Comments of the Government of the United States of America on the National Information Security Center (NISC)'s draft "Uniform Standards for Information Security Measures of Government Organizations (First Overall Version for December 2005)"
November 11, 2005

Introduction

The Government of the United States is pleased to submit comments on NISC's draft "Uniform Standards for Information Security Measures of Government Organizations (First Overall Version for December 2005)." The U.S. Government, via the National Institute of Standards and Technology (NIST), has substantial experience writing standards and guidelines for U.S. non-national security federal information systems. The U.S. Office of Management and Budget (OMB) similarly has substantial experience helping federal agencies evaluate their compliance with NIST's requirements.

The United States commends NISC for undertaking the challenging task of developing and implementing security requirements for Japan's government information systems. The United States believes it is important for governments to share best practices in this area, particularly given the rapid evolution of cyber security threats, research, and knowledge.

The United States also commends NISC for soliciting public comments on these draft standards. NIST benefits immensely from similarly using an open standards development approach. Such a process helps create the best possible and most technically feasible standards; ensures that potential standards and guidelines have been thoroughly vetted, which increases their acceptance; and provides the public with greater awareness of and enhanced confidence in the government's efforts to protect systems that contain personal information.

The United States is providing comments at this time only on certain general themes. The United States looks forward to more fully exploring aspects of these standards and to continuing to share ideas with Japan after the public comment period closes.

NIST has long enjoyed a cooperative relationship with the Ministry of Economy, Trade, and Industry (METI) and the Information-technology Promotion Agency (IPA), and regularly discusses information security issues with scientists and other officials there. OMB has met numerous times with various Japanese government and industry officials to discuss federal agency information security evaluation. Both NIST and OMB welcome future opportunities to consult with NISC regarding securing government information systems.

Assessment and integration of comments

The United States urges NISC to carefully assess all comments and feedback received on these standards during the public comment period and incorporate suggestions when

these can result in improved standards or processes. The United States suggests NISC make utmost effort to consult directly with comment providers if necessary to obtain clarification or more information.

The United States understands that, based on a timeline issued in September 2005, NISC plans to issue a final version of these standards in December 2005. The United States suggests NISC keep its deadline for issuing the final standards as flexible as possible and extend it if necessary. Instead of adhering rigidly to a predetermined date for final publication, it is more important to take adequate time to review comments received, gather additional information or clarification, and if appropriate issue revised drafts for additional comment periods. In recognition of this need, NIST was given three years under the 2002 Federal Information Security Management Act (FISMA) to develop mandatory minimum information security requirements for U.S. federal agencies. In addition, NIST's Special Publication 800-53 (an important security control guideline), originally scheduled to come out June 2004, was issued in February 2005 because more time was needed to incorporate comments from government and industry customers.

Finalizing information security requirements before they are adequately vetted and improved can result in the development of weak standards or can risk causing users to begin to implement requirements that are then changed. Extended development cycles and expanded public review periods also can allow your Ministries and Agencies to better prepare for the transition to new requirements. If NISC needs more time to integrate comments but cannot delay the release of its entire set of standards, the United States suggests that NISC release by the December 2005 deadline only those sections of the standards that it believes are adequately completed.

Development and review of future standards/guidelines

The United States understands that NISC plans to assess its security standards and guidelines over the next several years through a cycle of draft/introduction, application, evaluation, and review. The United States commends this approach. Implementation guidelines that provide guidance for selecting and specifying security controls for information systems should be updated as frequently as possible to enable them to accommodate new technologies. Although governments should make every effort to deploy standards that are general and can apply in the future as well as the present, any standard can quickly become obsolete in the face of rapid technical advances. Therefore, security standards and guidelines should be reviewed regularly to determine if they need refining or updating for technical or business reasons.

The United States urges NISC to use an open development process, including Public Comment Procedures and other methods of obtaining feedback, on all government computer security standards and guidelines it issues in the future. NISC may wish to consider using a guide/standard approach, whereby NISC puts out proposed requirements as guides to see how they are accepted and used. If they work well for Ministries and Agencies, they can then be issued as standards.

The United States also suggests that Japan supplement Public Comment Procedures with open workshops and public briefings. The United States has found that such methods help bring in the widest possible audience and comments.

Finally, the United States suggests that NISC accept formal and informal comments at any time (for example, after public comment periods have closed, or based on user experience). While Public Comment Procedures often help make the comment collection process easier, the best ideas can come at any time.

Consistency with standards developed by voluntary standardization bodies

In the 2004 Report to the Leaders under the U.S.-Japan Regulatory Reform and Competition Policy Initiative, the Government of Japan confirmed that its government "guidelines and standards will, where appropriate, be open (non-proprietary) and consistent with standards developed by voluntary standardization bodies constituted upon consensus in industry." The United States agrees with the approach of striving to issue government security standards that are consistent with standards developed by voluntary standardization bodies. To this end, the United States suggests that NISC consider using the following approaches, in order of priority, which NIST uses when issuing its standards and guidelines: First, adopt or adapt existing voluntary industry standards, if available and acceptable. If they are not, join voluntary industry standards efforts to develop common government-industry standards and adopt or adapt the completed standard for government use. As a last resort, use NISC's authority and internal resources to develop standards and guidelines for Ministries and Agencies.

Technology neutrality

The United States urges that all of Japan's government information security requirements be technology neutral, whenever possible. The United States understands that this first set of standards does not specify the selection of particular technologies, and the United States commends Japan for taking this approach. The United States urges Japan to ensure that, whenever possible, forthcoming guidelines and additional standards do not promote, mandate or unduly favor specific technologies (technological neutrality), in order to provide maximum flexibility for implementing Ministries and Agencies and to encourage innovation within the private sector. In addition, procurement of information technologies or services to meet Japan's government security standards and guidelines should be fair and transparent for all domestic and foreign vendors.

Mandating minimum government information security requirements and ensuring consistency in implementation

The United States suggests that Japan consider moving toward a mandatory set of minimum information security requirements for its Ministries and Agencies. These would include some fundamental requirements such as contingency planning and intrusion detection. Among others, Japan may wish to consider the U.S. FISMA model, where the legislative branch directs the development of mandatory minimum federal

information security requirements and the executive branch implements the legislation through the employment of appropriate security standards and guidelines. Mandatory minimum requirements can provide a baseline for Ministries and Agencies so they can budget more effectively for security. Mandatory minimum requirements can also provide predictability to vendors, helping them streamline or target their products and administrative tools in ways that help Ministries and Agencies to meet the requirements.

Finally, the United States suggests that NISC make every effort to ensure that all minimum information security requirements are implemented consistently by all Ministries and Agencies. Ministries and Agencies may have unique characteristics and security needs that require them to take security measures above and beyond the minimum requirements. However, having all Ministries and Agencies use the same baseline requirements will give them a greater selection of vendors and technologies that meet their needs.