美国信息产业机构
United States Information Technology Office

USITO Comments on *Information Security Technology- Guidelines for Grading of Classified Cybersecurity Protection*

Feb 5, 2018

The United States Information Technology Office (USITO) is pleased to have the opportunity to comment on the ***Information Security Technology-Guidelines for Grading of Classified Cybersecurity protection.*** We hope our input will be carefully evaluated, and hope to have continued chances to provide comments and perspective through further iterations of the standards.

General

Thank you for the chance to comment on the draft standard. We are pleased to provide input on specific articles below:

Chapter	Original Text	Comments	Recommendations
3.1-3.2	**Target of classified protection.** Targets to which cybersecurity classified protection is introduced, including basic information network, industrial control system, cloud computing platform, Internet of Things, network using mobile interconnection technology, other networks and big data. **Basic information network.** Network equipment and facilities underpinning transfer of information and network operation, including telecom network, radio & TV network, the Internet and dedicated networks.	The scope of the regulation could be considered to include virtually all networks, particularly given the broad definition of "basic information network." As a result, companies operating in very sizable and commercially significant markets in China are likely to see their networks designated as targets for classified protection. If, as in the past, they are required to use only equipment with Chinese indigenous IP, they will confront a much smaller pool of ICT vendors from which to choose. There is no guarantee that Chinese suppliers will be able to provide the best or most advanced cybersecurity features; it is very possible that non-Chinese vendors may offer better products which, under the CCP regulation, are no longer available for purchase. The net result may be to undermine network security in China's commercial sector rather than to improve it.	We would urge the Technical Committee to reconsider their expansion of cybersecurity classified protection to commercial markets and instead limit their reach to government networks.

United States Information Technology Office
1104 Sun Palace Building, 12 Taiyanggong Middle Road
Chaoyang District, Beijing, 100028 CHINA
Tel: +8610 8429.9070

3.4	**Critical information infrastructure.** Networks in key sectors and fields such as public communication and information service, energy, finance, transport, water resources, public services and e-government, and other networks whose destruction, incapacity or data breach may seriously endanger national security, national economy and people's life, and public interests.	Related to the issue above, we are concerned by the expansive definition of critical information infrastructure (CII) to include "public communication and information services." As noted above, imposing the CCP requirement on a very broad commercial sector risks undermining network security by limiting access to the best equipment available on the global market.	We encourage TC members to exempt "public communication and information services" from the category of cybersecurity classified protection.
4.1	**Security protection levels.** In accordance with relevant regulatory documents concerning classified protection, security protection provided to targets of classified protection is classified into 5 levels below: a) Level 1: A	Under the 2007 policy that has until now guided MLPS implementation, a network breach would need to cause "serious damage to social order and public interests or harm to national security" for the network to be classified as a level 3 or above. The draft regulation adds a new factor to that trigger list: "extremely serious harm to the legitimate rights and interests of citizens, legal persons and other organizations." In other words, the draft standard would make it easier for authorities to classify a	Major industrial economies have historically been sparing in invoking national security, reserving it for only the most exigent circumstances, in order to preserve its intended meaning and impact. Expanding the list of situations to which national security applies risks diluting its impact, and heightening essential concerns about fairness with China's trading partners. We would urge the TC to maintain the existing, more

	damaged target of classified protection causes harm to legitimate rights and interests of citizens, legal persons and other organizations, without prejudice to national security, social order and the public interest. b) Level 2: A damaged target of classified protection causes serious harm to the legitimate rights and interests of citizens, legal persons and other organizations, or harm to social order and public interests, without prejudice to national security. c) Level 3: A damaged target of classified protection causes extremely serious harm to the legitimate rights and interests of citizens, legal persons and other organizations, or serious harm to social order and public interests, or harm to national security. d) Level 4: A damaged target of classified protection causes extremely serious harm to	network as sensitive and therefore require the use of products with indigenous Chinese IP.	narrowly-scoped definition of national security contained in the existing rule, and refrain from broadening the definition.

	social order and public interests, or serious harm to national security. e) Level 5: A damaged target of classified protection causes extremely serious harm to national security.		
6.5	The security of a target of grading includes business information security and system service security.	The explicit reference to “business information security” (业务信息安全) underscores that cybersecurity classified protection is being extended into commercial markets. As noted earlier, we are concerned that TC members appear to be pulling commercial ICT sectors under the national security umbrella. Commercial entities should be permitted to assess and provide the most appropriate security protections for their networks. Broadening government requirements for network security from government networks to commercial networks will make it easier for malicious actors to engage in cyberattacks as the attack vectors would be the same for both. In terms of network security, heterogeneity is a better and more secure approach.	We would strongly recommend removing references to business information security, as this creates the impression that the scope of cybersecurity classified protection is overly broad. Presumably, damaging cyber breaches involving business information would already be covered under the original 2007 MLPS formulation that encompassed any trespasses causing “serious damage to social order and public interests or harm to national security.”