internship programs through industry and academia cooperation.

The government will make its efforts to develop and assign human resources who will play the central role in corporate information security through development of a model career development plan concerning information security for engineers and support for experts' communities.

In addition, the government will promote development of human resources who can handle migration to a new environment, such as the forthcoming NGN/IPv6 migration, who is observant to laws and regulations, and who can take information security measures with a clear understanding of risks concerning information assets and business continuity.

[Specific Measures]

A) Promotion of Information Security Measures in Small and Medium Enterprises (Ministry of Economy, Trade and Industry)

The government will hold the “Small and Medium Enterprise Information

[14] Non-functional requirements specify performance and quality of information system software, such as the response time, batch process limit time, and usability.

Security Leader Training" to educate leaders in small and medium enterprises, and encourage them to spread information security to the management.

B) Information Security Seminars for Small and Medium Enterprises (Ministry of Economy, Trade and Industry)

The IPA and Chamber of Commerce and Industry will hold the "Information Security Seminar" in various parts of Japan to nurture understanding of information security among management and information system staff in small and medium enterprises in FY2009. The IPA and Chamber of Commerce and Industry will reinforce liaison with regional core organizations as well as promote PR activities in collaboration with the IT Management Support Group.

C) Development of Human Resources for Information Security Audit (Ministry of Economy, Trade and Industry)

The government will make its efforts to develop human resources for information security audits who are able to assess information security measures both from the inside and outside of the organization as well as objectively and impartially.

D) Development of Information Security Supporters (Ministry of Internal Affairs and Communications)

The government will make its efforts to raise the standard of information security of all the population by supporting materials, seminars, and certificate tests concerning information security to develop well acquainted people (information security supporter) among users.

E) Further Dissemination of the 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, the government will review the Information-Technology Engineers Examination which measures skills of information human resources according to the common career skill framework, and reintroduce the examination in FY2009. The government plans to make good use of this examination to produce successful candidates since an effective career path will be created by the appropriate human resource assessment method based on the common career skill framework.

F) Dissemination of Private Sector Security Qualifications (Cabinet Secretariat,

Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

The government will publicize information on private sector qualifications concerning information security to further develop information security experts in the private sector.

G) IT Human Resource Development by Industry-Academia Cooperation (Ministry of Economy, Trade and Industry)

In order to develop advanced IT human resources including those in information security, the government promotes industry-academia cooperation to endorse teachers with an industrial background, develop and make use of practical materials and curriculums, and promote practical internship through industry-academia matching.

H) Support System for Information Communication Human Resource Seminars (Ministry of Internal Affairs and Communications)

The government will continue to support training activities to develop human resources for telecommunications, including those with specialist knowledge and expertise in information communication security in FY2009.

I) Preparation of a Test Bed for Acquiring IPv6 Operation Techniques (Ministry of Internal Affairs and Communications)

In order to address the forthcoming IPv4 exhaustion, IPv6 compliance is an urgent matter. However, development and assignment of IPv6-acquainted human resources are becoming a major issue due to insufficient IPv6 operation experience and knowledge among network operators.

Therefore, the Ministry of Internal Affairs and Communications will make its efforts to improve operation techniques of private sector network operators by establishing the “IPv6 Operation Training Center” with an IPv6 test network with complexity equivalent to real life network in order to develop and assign IPv6-acquainted human resources.

J) Model Career Development Planning (Ministry of Economy, Trade and Industry)

In order to develop advanced IT human resources including those in information security, it is important for students and young engineers to be able to imagine their own career path; however, career paths in the IT industry are not as clear as those in other industries. Therefore, the government will develop and

publicize a model career path for each function with assistance of experts' communities.

(d) Reinforcement of Business Continuity and Emergency Response System to Support an "Accident Assumed Society"

Information security incidents such as computer viruses and vulnerabilities must be dealt with precisely and effectively. The government will promote implementation of a communication network for information sharing, and reinforcement of liaison between organizations in preparation for such incidents. In order to reinforce business continuity ability, the government will promote development of business continuity plans in enterprises and distribute and improve the Guideline for Business Continuity Plans. In addition, the government will reinforce the necessary emergency response systems to provide swift and effective measures in the event of an information security incident.

[Specific Measures]

A) Reinforcement of the Computer Security Early Warning Partnership (Ministry of Economy, Trade and Industry)

Information security issues such as computer viruses, illegal access, and vulnerabilities are growing day-to-day, and the concerned parties must secure swift information sharing and smooth response to such incidents. The IPA and JPCERT/CC will reinforce their "Computer Security Early Warning Partnership" in response to changes in threats.

Specifically, in order to deal with highly skilled attack methods of recent computer viruses, organizations which support incident response such as the JPCERT/CC will improve their ability to analyze attack methods, and promote information sharing and liaison among experts. Also, they will encourage organizations' response to information security issues by studying and establishing methods for an effective internal incident response exercise with consideration to the trend of threats, and promoting information sharing.

B) Deployment of Emergency Response Teams in Organizations and Reinforcement of Liaison System (Ministry of Economy, Trade and Industry)

Swift and effective emergency response systems are required for dealing with an information security incident. The JPCERT/CC will take initiative to share materials concerning CSIRT[15] implementation, and make use of a system for sharing information on specific threats and measures as well as their attack details and required analysis to assist determining the incident response among appropriate parties in order to encourage formation of CSIRTs as well as a more efficient liaison among domestic and overseas CSIRTs both in an emergency and

[15] Abbreviation for Computer Security Incident Response Team.

peaceful time in FY2009.

C) Implementation of a Liaison System for Measures against Vulnerabilities in Control Systems (Ministry of Economy, Trade and Industry) [Reprise: Refer to Chapter 3, Section 1 (1) [2] (e) B) e)]

The number of potential threats to control system products is expected to rise as the number of implementations of standard protocols (TCP/IP, Ethernet, etc.) and general products rises. On the other hand, measures and best practice are still in the development phase. Therefore, development and implementation engineers are expected to suffer from an increasing burden of collecting and assessing information. For that reason, the government plans to use the “Control System Vendor Security Information Sharing Task Force”, set up in FY2008, with JPCERT/CC as the administrative office to launch its full scale operations. Activities such as collecting information concerning security measures on control systems and information sharing will contribute towards smooth measure application against threats to vulnerabilities in control systems.

D) Support for Management of Software Vulnerabilities (Ministry of Economy, Trade and Industry) [Reprise: Refer to Chapter 3, Section 1 (1) [3] (b) A)]

The IPA launched the operation of a mechanism where vendors and users quantitatively compare the severity of vulnerabilities under internationally confirmed standards and provide such information which would contribute towards determining the importance and priority of measures. The IPA will continue the operation and enhance the function.

Also, the JPCERT/CC’s efforts to emphasize the importance of vulnerability management of software at user organizations and support activities will be reinforced. Specifically, the government will encourage and improve various tools and methods for vulnerability management of organizations including critical infrastructure, and will enhance the service that distributes vulnerability information in a format that can be automatically loaded to the management tool in order to reduce costs in user organizations.

E) Distribution of Information on the Method of Targeted Attacks and Measures (Ministry of Economy, Trade and Industry)

The IPA and JPCERT/CC will collect and examine specimens of targeted attacks, analyze the attack methods and develop measures in liaison with concerned organizations, and provide information as necessary.

(e) Promotion of Information Security Measures in Small and Medium Enterprises

Application of information security measures are behind in small and medium enterprises due to shortage of resources such as available personnel, budget, and IT infrastructure. Therefore, the government will promote their information security measures by preparing an environment where these enterprises may easily select appropriate measures from various options. For instance, the government will continue to improve the information security benchmark which measures the information security level in order to develop and spread a unified check list that can be used to objectively assess and show an enterprise's information security level.

It is also necessary to take effective approaches to promote security measures in small and medium enterprises, such as providing easy and low cost security tools. Therefore, the government will promote the use of SaaS and ASP, and publish information security standards in these service providers.

In addition, the government will promote PR activities such as holding seminars in order to enhance understanding of information security among management and information system personnel of small and medium enterprises.

[Specific Measures]

A) Preferential Tax Treatment for Investment in Corporate Information Systems with Advanced Information Security (Ministry of Economy, Trade and Industry, and Ministry of Internal Affairs and Communications) [Reprise: Refer to Chapter 3, Section 1 (1) [3] (b) R)]

The information infrastructure reinforcement tax system was extended for two years and enhanced by the tax system reform in FY2008. The government will continue its efforts to spread the system and promote investment into information systems with high standard information security.

B) Promotion of Information Security Measures in Small and Medium Enterprises (Ministry of Economy, Trade and Industry)

In order to optimize the burden of cost for information security measures in small and medium enterprises, the government will distribute the information security measures guidelines for small and medium enterprises formulated in FY2008, and continue to study information security measure packages for small and medium enterprises.

C) Deployment and Establishment of the "SLA Guideline for SaaS" (Ministry of Economy, Trade and Industry) [Reprise: Refer to Chapter 3, Section 1 (1) [3] (b) I)]

In order to assist enterprises to ensure appropriate transactions when using SaaS and to use SaaS more effectively, the government will promote the use of

the “SLA Guidelines for SaaS” among SaaS users and providers. The document was formulated and published in January 2008 and describes guidelines concerning the service level where users and service providers should agree on from the viewpoint of information security.

D) Development of Systems to Facilitate Information Security Measures (Ministry of Economy, Trade and Industry) [Reprise: Refer to Chapter 3, Section 1 (1) [3] (b) L)]

The government will develop a system which will serve as the foundation of Software as a Service (SaaS) on the Internet to allow small and medium enterprises to improve operational efficiency inexpensively and easily, and applications such as security management which runs on the system.

E) Development of Human Resources for Information Security Audit (Ministry of Economy, Trade and Industry) [Reprise: Refer to Chapter 3, Section 1 (1) [3] (c) C)]

The government will make its efforts to develop human resources for information security audits who are able to assess information security measures both internally and externally to the organization objectively as well as impartially.

F) Promotion of Information Security Measures in Small and Medium Enterprises (Ministry of Economy, Trade and Industry) [Reprise: Refer to Chapter 3, Section 1 (1) [3] (c) A)]

The government will hold the “Small and Medium Enterprise Information Security Leader Training” to educate leaders in small and medium enterprises, and encourage them to spread information security to the management.

G) Information Security Seminars for Small and Medium Enterprises (Ministry of Economy, Trade and Industry) [Reprise: Refer to Chapter 3, Section 1 (1) [3] (c) B)]

The IPA and Chamber of Commerce and Industry will hold the “Information Security Seminar” in various parts of Japan to nurture understanding of information security among management and information system staff in small and medium enterprises in FY2009. The IPA and Chamber of Commerce and Industry will reinforce liaison with regional core organizations as well as promote PR activities in collaboration with the IT Management Support Group.

H) Support System for Information Communication Human Resource Seminars (Ministry of Internal Affairs and Communications) [Reprise: Refer to Chapter 3, Section 1 (1) [3] (c) H)]

The government will continue to support training activities to develop human resources for telecommunications, including those with specialist knowledge and expertise in information communication security in FY2009.

(f) Promotion of Information Security Policies to Support Global Business Deployment of Japanese Enterprises

The government will make its efforts to establish information security at overseas business bases of Japanese enterprises which seek global business development. For instance, the government will promote international liaison and cooperation to implement a secure network environment, as well as to establish an environment for smooth outsourcing in countries and regions closely related to business operations of Japanese enterprises such as Asia.

[Specific Measures]

A) Promotion of Implementation of a Secure Business Environment in the Asian Region (Ministry of Economy, Trade and Industry)

In response to a study on strategies concerning an Asian common information security measure benchmark which was carried out by the ERIA (Economic Research Institute for ASEAN and EAST Asia) in FY2008, and in accordance with the “Asia Knowledge Economy Initiative” proposed by Japan in the ASEAN Economic Ministers Meeting in FY2008, the government will conduct a joint study of the method to promote secure business implementation in the Asian region with researchers from Asian countries, using Japan’s knowledge. The government will also undertake promotion activities such as seminars on enterprises' information security measures in several countries of the Asian region, and human resource development.

B) Secure Coding Seminars in Software Development Outsourcing Countries (Ministry of Economy, Trade and Industry)

The JPCERT/CC will hold technical seminars on coding techniques that can prevent vulnerabilities in countries where Japanese enterprises are outsourcing embedded software development. Seminars are planned in three countries in the ASEAN region in FY2009.

C) Support for Implementation and Operations of Overseas Emergency Response Teams (Ministry of Economy, Trade and Industry)

The JPCERT/CC will support implementation and operations of in-house corporate CSIRTs in countries and regions closely related to business activities of

Japanese enterprises. The JPCERT/CC will carry out promotion activities such as CSIRT implementation seminars and provide technical support in the Asian region in FY2009.

[4] Individuals

With the aim of reducing the number of people "with concerns about using IT" to zero as much as possible, the government will prioritize the following measures in FY2009.

(a) Enhancement/Promotion of Information Security Education

Education/enlightenment will be promoted for children, students and guardians who are actively using and applying IT but may not necessarily be adequately aware of the risks nor recognize the importance of information security measures. For this reason, education on information ethics[16] will be promoted in schools and communities.

In addition, an environment will be prepared for individuals, as consumers, to recognize the risks arising from the use of various services so that those risks do not turn into harm. Besides the enlightenment activities for individuals, appropriate risk and countermeasure information will be provided by service providers and organizations for countermeasure support for promoting incident response actions.

[Specific Measures]

A) Promotion of Education/Enlightenment for Children, Students, and Guardians

a) Deployment of Study, Development, and Enlightenment Activities for the Improvement of Media Literacy (Ministry of Internal Affairs and Communications)

The development of literacy-related teaching materials in consideration with the special characteristics of the media will be studied in order to improve the ICT media literacy[17] required in the promotion of the sound use of ICT media such as Internet and mobile phones. In addition, the teaching materials (mainly targeted at elementary year 5 and 6 grades) already developed right through FY2008 will also be continuously published and promoted.

b) Dissemination and Enlightenment Based on "Information Security Measures" Slogans and Posters (Ministry of Economy, Trade and Industry)

In FY2009, as a joint operation with the Korea Information Security Agency

16 Information ethics is the "attitude and way of thinking as the base for appropriate conduct in an information society" (High School Curriculum Guidelines, Information Edition).

17 "ICT media literacy" is not just the ability to access and use ICT, but it is a concept that encompasses the ability to understand the special characteristics of media, the ability to perceive the intention of the media originator, and the ability to communicate through media.

(KISA), IPA will invite slogans and posters for raising awareness on information security measures among elementary, junior high and senior high school students nationwide, and publish the selected works.

c) Implementation of e-Net Caravan (Ministry of Internal Affairs and Communications, and Ministry of Education, Culture, Sports, Science and Technology)

In continuation from FY2008, a course for educating on the safe and secure use of the Internet, mainly targeting guardians and teaching staff will be conducted nationwide in liaison with telecommunication related organizations.

B) Information Ethics Education at Schools and Local Communities

a) Development of Advanced Security Human Resources from among the Young Generation (Ministry of Economy, Trade and Industry)

In FY2009, the government will organize training camps for the young generation for practical courses with technical experts engaged in the frontiers of industry as instructors towards raising security awareness as well as discovering and developing talented security human resources. The government will also hold one-day seminars throughout the country to disseminate the results/contents of the courses.

b) Nationwide Information Security Education (Ministry of Economy, Trade and Industry, and National Police Agency)

In continuation from FY2008, the government will hold “Internet Safety Classes” throughout the country for disseminating basic knowledge related to information security to general users, and the “National Council for Internet Safety Classes” for the nongovernmental organizations that conduct the safety classes in order for them to share and coordinate the information to be given.

c) Seminars for Cyber Security (National Police Agency)

In continuation from FY2008, the competent agency will organize throughout the country lectures with the current situation of cybercrimes and actual cases for educators, local government employees, and general users of the Internet in order to raise awareness/knowledge related to information security.

C) Appropriate Distribution of Risk and Countermeasures Information and Promotion of Incident Response Actions

a) Distribution of Tools for Learning/Verifying Web Vulnerability (Ministry of

Economy, Trade and Industry)

In order to support self-learning of the necessity of vulnerability countermeasures and the countermeasures by Web site operators and product developers, the government will start developing experience-based tools for learning about/verifying vulnerabilities.

b) Distribution of Tools to Support Collection of Information Security Related Information (Ministry of Economy, Trade and Industry)

The government will continue to provide the “Latest Security Information Navi (Security Information RSS portal)” that collects and accumulates RSSs related to information security sent from major Web news sites in order to support collection of information security countermeasure information through the Web and the like.

c) Collection and Distribution of Malicious Sites Information through Proactive Actions (Ministry of Economy, Trade and Industry)

The government will operate a system that automatically accesses Web sites on the Internet, collects and analyzes malware, and accumulates the results of the analyses (TIPS) for distribution to the general user.

In addition, as a countermeasure against zero-day attacks, the government will start developing a tool for automatically detecting zero-day attacks based on the analysis of the threat from the exploit code.

(b) Effective Dissemination and Enlightenment Activities for Raising Individuals’ Security Level

Dissemination and enlightenment activities for raising individuals’ security level will be further promoted in liaison with the concerned government agencies in order to achieve better results. Also, in order to effectively increase the security level of general users including individuals who are not necessarily well-versed in IT, the development of supporters that can provide appropriate advice to queries and deal with questions will be promoted, as well as the implementation of local organization networks.

[Specific Measures]

A) Continuous Nationwide PR and Publicity

a) Promotion of Dissemination and Enlightenment Activities Related to Information Security (Cabinet Secretariat, National Police Agency, Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

In order to improve people's information security awareness, in FY2009, appropriate information will be provided to each person through “@police”,

“information security site for the people”, “internet safety classes”, “Council of Anti-Phishing Japan”, “anti-phishing promotion liaison council”, and others in consideration of the rapidly increasing sophistication and complexity of the information security threats.

Furthermore, these efforts will focus not only on IT beginners, but also on active IT users who are not too concerned with information security.

b) Enlightenment Regarding Protection from Unauthorized Computer Access, and Dissemination of Knowledge (National Police Agency, Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

In continuation from FY2008, and based on the Unauthorized Computer Access Law, the government will promote dissemination of knowledge and enlightenment related to protection against unauthorized access through efforts such as the disclosure of occurrences of unauthorized computer access as well as the state of R&D related to access control functions.

c) Promotion of Preventive Measures against Cybercrime (National Police Agency)

In FY2009, the competent agency will produce pamphlets for the prevention of cybercrime and leaflets targeting junior and senior high school students for the prevention of crime on online dating sites which will be distributed by the respective local police. And so, the competent agency will promote PR and enlightenment activities by publishing countermeasures in response to troubles or cybercrime methods on the National Police Agency's web sites.

d) Reinforcement of Dissemination and Enlightenment Activities for Maintaining Radiowave Usage Discipline (Ministry of Internal Affairs and Communications)

During the radio wave protection period in June of 2009, dissemination and enlightenment are scheduled to be implemented on various media (such as national newspapers, local newspapers, industrial magazines, TV ads, train/bus ads, posters at local public organizations and relevant institutions, distribution of leaflets, and ads in PR bulletins) in order to disseminate the importance of radiowave usage rules such as by making people check the “technical conformity mark” with the catchphrase of “Let's obey the radiowave rules”, with the cooperation of the concerned government agencies.

In addition, to the dissemination and enlightenment for stores selling devices that use radio waves that will take place during May to July and September to

November of 2009, the telecommunication bureaus and offices will, in June, implement internet banner advertising with regard to the checking of “technical conformity mark.”

e) Enlightenment Activities Based on “Slogans for the Safe and Secure Use of Infocom” (Ministry of Internal Affairs and Communications)

In continuation from last year, the “Council for the Promotion of Safe and Secure Information and Communication” will invite “slogans for the safe and secure use of infocom”, and to select and give awards for works including best work (the Minister of Internal Affairs and Communications Award).

f) Security Measures for Wireless LAN (Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

In FY2009, the government will continue dissemination and enlightenment activities for general users with regard to wireless LAN security measures through the guidelines entitled “Guide for Safe Use of Wireless LAN” for wireless LAN security, and through the “Internet Safety Classes.”

g) Nationwide Information Security Education (Ministry of Economy, Trade and Industry, and the National Police Agency) [Reprise: refer to Chapter 3, Section 1(1)[4](a)B)b)]

In continuation from FY2008, the government will hold “Internet Safety Classes” throughout the country for disseminating basic knowledge related to information security to general users, and the “National Council for Internet Safety Classes” for the nongovernmental organizations that conduct the safety classes in order for them to share and coordinate the information to be given.

h) Implementation of e-Net Caravan (Ministry of Internal Affairs and Communications, and Ministry of Education, Culture, Sports, Science and Technology) [Reprise: refer to Chapter 3, Section 1(1)[4](a)A)c)]

In continuation from FY2008, a course for educating on the safe and secure use of the Internet, mainly targeting guardians and teaching staff, will be conducted nationwide in liaison with telecommunication related organizations.

i) Development of Information Security Supporters [Reprise: refer to Chapter 3, Section 1(1)[3](c)D)]

The government will make its efforts to rise the standard of information security of all the population by supporting materials, seminars, and certificate

tests concerning information security to develop well acquainted people (information security supporter) among users.

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)

The awareness of the people with regard to information security should be fostered, and in keeping with the purpose of the “Information Security Day” on February 2 each year, the government holds PR and enlightenment events throughout the country.

In conjunction with this day, the government awards individuals and organizations with particularly prominent achievements and meritorious contributions with regard to tackling information security.

C) Establishment of Mechanism to Arouse Public Opinion and Distribution of Information on a Daily Basis

a) Continuous Issuance of NISC Email Magazine (Cabinet Secretariat)

In order to arouse public opinion and provide information pertaining to information security on a daily basis to the people, the government will continue to issue the email magazine approximately once a month in FY2009.

b) Announcement of Award of the Information Security Promotion Category of the Information Promotion Contribution Award (Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

During the Information Month in FY2009, the government will hold the “Information Promotion Contribution Award (information security promotion category)” to award accomplishments of individuals and enterprises that greatly contributed toward ensuring information security.

D) Dissemination of Japan’s Information Security Strategy to Inside and Outside of the Country

a) Dissemination of Japan’s Information Security Strategy to Inside and Outside of the Country (Cabinet Secretariat)

Japan's information security strategy will be proactively made known to both inside and outside the country through the use of PR and educational media such as websites and publicity materials.

Specifically, the English version of “SJ 2009” will be posted to the English website of the NISC during FY2009.

(c) Efforts toward Improving the Information Security Level Including Individuals Who Are Difficult to Deal with

It is essential to make efforts through organizations for countermeasure support in order to improve the information security level including individuals who are difficult to deal with such as those who take no measures even they are aware of the need for measures. Therefore, enhancement of anti-spam measures and the use of information security measures implemented by telecommunication carriers as preventive measures must be promoted.

[Specific Measures]

A) Establishment of a Framework toward Shutting down Cyber Attacks (Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

The government will experiment and study from the technical and measure point-of-view measures for preventing infections by computer viruses (bot programs) that mount cyber attacks through remote operations by malicious third parties as well as measures for shutting down spam emails and cyber attacks from computers infected by bot programs promptly and effectively, with the objective of setting up a comprehensive framework that enables individuals to respond without being burdened by FY2010.

In addition, the government will exchange required information with related overseas organizations with regard to Japan's efforts.

B) Proving Test for the System that Avoids Accessing Hazardous Web Sites such as Malware Distribution Sites (Ministry of Internal Affairs and Communications)

Cases exist in which individuals using the Internet getting infected by bots not only become victims but also perpetrators unknowingly, causing harm to others. Therefore, the government in liaison with telecommunication carriers will carry out a proving test of mechanisms that prevent users from accessing malicious sites distributing malware.

C) Implementation of e-Net Caravan (Ministry of Internal Affairs and Communications, and Ministry of Education, Culture, Sports, Science and Technology) [Reprise: refer to Chapter 3, Section 1(1)[4](a)A)c)]

In continuation from FY2008, a course for educating on the safe and secure use of the Internet, mainly targeting guardians and teaching staff, will be conducted nationwide in liaison with telecommunication related organizations.

D) Enhancement of Anti-Spam Measures (Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry) [Reprise: refer to Chapter 3, Section 1(1)[3](b)M)]

In order to take measures against growing spam e-mails which are increasingly skillful and malicious, the government will steadily enforce the Act on Regulation of Transmission of Specified Electronic Mail, to which an opt-in system has been introduced under a change in the law in 2008, and the Act on Specified Commercial Transactions.

The government will also promote implementation of effective technologies for preventing spam e-mail transmission such as port 25 blocking and sender domain authentication in collaboration with industrial associations such as the JEAG (Japan Email Anti-Abuse Group) founded under an initiative of major Internet service providers and mobile phone service providers in Japan.

However, a large part of spam e-mails received in Japan are transmitted from overseas. The government will also reinforce liaison with overseas authorities in charge of spam e-mail measures as well as promote international spam e-mail measures in private sectors

In addition, the government will continue to promote the “Project for Eliminating Unsolicited E-mail” (since February 2005) which notifies information on illegal spam e-mail to the Internet Service Provider which was used to transmit such e-mail and requests them to take an action such as usage suspension.

(2) Enhancement and Expansion of Inter-Sectoral Information Security Infrastructure

[1] Promotion of Information Security Technology Strategy

With the aim of setting up a system that can proceed in the most effective and efficient manner in the world for the R&D of technologies related to Japan's information security, the government will prioritize the following measures in FY2009.

(a) Maintenance of Priority and Diversity in the Development of Information Security Technology

The government will prioritize researches and technological developments with the aim of enhancing IT as an infrastructure and realizing an environment where IT can be used safely by the people. As the economic environment becomes increasingly severe, IT is expected, more than ever, to be used not only for improving productivity but for promoting researches and technical developments that seek to secure a leading as well as advantageous position in the

field well into the future. Specifically, the government will prioritize the provision of a safe and secure equipment and user environment that do not overburden the users with information security measures to take as they are embedded in advance.

On the other hand, in order to ensure diversity in research and technical development, the government will be actively involved in fields that should be strategically maintained for the country, such as fields skipped by enterprises due to lack of market growth and advanced development for overcoming future risks, fields with enormous development costs, and basic research.

[Specific Measures]

A) Policy on Mid- and Long-term Research and Technology Development

a) Promotion of Research and Technology Development for 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)

For the mid- and long-term objectives that are directly connected to the enhancement of IT as an infrastructure, the government will study measures for priority investment of public research funds in continuation from FY2008.

b) R&D on Secure Cloud Networking Technologies (Ministry of Internal Affairs and Communications)

In order to establish leading technologies that will make it possible for anyone to use highly safe and secure cloud services by FY2013, the government will carry out R&D on secure cloud networking technologies to link different clouds as well as actively use NGN.

c) R&D Related to Next-generation Backbone (Ministry of Internal Affairs and Communications)

In order to establish technologies that will enable safe operations on the entire IP Backbone[18] by detecting and controlling abnormal traffic not seen in normal network operations by FY2009, the government will promote R&D related to next-generation backbone.

d) R&D Related to Detection, Recovery, and Prevention of Route Hijacking (Ministry of Internal Affairs and Communications)

Besides establishing technologies that will enable detection and recovery of route hijacking within several minutes by FY2009, the government will continue

[18] "IP backbone" generally refers to communication trunk lines that are based on Internet Protocol and mutually connect the relay facilities of telecommunication carriers.

to promote R&D related to detection, recovery, and prevention of route hijacking in FY2009 in order to establish technologies that will be able to prevent the occurrence of route hijacking.

e) R&D Related to Information Security Technologies in the Infocom Field (Ministry of Internal Affairs and Communications)

Based on the five-year plan commenced in FY2006, the government will carry out R&D on comprehensive technologies for the protection of information security by combining technologies that protect the safety and reliability of the network itself and the information flowing through the network with technologies that allow immediate and accurate access to information on disaster prevention and alleviation without being cut off even during a large-scale disaster.

f) R&D on New-generation Information Security Technologies (Ministry of Economy, Trade and Industry)

With information technology becoming a social infrastructure, incidents brought about by the information system create conditions that can totally paralyze economic activities or increase risks, affecting people's lives and properties. Therefore, in FY2009, the government will develop technology to counter zero-day vulnerability, research on the possibility of applying formal methods aimed at detecting vulnerabilities at the development stage, and develop technology to detect the vulnerabilities of embedded systems as R&D of new-generation information security technologies aimed at solving issues fundamentally rather than applying symptomatic therapy.

g) R&D of Technologies to Counter Information Leakage (Ministry of Internal Affairs and Communications)

In order to establish technologies to minimize the damage resulting from information leakage caused by the use of file sharing software which is difficult to be tackled through user's own effort by end of FY2009, the government will carry out R&D concerning the detection of information leaking through the network and automatically stopping the flow as well as R&D related to advanced and simplified management of the history and origin of information in continuation from FY2008.

h) Assurance of the Safety of Information Processing Infrastructure (Study on Usage of Malware Samples) (Ministry of Economy, Trade and Industry)

The government will study the usage of the malware samples and sample

analysis results kept by IPA.

i) R&D Related to Sophistication of the Safety Verification Technology for Infocom Components (Ministry of Internal Affairs and Communications)

In continuation from FY2008, the government will study on the R&D regarding technologies aimed at improving the accuracy of safety verification for the functions and devices that make up an infocom network.

j) Preparation of a Security Assessment System for System LSI (Ministry of Economy, Trade and Industry) [Reprise: refer to Chapter 3, Section 1(1)[3](b)G)]

The government will prepare the system required for ISO/IEC 15408 compliance security assessment within Japan to assess system LSIs used on IC cards by FY2011.

k) R&D Related to New-generation Network Infrastructure Technology (Ministry of Internal Affairs and Communications)

Aiming for materialization at around 2020, the government will promote R&D on new-generation network infrastructure technologies that can flexibly ensure optimal quality and security in response to the varied and diverse needs of users by overcoming the limits of the IP network. In 2009, in continuation from 2008, the government will carry out conceptual design of the new-generation network architecture besides developing key technologies for dynamic networks.

l) Preparation of a Green and Secure Cloud Computing Environment (Ministry of Economy, Trade and Industry)

The government will carry out R&D on technologies related to energy saving in cloud computing as well as reliability improvements that ensure secure and stable operations in business settings, such as enterprise and government agencies where users can safely and securely use highly efficient and highly reliable information systems that can be flexibly scaled to meet the management or business strategy.

m) Development and Publicity of Software Structure Status Visualization Technologies (Ministry of Education, Culture, Sports, Science and Technology)

In order to implement a safe and secure IT society of the highest standard in the world by disseminating the software traceability concept as a way of

enhancing the ability to deal with an “Accidents Assumed Society”, the government will develop by March 2012 technologies that add a “software tag” to software products to allow management/verification by the software ordering party so as to determine whether the software development is carried out in the proper steps through collection of empirical data related to software development from multivendors inclusive of those located offshore.

B) Short-term Research and Technological Development Policy

a) Improvement of the Investment Balance in Research and Technological Development with Short-term Targets (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 researches and technological developments with short-term targets such as improvement to existing technologies and development of operational technologies, the government will obtain the progress of the activities made by the public and private sectors and will study suitable methods for analyzing investment portfolios so as to avoid under-investment or over-investment in various areas.

b) Assessment and Improvement of Next Generation OS Environment to Achieve Advanced Security Functions (Cabinet Secretariat, Cabinet Office, Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry) [Reprise: refer to Chapter 3, Section 1(1)[1](b)F)]

The development of “Secure VM” prototype was completed in FY2008. The government will carry out a trial in the Cabinet Secretariat and a proving test on the assumption of its use in government agencies to summarize issues in the actual operation. Also, the government will effort to improve performance and expand the deployment environment of Secure VM through cooperation among industry, academia and government.

c) Promotion of Sophistication of Critical Communications in IP Networks (Ministry of Internal Affairs and Communications)

In order to protect critical communications over the IP network in times of disaster, and based on the “Research Council for the Proper Advancement of Critical Communications” report (May 2008), the government will study with the relevant providers the information that must be shared as well as the common issues in the handling of critical communications, and implement the required

policy.

d) Development of Innovative Virtualization Technology Incorporating a Mechanism that Consolidates and Centrally Manages Information Access Rights (Ministry of Economy, Trade and Industry)

The development of innovative virtualization technology (Secure Platform) that not only consolidates a number of different information systems onto a single server, but incorporates a mechanism that consolidates and centrally manages information access rights that hitherto have been set up separately for each information system has been carried out since FY2007. The government will continue the development into the final year in FY2009 based on the results so far.

C) Study toward Enhancing Investments in Embryonic R&D

a) Formulation of Basic Policies regarding Embryonic R&D (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 entrusting the fields of technology development carried out in the private sector to the initiatives of the private sector, analysis is required in relation to portfolios such as investment of public funds to embryonic research that lacks private sector involvement. In FY2009, the government will review the methods for improving the accuracy of effectiveness against investments for technological development fields in particular.

(b) Promotion of "Grand Challenge Type" Research and Technological Development

With regard to information security measures, there are issues with inadequate measures though urgent response is required, and issues that demand radical technological innovations from a mid- to long-term viewpoint. In order to address these issues, the government will promote "grand challenge type" research and technological development.

For the resolution of pressing issues, prompt response will be planned by integrating and installing key technologies. In addition, there are cases where the achievements of technology developments are not utilized due to reasons such as systems and training having fallen behind even though the development had been completed. In these cases, it is effective to promote an integral measure in parallel with the sophistication of organization/people management methods and user enlightenment.

In order to promote mid- and long-term R&D, the exploration of themes for the R&D as well as technological development will be carried out by predicting the image of a future society and investigating the required information security technologies. Specifically, it is desirable to have a mid- to long-term vision and implementation system, as well as support

environment because the establishment of methods to construct a product embedded with security from the design stage and the accumulation of development know-how cannot be realized over the short term and sizeable knowledge is required to be gained.

[Specific Measures]

A) Study of "Grand Challenge Type" Themes and Promotion Framework (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 cooperation with the Council for Science and Technology Policy and the Information Security Policy Council, the government will study the framework for promoting more detailed themes of projects and grand challenge type researches.

(c) Preparation of the Structure and Infrastructure of an Efficient Implementation System for Research and Technological Development

For a project supported by the country, the project contents and implementation conditions will be publicly disclosed besides incorporating the procedure (process) for using the result obtained halfway through the project at the planning phase of the research and technological development in order to maximize the investment effectiveness. In addition, in the midst of drastic changes to the environment surrounding information security, the effects of changes in social conditions and technological innovation will be evaluated, a flexible project management mechanism that allows changes to plans where necessary will be introduced, enabling prompt response to new threats.

In addition to direct efforts of research and technological development, the maintenance of the environment for R&D support will be actively promoted through cooperation between the public and private sectors in view of the peculiarity of the information security field. Specifically, R&D will be supported and speeded up based on the standardization of the risk description and evaluation methods, the preparation and sharing of database related to information security, and the setting up of a separate workbench[19].

[Specific Measures]

A) Understanding and Continual Review of Implementation Conditions (Cabinet Secretariat and Cabinet Office)

The Information Security Policy Council, in cooperation with the Council for Science and Technology Policy, will assess the implementation conditions of the research and technological development related to information security of Japan through industry-academia-government in continuation from FY2008.

B) Introduction of Continual Assessment Process for Investment Effectiveness

[19] An experimental arrangement simulating the network environment in order for research to be carried out by actually letting malware to work. The malware is isolated from the actual Internet and physically confined.

(Cabinet Secretariat and Cabinet Office)

The Information Security Policy Council, in cooperation with the Council for Science and Technology Policy, will implement the following assessments 1) ex-ante, 2) mid-term, and 3) ex-post at each stage with regard to the investment effectiveness of the research and technological development related to information security technology in continuation from FY2008, and the results will be promptly disclosed to the public.

C) Study of Project Management/Assessment in a Competitive Public Funding System (Cabinet Secretariat, Cabinet Office, and Concerned Government Agencies)

For R&D projects, considerations will be given toward improving the system for promoting the use of mid-term results of R&D besides allowing a flexible change of plan in response to new changes of conditions during the development period.

D) Study on Policy on the Use of Results in Government Procurement (Cabinet Secretariat, and all government departments)

The policy for the government to have the greatest possible direct use of the outcomes of research and technological development through procurement will continue to be studied in FY2009.

E) Setting up of Minimal Attack Reproduction Testbed and Malware Isolation Analysis Testbed (Ministry of Internal Affairs and Communications)

Testbeds for shedding light on cyber attacks and verification of countermeasure technologies will be built, and sophistication of analytic ability/countermeasure technologies against increasingly sophisticated cyber attacks/malware will be promoted.

[2] Development and Assignment of Information Security Human Resources

In order to gather talented people into information security fields regardless of private or public sector so as to make the business attractive through adequate recognition of the importance of information security human resources by society, the government will prioritize the following policies in FY2009.

(a) Human Resource Development and Assignment in Government Agencies and Raising of Personnel Awareness (Reprise)

The government will examine and verify information security related tasks in government agencies and summarize the skills required for the personnel involved in these tasks.

Based on the identified skills, each government agency will create specific plans for training and assignment of internal human resources involved in information security measures to compile the “Guidelines for Human Resource Development/Securement in IT” in accordance with the “Guidelines for Human Resource Development/Securement in IT at Administrative Agencies.”

Also, each government agency will actively employ private sector security specialists in strategic outsourcing to secure the chief information security adviser and support staff by making use of systems such as fixed-term contract.

Each government agency will promote awareness of information security for all officials including management in collaboration with the Personnel and Information System Departments such as including information security in staff training as well as promoting public and private sectors personnel exchange system.

[Specific Measures]

A) Enhancement of Training Programs for Government Officials (Cabinet Secretariat, and Ministry of Internal Affairs and Communications) [Reprise: refer to Chapter 3, Section 1(1)[1](a)2)A)]

The Cabinet Secretariat and the Ministry of Internal Affairs and Communications will improve the quality of the government's standard training programs for government officials (general staff, management, and staff in charge of information security measures).

B) Examination of Information Security Related Tasks (Cabinet Secretariat) [Reprise: refer to Chapter 3, Section 1(1)[1](a)2)B)]

The Cabinet Secretariat will examine and verify information security related tasks in government agencies and summarize the skills required for the human resources involved in these tasks.

C) Execution of the Guidelines for Human Resource Development/Securement in IT (All Government Agencies) [Reprise: refer to Chapter 3, Section 1(1)[1](a)2)C)]

In order to develop and assign human resources with knowledge and capability including information security to contribute towards the safe and secure use of information systems, each government agency will take actions as described in the “Guidelines for Human Resource Development/Securement in IT” formulated based on the “Guidelines for Human Resource Development/Securement in IT at Administrative Agencies” (decided by the Chief Information Officer (CIO)

Council on April 13, 2007).

D) Employment of Private Sector Specialists (All Government Agencies) [Reprise: refer to Chapter 3, Section 1(1)[1](a)2)D)]

Each government agency will actively employ private sector security specialists in strategic outsourcing to secure the chief information security advisor and support staff by making use of systems such as fixed-term contract.

E) Human Resource Development for Government Officials (All Government Agencies) [Reprise: refer to Chapter 3, Section 1(1)[1](a)2)E)]

Each government agency will promote awareness of information security for all officials including management in collaboration with the Personnel and Information System Departments such as by including information security in staff training as well as promoting public and private sectors personnel exchange system.

F) Improving the Evaluation Technologies for Information Systems and Cryptographic Modules (Ministry of Economy, Trade and Industry)

IPA, in order to set up a safety assessment system using security LSI and deal with standards related to next-generation cryptographic module testing, will develop human resources capable of assessing tamper resistance including side channel attacks against security LSI.

(b) Development and Assignment of Information Security Human Resources in Enterprises (Reprise)

Development and assignment of information security human resources are essential in enterprises as well as improving awareness of information security measures in management. The government will widely promote PR and dissemination by holding seminars on human resource development. In terms of measures, it is essential to foster and maintain human resources who can flexibly handle environmental changes such as new IT services, or human resources who are capable of making decisions based on a broad view of the entire enterprise management. In such a case, it is also important to consider the career path the information security human resource can aim for. Therefore, the government will encourage development of a common career skill framework to establish skill standards as an objective human resource assessment mechanism by the joint effort of public and private sectors. The government will also promote the use of the Information-Technology Engineers Examination, and frameworks and qualification tests concerning human resource development in private sectors which are compliant with the above mentioned common career skill framework. In addition, the government will also prepare a system to establish curriculums for advanced information security human resource development, teacher training, and internship programs through industry and academia cooperation.

The government will make its efforts to develop and assign human resources who will play the central role in corporate information security through development of a model career development plan concerning information security for engineers and support for experts'

communities.

In addition, the government will promote development of human resources who can handle migration to a new environment, such as the forthcoming NGN/IPv6 migration, who is observant to laws and regulations, and who can take information security measures with a clear understanding of risks concerning information assets and business continuity.

[Specific Measures]

A) Support System for Information Communication Human Resource Seminars (Ministry of Internal Affairs and Communications) [Reprise: refer to Chapter 3, Section 1(1)[3](c)H)]

The government will continue to support training activities to develop human resources for telecommunications, including those with specialist knowledge and expertise in information communication security in FY2009

B) Development of Information Security Supporters (Ministry of Internal Affairs and Communications) [Reprise: refer to Chapter 3, Section 1(1)[3](c)D)]

The government will make its efforts to rise the standard of information security of all the population by supporting materials, seminars, and certificate tests concerning information security to develop well acquainted people (information security supporter) among users.

C) Leading IT Expert Development Promotion Program (Ministry of Education, Culture, Sports, Science and Technology)

In FY2009, the government will support the establishment of centers in graduate schools through industry-academia cooperation to develop and implement programs for developing highly qualified information security human resources for creating an environment that allows people to use IT safely and securely.

In addition, with regard to the results obtained through development and implementation of varied education programs at each center, the government will support activities for a more effective and efficient deployment and establishment as well as for the task of further improvement of the learning materials.

D) Development of Human Resources for Information Security Audit (Ministry of Economy, Trade and Industry) [Reprise: refer to Chapter 3, Section 1(1)[3](c)C)]

The government will make its efforts to develop human resources for information security audits who are able to assess information security measures both from the inside and outside of the organization as well as objectively and

impartially.

E) Further Spread of the Information Technology Engineers Examination (Ministry of Economy, Trade and Industry) [Reprise: refer to Chapter 3, Section 1(1)[3](c)E)]

In order to enhance the development of advanced IT human resources, including those in information security, the government will review the Information-Technology Engineers Examination which measures skills of information human resources according to the common career skill framework, and reintroduce the examination in FY2009. The government plans to make good use of this examination to produce successful candidates since an effective career path will be created by the appropriate human resource assessment method based on the common career skill framework.

F) Model Career Development Planning (Ministry of Economy, Trade and Industry) [Reprise: refer to Chapter 3, Section 1(1)[3](c)J)]

In order to develop advanced IT human resources including those in information security, it is important for students and young engineers to be able to imagine their own career path; however, career paths in the IT industry are not as clear as those in other industries. Therefore, the government will develop and publicize a model career path for each function with assistance of experts' communities.

G) IT Human Resource Development by Industry-Academia Cooperation (Ministry of Economy, Trade and Industry) [Reprise: refer to Chapter 3, Section 1(1)[3](c)G)]

In order to develop advanced IT human resources including those in information security, the government promotes industry-academia cooperation to endorse teachers with an industrial background, develop and make use of practical materials and curriculums, and promote practical internship through industry-academia matching.

H) Promotion of Information Security Measures in Small and Medium Enterprises (Ministry of Economy, Trade and Industry) [Reprise: refer to Chapter 3, Section 1(1)[3](c)A)]

The government will hold the “Small and Medium Enterprise Information Security Leader Training” to educate leaders in small and medium enterprises, and encourage them to spread information security to the management.

I) Information Security Seminars for Small and Medium Enterprises (Ministry of Economy, Trade and Industry) [Reprise: refer to Chapter 3, Section 1(1)[3](c)B)]

The IPA and Chamber of Commerce and Industry will hold the “Information Security Seminar” in various parts of Japan to nurture understanding of information security among management and information system staff in small and medium enterprises in FY2009. The IPA and Chamber of Commerce and Industry will reinforce liaison with regional core organizations as well as promote PR activities in collaboration with the IT Management Support Group.

J) Dissemination of Private Sector Security Qualifications (Cabinet Secretariat, Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry) [Reprise: refer to Chapter 3, Section 1(1)[3](c)F)]

The government will publicize information on private sector qualifications concerning information security to further develop information security experts in the private sector.

(c) Promotion of the Visualization of Skills Possessed by Information Security Human Resources

In order to recruit human resources in the information security field, and build information security supported by highly capable human resources, it is effective, from the long-term perspective, to link the self-improvement of ability of the information security human resources to the job and make it possible for them to paint their own career path.

For this reason, the government, besides clarifying the skills demanded in actual jobs, will implement policies for making it easy for outsiders to understand the skills possessed by the human resources. For example, it is possible to put forth the efforts to build a mechanism capable of externally showing the possessed skills through the use of efforts for making it easy to visualize the relation between the information security qualification system/education system and the skills demanded by the job or the career path targeted by the information security human resources, as well as through the use of the Common Career/Skill Framework: ITSS[20] or the various types of effective frameworks available in the private sector's human resource development.

[Specific Measures]

A) Dissemination of the Common Career/Skill Framework (Ministry of Economy, Trade and Industry)

In the Industrial Structure Council's Information Economy Subcommittee's Information Services/Software Subcommittee's Human Resource Development Working Group report (July 20, 2007), setting up of an objective advanced IT

[20] Abbreviation for IT Skill Standards (Information Technology Skill Standards).

engineer evaluation mechanism was proposed, the coordination of user skills standard, embedded skills standard and IT skills standard which are systematic evaluation methods for IT engineers was planned in October 2008, and the "Common Career/Skill Framework" conforming to the Information Technology Engineers Examination was set up. Hereafter, the nurturing of advanced security human resources will be sought through the facilitation of further popularization of the framework.

B) Further Popularizing of the Information Technology Engineers Examination (Ministry of Economy, Trade and Industry) [Reprise: refer to Chapter 3, Section 1(1)[3](c)E)]

In order to enhance the nurturing of advanced IT human resources inclusive of information security human resources, a review based on the Common Career/Skill Framework with regard to the Information Technology Engineers Examination that measures the human resource skills of various types of information fields including the information security field will be implemented from FY2009. Based on the large number of people having passed the test, the formation of an effective career path through appropriate human resource evaluation methods based on the Common Career/Skill Framework is awaited, and human resource development utilizing the test will be planned.

C) Model Career Development Planning (Ministry of Economy, Trade and Industry) [Reprise: refer to Chapter 3, Section 1(1)[3](c)J)]

In order to develop advanced IT human resources including those in information security, it is important for students and young engineers to be able to imagine their own career path; however, career paths in the IT industry are not as clear as those in other industries. Therefore, the government will develop and publicize a model career path for each function with assistance of experts' communities.

D) IT Human Resource Development Task with Industry-academia Cooperation (Ministry of Economy, Trade and Industry) [Reprise: refer to Chapter 3, Section 1(1)[3](c)G)]

In order to nurture advanced IT human resources inclusive of information security human resources, the industry-academia cooperation system for the promotion of practical internship through filling/reinforcement of teaching staff from industry, development/dissemination of practical teaching materials/curriculum, and industry-academia matching will be shored up.

E) Publicizing the Private Sector Security Qualifications (Cabinet Secretariat, Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry) [Reprise: refer to Chapter 3, Section 1(1)[3](c)F)]

The qualifications related to private sector information security will be publicized from the viewpoint of perfecting the information security professionals in the private sector.

[3] Promotion of International Liaison and Cooperation

With the objective of contributing to the world with Japan's efforts centered on public and private sector cooperation as the world's most up-to-date and advanced best practice, the government will prioritize the following policies in FY2009.

(a) Enhancement of POC Functions Related to Information Security Policies and Promotion of Information Sharing

Following the First National Strategy, NISC will continue with efforts to clarify the roles as POC that handles inter-sectoral information security policies and will aim to enhance the functions.

Specifically, the efforts will be made from three points of view. Firstly, more efforts will be put into understanding and accumulating the latest trends through opportunities such as at international meetings related to information security where discussions are held from various perspectives such as national security, protection of critical information infrastructure, continuity planning for global economic activities, and prevention of cybercrimes. Since for that it is necessary to foster trust and make visible contributions, the function for grasping and collecting international meetings will be enhanced in a inter-sectoral manner. Secondly, the trend information grasped and accumulated through highly-reliable contacts will become meaningful only when appropriately shared with the necessary relevant domestic agencies and parties. Based on this, NISC, as the POC, will proceed with sharing based on appropriate rules with domestic government agencies and will aim to make meaningful contributions to policy making and implementation in government agencies. Thirdly, it will aim to contribute to the world through official announcements via POC on necessary and suitable matters with regard to trends in Japan from the perspective of setting up an environment that allows the safe and secure use of IT globally.

[Specific Measures]

A) Promotion of International Liaison and Cooperation within Multilateral Frameworks (Cabinet Secretariat and Concerned Government Agencies)

Continuing into FY2009 too, the Cabinet Secretariat will actively participate in international meetings of various fields such as the fields involved with national security like ARF (ASEAN Regional Forum), protection of critical information infrastructure like MERIDIAN, incident response like FIRST (Forum for Incident Response and Security Teams), and global economic activities like APEC (Asia-Pacific Economic Cooperation), OECD (Organisation for Economic

Co-operation and Development) and ASEAN (Association of Southeast Asian Nations), make informative announcements as POC function, and will also proactively share information with concerned government agencies as well as various institutions on the results obtained at the meetings.

B) Information Security International Conference (Cabinet Secretariat and Concerned Government Agencies) [Reprise: refer to Chapter 3, Section 1(1)[2](d)C)]

The government will start a campaign for inviting the International Watch and Warning Network (IWWN) Conference which will be attended by experts from critical infrastructure protection teams, emergency response teams, and law enforcement agencies all over the world in preparation for participation in the global scale cyber exercise "Cyber Storm III."

C) Strengthening of Bilateral Dialogues Related to Information Security Policies (Cabinet Secretariat and Concerned Government Agencies)

In order to build close cooperation among the regions with regard to information security policies, discussions will be held toward establishing a new place to exchange information and enhance strategic bilateral cooperation besides holding the Japan-US bilateral meeting on cyber security in FY2009.

(b) Establishment of Public and Private Sector Cooperation for Grasping the Global Trend of Threats, and Promotion of Efficient and Effective International Cooperation Activities

For a safe and secure cyberspace, close international cooperation has been promoted not only by the government but also by major bodies such as the national-level CSIRT, ISPs[21] and various in-house corporate CSIRTs, and research institutions. Under this sort of conditions, the government will concentrate on fields that it can be particularly strong in. In addition, a cooperation system between the public and private sectors will also be built for Japan as a whole to efficiently/effectively proceed with international activities related to information security beginning with the understanding of global trend of threats and the response to incidents. Based on this, the aim is to build a relation between the relevant domestic institutions that already conduct the activities and the complementation and mutual help in international cooperation activities.

In specific, efforts will be made from three points of view. Firstly, the Japanese government's public and private cooperation system will be proactively made known overseas, and the public and private sector division of roles in international cooperation will be clarified. Secondly, domestic cooperation will be reinforced to clarify the information that can be spread by Japan through cooperation between the public and private sectors. Thirdly, in order to accelerate information sharing by improving the trust relationship between the government and non-governmental organizations in the various countries, the concepts involved in international information sharing will be put in order.

[21] Abbreviation for Internet Service Provider.

Moreover, as for the fields that the government can be particularly strong in, besides the opinion exchanges concerning the latest policy trends which have been exchanged with various foreign government institutions, it is possible to mention, for example, the sharing of risk information such as of vulnerabilities and threats targeting mainly to government agencies and critical infrastructure, and the setting up of an international cooperation system for incident response in the fields of government agencies and critical infrastructure. In this case, existing international activities by the relevant agencies should be used to proceed.

[Specific Measures]

A) Enhancement of Liaison with Relevant Domestic Institutions (Cabinet Secretariat)

In order to domestically share and provide information on the international information security policy trends, the government will enhance the liaison with the relevant domestic institutions.

B) Study toward Preparation of International Information Sharing Rules (Cabinet Secretariat and Concerned Government Agencies)

Study on rule-making in relation to information sharing will commence through bilateral dialogues and proactive participation in international frameworks for grasping the global trend of threats.

C) Support for the Strengthening of Overseas CSIRT Systems (Ministry of Economy, Trade and Industry)

The government will support the establishment of overseas CSIRTs in the Asia-Pacific region through JPCERT/CC. In FY2009, JPCERT/CC will provide support such as the sharing of accumulated experience or operational technologies for incident response tasks.

In addition, cooperation will be provided for the improvement of domestic coordination capability in the respective countries so as to enable the provision of prompt and effective incident response by further enhancing the cooperation with each country's CSIRT through activities such as incident response exercise in the Asia-Pacific region as well as the activities of FIRST (Forum of Incident Response and Security Teams), IWWN and APCERT.

In particular, as FIRST meeting will be held in Kyoto in June of FY2009, further strengthening of cooperation with the overseas member teams visiting Japan will be planned by taking advantage of this opportunity.

D) Enhancement of the Information Sharing System in Relation to Network Information Security in Japan, China and South Korea (Ministry of Internal Affairs and Communications)

In continuation into FY2009, the cooperation of the relevant institutions including network operator organizations will be promoted besides enhancing the sharing of information related to each country's basic policies, incident reports and security trend through efforts related to infocom network security protection in Japan, China and Korea.

E) Promotion of Information Sharing between Network Operators in Japan and ASEAN (Ministry of Internal Affairs and Communications)

In FY2009, the knowledge and experience gained through cooperation among the network operators of Japan will be supplied for the network operators of ASEAN countries, and information sharing among the network operators will be facilitated between Japan and ASEAN.

(c) Wisdom Concentration and Improvement of Information Security in Asia (Realizing One-Asia)

The threats such as unauthorized access, phishing, spam, targeted attacks and malware infection through websites can occur beyond the national borders, and at the same time, they also have a certain level of common characteristics in regions that are closely related in terms of geography, culture, and politics. Therefore, as already can be symbolically observed within the European region or regions centered on the US, there has been intra-regional cooperation. Under this sort of conditions, Japan should promote cooperation to enhance information security countermeasures against threats in Asia, and will aim to realize the following efforts.

The efforts will be made from three points of view. Firstly, from the recognition of the need for people links-, professionals and researchers would be proactively trained for understanding and analyzing the trend of threats in Asia together with Japan. Secondly, support will be provided, in a form that will also be greatly advantageous for Japan, to the efforts for establishing a joint capability to understand the trend of threats in Asia which has been discussed in international institutions and international forums. Thirdly, Japan will reinforce the cooperation with US and Europe which was set up during the First National Strategy period, and proactively feed back to the Asian region the lessons and information gleaned through joint efforts and sharing of best practice.

Furthermore, the existing framework will be used up to maximum as well as the cooperation the relevant agencies in order to promote the efforts efficiently.

[Specific Measures]

A) Promotion of Research Cooperation in the Field of Network Security in Japan and ASEAN (Ministry of Internal Affairs and Communications)

In FY2009, discussions will commence between Japan and ASEAN countries regarding research cooperation in the field of network security.

B) Promotion of the Sharing of Early Warning Information in the Asia-Pacific Region (Ministry of Economy, Trade and Industry)

In FY2009, while cooperating with the relevant institutions such as that of the

Asia-Pacific region, JPCERT/CC will begin the transition to actual operations and joint analysis with the participating countries with regard to the setting up of an information sharing system for internet fixed-point observation targeting the same region.

In addition, with regard to the information on threats pertaining to information security and the analysis information pertaining to software vulnerabilities sent to the respective CSIRTs in the Asia-Pacific region on a daily basis since FY2008, expansion of delivery region and bidirectionality will be promoted in FY2009.

C) Enhancement of the Attack Method Analysis Capability in the Asian Region and Promotion of the Sharing of Analysis Results (Ministry of Economy, Trade and Industry)

In order to formulate effective preventive measures against cyber attacks, the techniques and methods used in the attacks as well as their trend and regional characteristics will be analyzed, and then the method of sharing the analysis method and the analysis results studied.

Specifically, in FY2009, the study will be carried out on the joint or cooperative basis among members centered on Asian region's CSIRTs.

D) Efforts for the Improvement of the Information Security Assessment and Authentication Technology in the Asian Region (Ministry of Economy, Trade and Industry)

With IPA as the main body, in order to plan for the improvement of the assessment and authentication technology, and sharing of various types of information in Asia, the Asian IT Security Evaluation and Certification (AISEC) forum will be established by Japan, South Korea, Singapore and Malaysia, and the first meeting will be held in Japan (May 2009).

(d) Protection of Information Security in Response to Globalization of Economic Activities

The government will put in efforts toward setting up a business environment to protect the safety/security of the global economic activities of Japanese enterprises. In other words, the aim is to reliably protect critical information assets at overseas business locations and ensure high business continuity.

Specifically, firstly, the aim is to set up a system implemented with a high level of information security measures at the overseas locations involved in the business activities of Japanese enterprises. Secondly, the aim is to set up a highly reliable network environment with assured availability. Thirdly, the aim is to promote efforts inside and outside the country for ensuring consistent security and reliability throughout the entire supply chain of manufacturing processes in a form that does not hinder globalization with regard to IT products and services. This sort of efforts will contribute to the improvement of the international competitiveness of Japanese products and services which are of high quality even from the perspective of

information security.

The government will proceed with efforts through active participation in international institutions that actively support developing countries/regions besides using such opportunities to hold direct discussions with regions having particularly deep relations.

[Specific Measures]

A) Sound Implementation of the Agreed Details of the ASEAN Japan Information Security Policy Meeting (Cabinet Secretariat, Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

In order to speed up the efforts toward the setting up of secure business environment in Asian regions with deepening economic relations with Japan, the assurance of the reliability of infocom infrastructure that supports economic activities and technology innovations, and the development of cross-sectoral information security policy by the government, efforts will be made toward sound implementation of the agreed details of the first ASEAN Japan Information Security Policy Meeting.

B) Promotion of Implementation of a Secure Business Environment in the Asian Region (Ministry of Economy, Trade and Industry) [Reprise: refer to Chapter 3, Section 1(1)[3](f)A)]

In response to a study on strategies concerning an Asian common information security measure benchmark which was carried out by the ERIA (Economic Research Institute for ASEAN and EAST Asia) in FY2008, and in accordance with the “Asia Knowledge Economy Initiative” proposed by Japan in the ASEAN Economic Ministers Meeting in FY2008, the government will conduct a joint study of the method to promote secure business implementation in the Asian region with researchers from Asian countries, using Japan’s knowledge. The government will also undertake promotion activities such as seminars on enterprises' information security measures in several countries of the Asian region, and human resource development.

C) Secure Coding Seminars in Software Development Outsourcing Countries (Ministry of Economy, Trade and Industry) [Reprise: refer to Chapter 3, Section 1(1)[3](f)B)]

The JPCERT/CC will hold technical seminars on coding techniques that can prevent vulnerabilities in countries where Japanese enterprises are outsourcing embedded software development. Seminars are planned in three countries in the ASEAN region in FY2009.

D) International Deployment of Information Technology Engineers Examination and IT Skill Standards (Ministry of Economy, Trade and Industry)

With regard to the Information Technology Engineers Examination, mutual certification will be carried out with 11 Asian countries/regions. In particular, Japan's Information Technology Engineers Examination system will be introduced, and the IT Professional Examination Council (ITPEC), which is the council for implementing the examination with the cooperation of the countries in which the examination system had been established (Philippines, Vietnam, Thailand, Myanmar, Malaysia, Mongolia), will hold a unified examination for Asia at the same time on the same day. In future, in order for a suitable proficiency evaluation method to be set up by ITPEC in each country for those who passed the examination, the development of security human resources will be further planned in Asia based on the dissemination of Japan's IT skill standards.

(e) Realization of Strategic Contributions by Japan Including Standardization

Unified standard setting and standardization related to information security measures have been carried out by various international institutions. In recent years, the standardization efforts have been made not only in technical fields as in the past, but also in the field of policies. The discussions extend over many branches, and even though limited to the information security fields, it is very difficult for the government to be involved in all the activities from among a wide range of activities. On the other hand, quite a number of relevant organizations including enterprises from Japan have been separately carrying out standardization through continuous participation and contributions.

As international contributions made through international institutions are essential in setting up continual relations with the relevant parties overseas, the government will aim to maintain a system that will allow Japan to make strategic contributions by grasping the trends of standardization and guideline formulations in international institutions while cooperating with the relevant domestic agencies and enterprises that are participating in standardization efforts, and building relations.

[Specific Measures]

A) Enhancement of the Information Security Management in Telecommunication Services (Ministry of Internal Affairs and Communications)

With regard to information security management in the telecommunication field, the guideline (ISM-TG) described in Chapter 3 Section 1(2) was proposed to the International Telecommunication Union (ITU) and the International Organization for Standardization (ISO) from FY2006 through FY2008, and played a leading role in international standardization. In FY2009, contributions will be made toward improving the level of international information security management with efforts in the international standardization of requested items based on the trend of discussions in ITU and ISO.

B) Participation in International Standardization in the Information Security Field (Ministry of Economy, Trade and Industry)

Japan will participate in international meetings under the auspices of ISO/IEC and JTC1/SC27 which are international standardization activities in the information security field, and will proactively take part in the planning so that Japan's IT environment, standards, guidelines and others be reflected in international standards.

(f) Fostering of Information Security Culture

The fostering of information security culture is put forth as one of the objectives even in the First National Strategy. In recent years, awareness has also been raised globally through discussions in international institutions closely related to the fields of information systems and the Internet.

In order to foster a true information security culture, the government, recognizing the necessity of efforts through sharing of understanding at the high level of the governments of the world in a similar manner to the necessity of raising the awareness of corporate management, will aim to make use of the high level opportunities such as that of G8 and APEC while cooperating with governmental institutions of various foreign countries.

By fostering this sort of common understanding, the aim is to set up an environment that can send out messages from high level staff not just for cooperations arising from operations during incidents.

The overview of each type of policy toward the promotion of international liaison and cooperation is shown below.

Field	Regional	Global
Policy	(iii) Improvement of the information security level and wisdom concentration in Asia (realizing One-Asia). (iv) Protection of information security in response to globalization of economic activities	(iv) Protection of information security in response to globalization of economic activities (vi) Fostering the information security culture
Operation	(iii) Improvement of the information security level and wisdom concentration in Asia (realizing One-Asia)	(ii) Establishment of public and private sector cooperation for understand the global trend of threats, and promotion of efficient and effective international cooperation activities
Standardization	(v) Realizing the strategic contributions of Japan including standardization.	

(Note) The measure (i) is not stated here as it is the premise of all policy implementations.

[Specific Measures]

A) Promotion of International Publicity Activities Related to Japan's Information Security Strategy (Cabinet Secretariat)

International publicity activities will be carried out on the basic concept and strategy of the information security policy of Japan as an advanced information security country, the overall government policy, and the functions and positioning

of NISC that shoulders the core. The English version of SJ2009 will be published on the English website of NISC.

B) Bottom-up Support for Developing Countries' Information Security Policy through Multilateral Meetings (Cabinet Secretary and Concerned Government Agencies)

In order to plan for bottom-up approach of information security policy in developing countries, efforts toward support for formulation of basic plans related to national cyber security strategy and critical information infrastructure protection as well as raising international awareness will also be actively pursued in FY2009 and thereafter through opportunities presented by multilateral meetings.

C) Promotion of International Cooperation through ITU-D (Ministry of Internal Affairs and Communications, and Cabinet Secretariat)

In FY2009, support will be provided for the formulation of policies related to the safety of infocom networks in developing countries through the International Telecommunication Union-Telecommunication Development Sector (ITU-D).

D) Holding of APT Training/Seminar (Ministry of Internal Affairs and Communications)

Based on Extra Budgetary Contribution from Japan to the Asia-Pacific Telecommunity (APT), information security training is scheduled to be held in FY2009 for telecommunication carriers and government-related parties of APT-member countries.

E) Efforts for Realization of International Security Culture and Improvement of Awareness/Literacy (Cabinet Secretariat)

Contributions will be made to the fostering of security culture using opportunities inside and outside the country while taking into account the trend of international discussions around the "security culture" defined by the "Guidelines for the Security of Information Systems and Networks" by OECD. At the same time, discussions on policies for the improvement of information security awareness and literacy among various foreign countries will be deepened through the opportunities presented by policy dialogues.

[4] Crime Control and Protection and Redemption of Rights and Interests

With the objective of enabling safe and secure use of cyberspace, the

government will prioritize the following policies in FY2009.

(a) Promotion of Infrastructure Preparedness for Crime Control

Infrastructure enhancement such as reinforcement of the control system in law enforcement institutions, improvement of technical skills, and promotion of international cooperation will be further promoted.

Furthermore, efforts will be promoted toward public and private sector cooperation for building a strong IT society against crimes by further promoting the building of good cooperative relations between the law enforcement institutions and the victims so that it can lead to the arrest of suspects and prevention of the spread of damage providing essential information in identifying the causes and shedding light on the criminal processes.

In addition, preparations will also be enhanced against cyber terrorism through the above-described efforts but by taking into consideration the special characteristics.

[Specific Measures]

A) Enhancement of the Preparedness against Cybercrime (National Police Agency)

In FY2009, the competent agency will enhance the preparedness to appropriately tackle cybercrimes by actively implementing training inside and outside the department for police officers who are engaged in cybercrime investigations and by promoting the maintenance of vehicles for the control of cybercrimes.

B) Promotion of Efforts Regarding Digital Forensics[22] (National Police Agency)

In order to appropriately deal with increasingly varied and complicated cybercrimes, in FY2009, there will be promotion for the enhancement of the systems involved in digital forensics, public and private sector cooperation starting with technical cooperation, and cooperation with relevant domestic institutions such as by holding the digital forensics conferences, improvement and strengthening of equipments, and implementation of training for police officers engaged in cybercrime investigations.

C) Promotion of International Cooperation for Cybercrime Control (National Police Agency)

In FY2009, the building of multilateral cooperative relations will be promoted by holding the Cybercrime Technology Information Network System (CTINS) Annual Conference as well as active participation in international frameworks

22 "Digital forensics" is the general term for the techniques and methods in clarifying the legal evidence by collecting and analyzing devices, data and electronic records required in the investigation of causes and probe when crimes or legal disputes arise in relation to computers such as unauthorized access or leakage of classified information.

involved with cybercrimes such as G8 and ICPO besides implementing effective information exchange with law enforcement institutions of the countries closely related to Japan's cybercrime situation.

D) Promoting Promptness of International Assistance in Investigation by Using Central Authority System[23] (Ministry of Justice)

Bilateral mutual legal assistance agreements, by designating central authorities in each state party to communicate directly for the purpose of execution of international assistance in investigation, can expedite the execution of the international assistance and secure such assistance by making it obligatory in principle. Japan has already concluded such bilateral mutual legal assistance agreements with the United States, Korea and China. In addition, an agreement on mutual legal assistance was signed between Japan and Hong Kong on May 23, 2008. In FY2009, the competent agency will expedite the necessary procedures, such as obtaining early approval of the agreements with Hong Kong and Russia(substantive agreement completed in May 2008) by the Diet, and work on concluding the agreements on mutual legal assistance with the European Union (EU), Brazil and other Asian countries.

E) Promotion of Legislative Measures against Cybercrimes (Ministry of Justice)

Considering the recent situation concerning advanced information processing, the legislative measures against cybercrimes should be promoted in order to conclude the U.N. Convention against Transnational Organized Crime. (The Bill on Partial Amendment to the Penal Codes and Other Acts in response to Globalizing and Organized Crimes and Advanced Information Processing was submitted to the Diet at the 163rd session, and is under consideration.)

F) Reinforcement of Cooperation with the Private Sector for Maintenance of Cyberspace Safety and Discipline (National Police Agency)

In order to reinforce cooperation between public and private sectors for appropriately dealing with cybercrimes, efforts for the set up of Internet Cafe Liaison Councils will be promoted in the respective local police organizations.

G) Promotion of Efforts toward Public and Private Sector Cooperation for Building a Strong IT Society against Crimes (National Police Agency)

The Comprehensive Security Measures Conference which is comprised of

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

experts, related business providers, PTA (Parent-Teacher Association) representatives and others will be held, and discussions will be held on how the cooperation between the government and industry in relation to information security ought to be.

H) Reinforcement of the System against Cyber Terrorism (National Police Agency)

In FY2009, in order to deal with the sophistication of cyber attack methods that are the means of cyber terrorism, reinforcement of the police's counter cyber terrorism system will be promoted such as by enhancing the information collection and analysis system, maintaining the technical capability and ability to deal with cases by cyber terrorism countermeasure personnel, training inside and outside the department for improvement purposes, and increasing the assets for implementing emergency measures.

I) Reinforcement of Public and Private Sector Cooperation against Cyber Terrorism Targeting Critical Infrastructure (National Police Agency)

In FY2009, besides holding enlightenment activities linked to raising the awareness of cyber terrorism countermeasures as necessary based on the special characteristics of the business of critical infrastructure providers, efforts will also be made to contribute to incident response activities during occurrence of cyber terrorism by participating in various exercises and implementing joint exercises while respecting the intentions of critical infrastructure providers.

J) Reinforcement of the Measures to Prevent Interference with Important Radio Communication (Ministry of Internal Affairs and Communications)

Based on 3-year plan of reinforcing and enhancing the radio monitoring system, and in order to enhance the ability to cope with important radio communication interference, the government will reinforce the radio monitoring system including the important radio communications interference notification reception system.

a) To maintain radio wave usage order, radio wave monitoring facilities will be updated/upgraded by remote operations and 16 DEURAS sensor stations will be equipped in FY2009 in the regions where interferences constantly occur.
b) In order to improve the functionality and performance of space radio wave monitoring facilities target of the materialization of uplink interference source identification function. Upgrade and improve the functionality of radio monitoring facilities, studies and research are scheduled to be implemented for broadband monitoring technologies.

(b) Promotion of PR and Enlightenment for the Deterrence of Crime

PR and enlightenment will be further promoted regarding criminal damage situation and methods as well as specific countermeasures so that people will not become victims of cybercrimes.

[Specific Measures]

A) Promotion of Preventive Measures against Cybercrime (National Police Agency) [Reprise: refer to Chapter 3, Section 1(1)[4](b)A)c)]

In FY2009, the competent agency will produce pamphlets for the prevention of cybercrime and leaflets targeting junior and senior high school students for the prevention of crime on online dating sites s which will be distributed by the respective local police. And so, the competent agency will promote PR and enlightenment activities by publishing countermeasures in response to troubles or cybercrime methods on the National Police Agency's web sites.

(B) Promotion of PR and Enlightenment for the Deterrence of Crime (National Police Agency)

In FY2009, PR and enlightenment activities for the deterrence of crime will be promoted through the National Police Agency's security portal site “@police” by providing information related to information security such as vulnerability information of various types of software and information of internet observation from fixed points, appropriately and as situation changes.

C) Enlightenment Regarding Protection from Unauthorized Computer Access, and Dissemination of Knowledge (National Police Agency, Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry) [Reprise: refer to Chapter 3, Section 1(1)[4](b)A)b)]

In continuation from FY2008, and based on the Unauthorized Computer Access Law, the government will promote dissemination of knowledge and enlightenment related to protection against unauthorized access through efforts such as the disclosure of occurrences of unauthorized computer access as well as the state of R&D related to access control functions.

(c) Promotion on the Preparation of Infrastructure for the Protection and Redemption of Rights and Interests

While adequately taking into consideration the people's fundamental human rights, efforts will be put into further preparing an infrastructure for the protection and redemption of rights and interests in the cyberspace. Specifically, efforts will be put into the promotion of disclosure of information related to efforts on the protection and redemption by the

information keeper, and of the rights and interests of the information depositor, and the development and dissemination of technologies that will improve the safety and reliability of the cyberspace.

[Specific Measures]

A) Promotion of Publicity of the Provider Liability Limitation Law and Related Guidelines (Ministry of Internal Affairs and Communications)

Similarly to other cases, the Ministry of Internal Affairs and Communications will support the publicity of the law and related guidelines through the websites of industrial associations.

B) Promotion of Formulation and Publishing of Information Security Report (Ministry of Economy, Trade and Industry)

In order to contribute to the protection of the rights and interests of the people depositing information and promote appropriate information management as well as implementation of measures against information leakage, the government will disclose the efforts on information management and compliance to laws and regulations of the enterprises handling information deposited by the people in a format that is comparatively easy for the people to understand as well as disseminate an information security report model.

Chapter 4: Structure of the Policy Promotion System and Sustainable Improvement

The government should comprehensively deal with the important policies described in the previous chapter in FY2009 under the following system and sustainable structure.

Section 1: Policy Promotion System

(1) Strengthening of the National Information Security Center (NISC) and its Role

NISC will continue to aim for the strengthening of its role as the core for making the promotion system of the entire government function effectively as a system to gather the highest intellects internationally and domestically in the same manner as the efforts under the First National Strategy. In addition, the role as international POC in relation to inter-sectoral information security issues will continue to be enhanced so as to have adequate results.

In addition, NISC will plan to maintain/enhance the capability to flexibly use the human resources in the government up to the maximum besides working on actively using private sector human resources as a great amount of knowledge related to information security is accumulated in the private sector. At the same time, it will also continuously aim to function as the core location for human resources development for government officials.

As it is also clear from the contents of this National Strategy, the information security policy field extends over many branches. For this reason, NISC will take the initiative and put in efforts in order to realize the maximization of problem solving capability of Japan as a whole against issues related to information security by flexibly proceeding with the optimization of the cooperation system of relevant agencies toward resolution on a per issue basis besides becoming a joint with various institutions in charge of related areas.

[Specific Measures]

A) Strengthening of NISC (Cabinet Secretariat)

As it should be the core for the promotion system of the information security measures of the entire government, outstanding talent will be proactively used regardless of public or private sector in order for the personnel system of the NISC to be continuously maintained and the highest intellects gathered.

Under this system, the Standard of Measures and a PDCA cycle based on the Standards of Measures are established as the government agency measures while the policies set forth in Chapter 3 Section 1 (1)[1] “Government Agencies and Local Governments” are implemented to enhance the emergency response capability of the government as a whole. Apart from the measures related to the Standard of Measures and the emergency measures, others are implemented for various needs toward the promotion of information security measures of each government agency aimed at reinforcing the information security of e-Government. With respect to the measures related to the critical infrastructure

field, the policies set forth in Chapter 3 Section 1 (1)[2] are implemented in accordance with the Second Action Plan.

Furthermore, the system and functions of NISC are enhanced for it to be able to act as Japan's international POC with regard to cross-sectoral information security item of the government agencies, and play the role as the international interface trusted by various foreign countries through international communications and information sharing. For this, it is assigned with functions for increasing its recognition as POC, promote the set up of trusted relations with various foreign countries, as well as with functions for acting as the core of cross-sectoral information security measures promotion which enhances the information collection capability and plans for the enhancement of information sharing and analysis functions with relevant agencies.

In addition, it is expanded with functions for carrying out investigations and studies regarding basic information and various trends that are required in the promotion of information security measures.

B) Enhancement of the Information Security Consulting Functions for the Promotion of Information Security Measures of Various Government Agencies (Cabinet Secretariat)

In order to support the promotion of the information security measures of each government agency, NISC will enhance the information security consulting functions by the professionals of the same Center in order to respond to the various needs toward the promotion of information security measures of each government agency such as the measures related to the Standards of Measures, the emergency measures, and the measures for enhancing the information security of e-Government.

(2) Reinforcement of Each Government Agency and Roles

Each government agency will continue to reinforce and enhance the system involved in the information security measures and related fields of its own under the framework for promoting the information security policy through the Information Security Policy Council and NISC at the core. For the reinforcement and enhancement of the system, effective policies will be used in a flexible and maximal manner including the active use of private sector human resources as required. Then, while adequately taking care not to vertically partition the promotion system, efforts will continue to be put into implementing the respective types of policies so that the promotion of a unified and cross-sectoral information security measures is carried out in the public and private sectors.

[Specific Measures]

A) Reinforcement of the System for Information Security Measures and Implementation of Cross-sectoral Efforts of the Government Agencies (All

Government Agencies)

In FY2009, each government agency will continue to reinforce its own information security measures system as well as put in efforts for the cross-sectoral sharing of procedures and results, and unification of measures of the information security measures in the private and public sectors, by cooperating throughout the entire government institution besides enhancing the system of own information security measures.

B) Information Security Analysis and Recommendations (Ministry of Economy, Trade and Industry)

In FY2009, IPA will perform social science analysis and investigate the risks and the human behavior and investment against risks in order to promote information security measures. In addition, IPA will hold joint workshop with related domestic agencies in order to clarify the cost and countermeasure results, as well as the positioning of countermeasure behavior in the social system.

(3) Timely and Appropriate Grasp of Situational Changes and Measures against New Issues

The information security field changes very fast in various aspects such as threats and technologies. For this reason, it is important to promptly and accurately respond to the newly occurring issues besides the timely and appropriate grasping of conditions that change with each moment. In addition, it is also essential to appropriately study new policy making schemes that may become the new trend. Furthermore, it is also necessary to take new measures targeted at information providing organizations.

Thus, the government will reinforce the system for carrying out studies dynamically and flexibly by cooperating with various related agencies and interested parties including NISC, and by using expert councils suitably set up under the Information Security Policy Council, and from the general viewpoint involving law, technology, and enlightenment policies.

[Specific Measures]

A) Study on Coordination of the Information-sharing Scheme and Information Exchange Model of Each Specialty Field (Cabinet Secretariat, Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

The formulation of appropriate measures for dealing with IT failures and cyber attacks that have become advanced these days requires information collection and correlation analysis utilizing diverse expertise as well as coordinated measures according to the objectives and functions of each information-sharing scheme.

For this reason, the roles and coordination of information-sharing schemes of each specialty field such as the “system design field, virus analysis field, CSIRT field, and ISP field” will be properly organized, and the information coordination

and information exchange models (coordination structure design) according to the respective objectives and functions will be studied by the end of March 2010.

Section 2: Relations with Other Relevant Agencies

The Second National Strategy lays out the mid- to long-term strategies that look at Japan's information security issues in its entirety, and the information security policy is broadly related to the people's lifestyles and socioeconomic activities, so its implementation requires cooperation with various relevant agencies in the same manner as for the First National Strategy.

Among the various relevant agencies, the information security policy can be positioned as one of the key IT portions in the relation with the IT Strategic Headquarters, and it is necessary to bear in mind that the Second National Strategy practically shoulders the information security related portions of the "new IT reform strategy." In addition, it is essential to further reinforce the cooperation with the Administrative Management Bureau of the Ministry of Internal Affairs and Communications regarding the efforts related to the administrative information system.

In the relation with the Central Disaster Prevention Council, it is necessary to carry out the required cooperation with regard to critical infrastructure related portions of the information security policy. In addition, in the relation with the Council on Science and Technology Policy, it is necessary to ensure that the entire science and technology policy and the research and technological development related portions of the information security policy should be promoted in a coordinated manner. Furthermore, in the relation with the Quality-of-Life Policy Council, it is necessary to ensure adequate cooperation in proceeding with the efforts involving subjects providing information from the viewpoint of personal information protection.

The Information Security Policy Council and NISC should promote the information security policy with the adequate cooperation from these councils.

[Specific Measures]

A) Reinforcement of the Cooperation with Relevant Agencies (Cabinet Secretariat, and Cabinet Office)

In FY2009, the Information Security Policy Council will promote the information security policy in its entirety for the government as a whole by closely cooperating on the proposal and implementation of various measures besides clarifying the role divisions by closely working with other relevant agencies and councils such as the IT Strategic Headquarters, Council on Economic and Fiscal Policy, and Council for Science and Technology Policy.

In particular, in the relation with the Council for Science and Technology Policy, the research and technological development in the security field will continue to be promoted in FY2009 and thereafter while maintaining cooperation with the NISC based on area-specific promotion strategy (infocom field) during the Third Science and Technology Basic Plan. In addition, with regard to how the information security measures for disaster prevention and reduction ought to be, the critical infrastructure information security policy will be promoted in its

entirety by closely cooperating in the intensification of opinion exchange with other relevant councils such as the Central Disaster Prevention Council.

Section 3: Set up of a Sustainable Improvement Structure

The issues surrounding information security necessitate improvements to be made by constantly assessing policy results as new risk factors occur one after another and change very fast. For this reason, the government uses the structure for sustainable improvements as shown below continuing the efforts under the First National Strategy.

(1) Formulation of “Annual Plan” and Its Assessment

> The government, in seeking to realize the Second National Strategy, besides formulating a more specific policy implementation program each year as the “Annual Plan (Secure Japan 20XX)”, assesses the implementation situation together with the changes in social conditions and publishes the results. In addition, the government implements supplementary surveys as required whose results are also combined and published as the “FY20XX Information Security Policy Assessment.” The details of these efforts should conform to the framework stipulated in the framework document such as the Information Security Policy Assessment.
>
> Furthermore, when it is necessary to lay down a mid- and long-term plan from the viewpoint of smooth policy progression as it involves essential measures by relevant agencies other than the government, multiple-year milestones can be set without adhering to single years.

[Specific Measures]

A) Assessment[24] and Publishing of the Assessment Results (Cabinet Secretariat)

With regard to the situation of efforts of specific implementations described in SJ2009, the assessments, etc. will be carried out at year end besides publishing the progress every half year.

B) Study on the Milestone toward Enhancement of Information Security Measures of Government Agencies (Cabinet Secretariat)

The schedule for regular assessment involving the measures for improving government institution's own information security, the assessment items, and the purport in the choice of assessment items are formulated.

C) Annual Result Verification of Information Security Measures of the Critical Infrastructure Field (Cabinet Secretariat, and Government Agencies in Charge

[24] In this chapter, “Evaluations, supplementary study and analysis based on evaluation index” is written as “evaluations, etc” in accordance with the definition in "1. Operational Policies for Evaluations based on Evaluation Criteria” of the “Evaluations, etc.”, toward Realization of Secure Japan and Promotion of Reasonable and Continuous Improvements” (decided on February 2, 2007 by the Information Security Policy Council).

of Critical Infrastructures)

With regard to the assessment of information security measures of the critical infrastructure field, the result verification of the measures, result verification of the policy, and the supplementary survey will respectively be carried out with the cooperation of the government agencies in charge of critical infrastructures based on the Second Action Plan. In addition, the details shown by an index in the same plan will hereby be collected and published.

(2) Implementation of Efforts toward Emergency Measures Midway through the Fiscal Year

The government, even midway into the implementation of the "annual plan", will implement efforts for responding to emergency situations such as unexpected accidents, disasters and attacks as well as new risk factors.

[Specific Measures]

A) Study on Review of the Plan (Cabinet Secretariat)

In the event of an emergency such as an abrupt change in situation or the occurrence of a large-scale disaster or attack related to information security, suitable efforts will be promptly formulated and carried out even midway into the implementation of this SJ2009.

(3) Improvement of Assessment Index

With regard to the assessment index related to information security used in each field where measures have been implemented are set based on the framework document of the information security policy, and the government will continuously improve[25] the assessment index hereafter based on the methods stipulated in the same framework document.

[Specific Measures]

A) Improvement of the Assessment Index Related to Information Security Measures (Cabinet Secretariat, Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

Based on the assessment index that will be established during FY2009, besides promoting the use of the index, which evaluates the extent of dissemination of information security measures in the respective measure implementation field (government agency, local government, critical infrastructure, enterprise, individual), in international institutions and in the government. Once the assessment results are ready, its improvement can be studied. In addition, as

[25] Moreover, with regard to the critical infrastructure field, as the assessment index in Second Action Plan has been improved in advance, when making improvements to the assessment index in the same framework document, the study should basically be carried out to the evaluation index in the Second Action Plan.

supplementary surveys will also be suitably implemented in the assessment, etc., smooth promotion of the entire assessment, etc. process will be planned while the function for carrying out the is enhanced by the Cabinet Secretariat.

(4) Review of the Second National Strategy for Information Security

The government should review the Second National Strategy even midway into the period if environmental changes occur, besides the review to be conducted after 3 years.

[Specific Measures]

(A) Review of the Second National Strategy for Information Security (Cabinet Secretariat)

The government should review the Second National Strategy even midway into the period if environmental changes occur.

Chapter 5: Issues to be Urgently Addressed in FY2010

~ Emphasis for FY2010 is “Intensive promotion of information security measures through joint actions of all major bodies” ~

In Chapter 3 and Chapter 4, the idea of “all entities should assume they may be subject to accidents” was emphasized for the initial year of the Second National Strategy which is a 3-year plan, and has now been put forth as a specific policy that should be implemented in FY2009. For this effort, under the common understanding of the importance of efforts toward information security issues by all organizations, while being self-aware of the own responsibilities, efforts toward the realization of “new public and private sector cooperation model” directed at the implementation of measures under suitable role division in response to the respective standpoints are intended to be evolved by the addition of new factors such as “Accidents Assumed Society” or “rationally proven approach.”

As shown in Chapter 2 Section 2, as Japan grows toward a “mature and advanced country in information security”, the growth process “self-awareness” -> “joint action” -> “maturity” of “individual” and “society” is necessary. FY2009 does not go beyond the first step of a new stage, and in future, the promotion of the reinforcement of the efforts will be sought. For this reason, as shown by the thinking behind “new government and private sector cooperation model”, it is necessary to implement measures under suitable role division in response to the respective standpoints in addition to the respective organization being aware of the importance of the information security measures and the efforts put in spontaneously.

By proceeding with the efforts through “cooperation” or “joint action” of each organization in this way, besides the efforts commenced in FY2009 starting to show results, it is also possible to improve the results of the efforts continuously implemented since the First National Strategy. As a result, in FY2010 as the second year of the Second National Strategy, while the directionality of the future 3-year efforts shown in Chapter 2 Section 1 is considered basic, the idea of “intensive promotion of information security measures through joint actions of all entities ” will be emphasized, and in particular, the promotion of policy with the directionality below should be planned for.

[Efforts toward human infrastructure/system preparation in public and

private sectors]

The issues that should be addressed in the Second National Strategy extends over many branches such as the promotion of e-Government that can be used safely and conveniently, the accurate response to cyber attack and cybercrime, the promotion for the establishment of information security governance in enterprises, and the information security improvement in the private sector.

For each organization implementing measures to promote specific efforts, it is essential for it to develop and assign human resources with knowledge related to information security as well as prepare a system for promoting information security measures.

The government will proceed to study the preparation of human infrastructure and promotion system which will become the base for promotion of all information security measures as well as promote the efforts in public and private sectors with emphasis on the policies below.

[Specific Measures]

A) Efforts toward Establishing Information Security Governance (All Government Agencies)

Each government agency will promote the efforts based on the system preparation policy for the establishment of information security governance formulated in FY2009. In particular, besides setting up the chief information security advisor with specialized knowledge to assist the chief information security manager, efforts will be put into assigning human resources who will be the staff.

B) Creation of the Information Security Report (Trial Version) (Cabinet Secretariat, and all government ministries and agencies)

Each government agency will create the information security report (trial version) based on the guidelines for creating information security reports formulated in FY2009. In this case, from the viewpoint of ensuring objectivity in the information security report, apart from the chief information security advisor, the use of an external audit system will also be actively promoted in government agencies where possible. In addition, in the created information security report, besides making comparisons/assessments in the Chief Information Security Advisor Liaison Council (temporary name), feedback and sharing of knowledge obtained through in this manner will be planned, and the chief information security manager will report at such meeting as the “Council for the Promotion of Information Security Measures” set up under the Information Security Policy

Council.

C) Enhancement of Training Programs for Government Officials (Cabinet Secretariat, and Ministry of Internal Affairs and Communications)

The Cabinet Secretariat and the Ministry of Internal Affairs and Communications will improve the quality of the government's standard training programs for government officials (general staff, management, and staff in charge of information security measures).

D) Enhancement of the Emergency Response Capability in Government Agencies against Cyber Attack (Cabinet Secretariat)

Based on the state of operations of the GSOC and the preparedness of each government agency regarding emergency response system, study will be carried out on the methods of further improving the incident response capability against cyber attack for the government as a whole.

E) Promotion of the Establishment of Information Security Governance (Ministry of Economy, Trade and Industry)

In order to promote the efforts toward the establishment of information security governance in enterprises, the dissemination of guidelines will continue. In particular, for small and medium enterprises, the support system for the promotion of information security measures will be reinforced in cooperation with relevant agencies such as the IPA.

F) Use of Information Security Supporter (Ministry of Internal Affairs and Communications)

The activities for improving the information security in the private sector will be supported, and the information security level of the people as a whole will be raised by using knowledgeable persons (information security supporters) around the user.

G) Reinforcement of the System against Cyber Terrorism (National Police Agency)

In order to deal with the sophistication of cyber attack methods that are the means of cyber terrorism, the police will promote the reinforcement of systems involved with cyber terrorism countermeasures such as maintaining the technical capability and case response ability of the cyber terrorism countermeasure staff as well as implementing trainings inside and outside the department for

improvement purposes. In addition, besides holding enlightenment activities linked to raising the awareness of cyber terrorism countermeasures based on the special characteristics of the business of critical infrastructure providers, efforts will be made to contribute to incident response activities during occurrence of cyber terrorism by participating in various exercises and implementing joint exercises while respecting the intentions of critical infrastructure providers.

H) Promotion of the Efforts regarding Digital Forensics for Cybercrime Control (National Police Agency)

In order to promote control with the accurate use of digital forensics against varied and complicated cybercrimes, the enhancement of the system starting with training for police officers engaged in cybercrime investigations will be promoted. In addition, the reinforcement of international liaison and cooperation will include holding of the Cybercrime Technology Information Network System (CTINS) Annual Conference.

[Efforts for international liaison and cooperation]

In relation to international liaison and cooperation, the ASEAN Japan Information Security Policy Meeting was held in February 2009 with the cooperation of Cabinet Secretariat, Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry, and starting with the set up of a secure business environment within the Asian region, the efforts toward reinforcing liaison related to information security measures in Asia have taken off in earnest.

As this sort of efforts show cumulative effectiveness spanning the mid- and long-term period, efforts will also be promoted in the public and private sectors in FY2010 with emphasis on the following policies.

[Specific Measures]

A) Holding of International Meeting for Security Policy (Cabinet Secretariat, Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

Based on the information security policy taking into account the agreement at the ASEAN Japan Information Security Policy Meeting held in February 2009, preparations will proceed for holding a conference in Japan in mid 2011 for discussing the policy toward enhancing cooperation and sharing the success stories of each country.

B) Promotion of the Set up of a Secure Business Environment in the Asian Region (Ministry of Economy, Trade and Industry)

Based on the “Asian knowledge economy initiative”, study will be carried out on further specific promotion policies for setting up a secure investment and business environment in various Asian countries.

[Promotion of technology R&D by public and private sectors, and its introduction]

In order for each organization implementing information security measures to carry out information security measures more effectively and easily, the promotion of technology R&D as well as its introduction is essential.

Since R&D requires mid- to long-term efforts and accumulation of various types of knowledge, efforts will be promoted in the public and private sectors with emphasis on the following policies.

[Specific Measures]

A) Assurance of Information Processing Infrastructure’s Safety (Ministry of Economy, Trade and Industry)

In order to deal with the localization of cyber attacks, refinement and concealment of attack methods, and expansion of systems (control system, etc.) that are targets of attack targets, besides promoting the enhancement of analysis capability related to the technologies and methods used in cyber attacks, preparation will be planned for a shared system between the relevant domestic and foreign organizations in industry, government and academia such as for malware sample, detection information, analysis technology/tools, vulnerability related information, and analysis technology and tools.

In addition, the preparation of a suitable information processing environment will be planned through the provision of information related secure product development method and verification method for incident response support and IT product and system developer, dissemination and enlightenment activities for intranet administrator and IT user as well as the development of technical response policies tuned to the times.

B) Enhancement of Anti-Spam Measures (Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry)

In order to increase the effectiveness of the countermeasures against spam e-mail which are progressively getting more sophisticated and malicious as a whole, the required system preparation and the sophistication of spam mail

countermeasure tasks will be devised.

In addition, in cooperation with industrial organizations such as “JEAG” which is a private sector organization established by major domestic internet service providers and mobile phone service providers, the introduction of sender domain authentication technology or port 25 blocking which are effective technologies in the prevention of spam mail transmissions will be promoted.

Furthermore, in order to cope with the abrupt increase in spam mails sent from overseas computers, besides reinforcing the cooperation with overseas enforcement authorities that implement anti-spam measures, cooperation on international anti-spam measures in the private sector will be promoted.

Besides, the government will continue to implement the “Project for Eliminating Unsolicited E-mail” (since February 2005) that notifies information related to the illegal spam mail to the internet service provider used for sending the spam mail to request actions such as suspension.

C) Preparation of System for Protecting the Embedded System's Security and Reliability (Ministry of Economy, Trade and Industry)

Environment preparation and technology development will be carried out toward the reinforcement of efforts on the security and reliability of embedded systems for information systems and IT products.

D) Study on Security Measures in a New Information Environment through Industry-Academia-Government Cooperation (Ministry of Internal Affairs and Communications)

Amidst the spreading popularity of new technologies such as cloud computing, study will be carried out on security measures such as technology development and human resource development so that the popularization of new technologies is not hindered due to spread of information security threats such as information leakage.