君合研究简讯

JUNHE

2019 年 6 月 21 日

网络安全法律热点问题

网络安全漏洞将何去何从

——简析《网络安全漏洞管理规定（征求意见稿）》

2019年6月18日，工业和信息化部（以下简称“**工信部**”）发布会同有关部门起草的《网络安全漏洞管理规定（征求意见稿）》（以下简称“**《管理规定》**”）征求意见至2019年7月18日。此前安全漏洞的处置流程是通过推荐性国家标准的形式进行规范。而《管理规定》则将以具有法律约束力的条款明确网络安全漏洞的监管对象、主管机构，并规范网络安全漏洞处置流程。

一、监管对象、主管机构

《网络安全法》第22条规定，网络产品、服务的提供者……发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

《管理规定》明确的监管对象包括**网络产品、服务提供者和网络运营者，以及开展漏洞检测、评估、收集、发布及相关竞赛等活动的组织**（以下简称“**第三方组织**”）或个人（*第2条*），主管机构为**工信部、公安部和有关行业主管部门**（*第4条*）。

二、网络安全漏洞处置流程

《管理规定》要求网络产品、服务提供者和网络运营者发现或获知其网络产品、服务、系统存在漏洞后，应当按照相应的时间采取漏洞修补或防范措施并向社会或用户发布（*第3条*）。

与原国家标准相比，《管理规定》并没有沿用其详细的漏洞管理生命周期流程，对于漏洞发现、接受等问题进行详细规范，调整了原标准规定的处理时间表，并且区别网络产品和网络服务、系统提供者漏洞修补或防范措施期限中规定的漏洞修补或防范措施期限。

《管理规定》所规定的具体流程如下：

流程	要求
验证	网络产品、服务提供者和网络运营者发现或获知其网络产品、服务、系统存在漏洞后**立即**对漏洞进行验证
漏洞修补或防范措施	相关**网络产品应当在90日**内采取漏洞修补或防范措施
	相关**网络服务或系统应当在10日**内采取漏洞修补或防范措施
通知	需要用户或相关技术合作方采取漏洞修补或防范措施的，**应当在对相关网络产品、服务、系统采取漏洞修补或防范措施后5日内**，将漏洞风险及用户或相关技术合作方需采取的修补或防范措施**向社会发布或通过客服**等方式**告知所有可能受影响的用户和相关技术合作方**，提供必要的技术支持，**并向工信部网络安全威胁信息共享平台报送相关漏洞情况**。

三、第三方组织向社会发布漏洞信息

《网络安全法》第25条要求，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。

而《管理规定》明确，第三方组织或个人通过网站、媒体、会议等方式向社会发布漏洞信息应当遵循必要、真实、客观、有利于防范和应对网络安全风险的原则*（第6条）*。第三方组织应当加强内部管理，履行管理义务，防范漏洞信息泄露和内部人员违规发布漏洞信息*（第7条）*。

特别的，此前主要收集、发布漏洞信息的中国信息安全测评中心下设的国家信息安全漏洞库，或是国家计算机网络应急技术处理协调中心下设的国家信息安全漏洞共享平台也将会被视为第三方组织，需要遵守第三方组织发布漏洞的规定*（第10条）*。

四、法律责任

《管理规定》第8条规定，网络产品、服务提供者和网络运营者未按规定采取漏洞修补或防范措施并向社会或用户发布的，由工信部、公安部等有关部门按职责依据《网络安全法》第56条、第59条、第60条等规定组织对其进行约谈或给予行政处罚。

另，第9条规定，第三方组织违反规定向社会发布漏洞信息，由工信部、公安部等有关部门组织对其进行约谈，或依据《网络安全法》第62条、第63条等规定给予行政处罚；构成犯罪的，依法追究刑事责任；给网络产品、服务提供者和网络运营者造成经济或名誉损害的，依法承担民事责任。

五、我们的观察

《管理规定》作为规范性文件，在《网络安全法》的体系下，直接明确了网络产品、服务提供者和网络运营者和第三方组织对于网络安全漏洞的处理要求，明确了法律责任。对于企业将如何在实践中做到合规处理网络安全漏洞，我们将持续关注。

董　潇　合伙人　电话：86-10 8519 1718　邮箱地址：dongx@junhe.com
朱　彤　律　师　电话：86-10 8519 1739　邮箱地址：zhutong@junhe.com
贾子豫　律　师　电话：86-10 8540 8702　邮箱地址：jiazy@junhe.com

本文仅为分享信息之目的提供。本文的任何内容均不构成君合律师事务所的任何法律意见或建议。如您想获得更多讯息，敬请关注君合官方网站

JUNHE BULLETIN

JUNHE

June 21, 2019

Cybersecurity Law Hot Issues

What course should cybersecurity vulnerability administration follow?

——A brief analysis of the Provisions on the Administration of Cybersecurity Vulnerability (Draft for Comment)

On June 18, 2019, the Ministry for Industry and Information Technology ("**MIIT**") released the *Provisions on the Administration of Cybersecurity Vulnerability (Draft for Comment)* (the "**Provisions**"), jointly drafted by the MIIT and relevant departments of the State Council, and which will be open for public comment until July 18, 2019. Whereas cybersecurity vulnerability had previously regulated by voluntary national standards, the Provisions now aim to clarify the regulatory objects and the competent authorities of cybersecurity vulnerability, as well as to provide procedural regulations for dealing with cybersecurity vulnerability.

I. Regulatory Objects and Competent Authorities

Article 22 of the *Cybersecurity Law* (the "**CSL**") stipulates that "*for any risk such as a security defect or vulnerability that is found, the provider concerned shall promptly take remedial measures, inform the users of the said risk, and report the case to the competent authority.*"

The Provisions clarifies that the regulatory objects shall be **providers of network products or services, network operators and organizations or individuals that carry out detection, assessment, collection and publication of cybersecurity vulnerability or hold relevant events such as competitions** ("**third-party organizations**") *(Article 2)*, while the competent authorities shall be **MIIT, the Ministry of Public Security** ("**MPS**") **and relevant industry authorities** *(Article 4)*.

II. Procedures for Dealing with Cybersecurity Vulnerability

The Provisions requires that, upon discovery or having been informed of any vulnerability of its network products, services or systems, a concerned provider of network products or services or network operator shall, in a timely manner, take remedial or preventive measures, and release such cybersecurity information to its users or the public *(Article 3)*.

Compared with the original national standards, the Provisions do not follow the same procedures for dealing with cybersecurity vulnerability in specifying the discovery, acceptance of vulnerability and other relevant issues. The Provisions have adjusted the processing schedule for taking remedial measures and preventive measures, and different time requirements are specified for providers of network products and for providers of network services or systems.

The specified procedures stipulated in the Provisions are as follows:

Procedures	**Requirements**
Verification	A provider of network products or services and a network operator shall **promptly** verify the vulnerability upon its discovery or having been informed of such vulnerability in its products, services or systems.
Remedial or Preventive Measures	Remedial or preventive measures shall be undertaken **within 90 days for the relevant network products** after the verification of the vulnerability.
	Remedial or preventive measures shall be undertaken **within 10 days for relevant network services or systems** after the verification of the vulnerability.
Notification	When it is necessary for a user or technical partner to carry out remedial or preventive measures, the provider of network products, services or systems shall, **within 5 days after it has taken measures**, **release to the public or notify all the potentially affected users or relevant technical partners of the risk of such vulnerability and the remedial or preventive measures that the user or technical partner shall take through customer service**, and provide them with the necessary technical support, **and such vulnerability shall also be reported to the MIIT's Information Sharing Platform of Cybersecurity Threat as well.**

III. Third-party Organizations Releasing Cybersecurity Information to the Public

Article 25 of the CSL stipulates that the release of cybersecurity information, such as system vulnerability, computer virus, network attacks and intrusions shall be carried out in compliance with applicable regulations of the State.

The Provisions further stipulates that third-party organizations and individuals shall adhere to the principles of being "necessary, authentic, objective, preventive and responsive to cybersecurity risks" when releasing information of cybersecurity vulnerability to the public through a website, a media conference, etc. *(Article 6)*. Third-party organizations shall enhance their internal management, perform relevant administrative obligations, and prevent leaks of information about cybersecurity vulnerability, and prohibit its staff from releasing such information *(Article 7)*.

The China National Vulnerability Database of

Information Security, which comes under the China Information Technology Security Evaluation Center, and the China National Vulnerability Database, which is under China National Internet Emergency Center, previously collected and published vulnerability information,according to the Provisions, they will be deemed as third-party organizations, and as such are required to observe relevant regulations *(Article 10)*.

IV. Legal Liability

Article 8 of the Provisions stipulates that, for a network product or service provider or a network operator that fails to take remedial or preventive measures, and that releases vulnerability information to the public or its users, administrative penalties shall be imposed and interviews may be organized by the MIIT, MPS and other relevant authorities, according to Articles 56, 59 and 60 of the CSL.

Additionally, Article 9 of the Provisions stipulates that, for third-party organizations which illegally release vulnerability information to the public, interviews with the MIIT, MPS and other relevant authorities will be organized, and administrative penalties shall be imposed according to Articles 62 and 63 of the CSL; violations constituting crimes shall be subject to investigations on criminal liabilities; and civil liability shall be borne when the violations have caused economic loss or reputational damage to network product or service providers and network operators.

V. Our Observation

The Provisions, as a regulatory document under the CSL, directly clarifies the legal requirements regarding cybersecurity vulnerability processing for network product or service providers, network operators and third-party organizations, and the legal liabilities of relevant subjects thereunder. We will continue to pay close attention to how enterprises will manage the legal aspects of cybersecurity vulnerability in practice.

Marissa DONG	Partner	Tel: 86 10 8519 1718	Email:dongx@junhe.com
Tong ZHU	Associate	Tel: 86 10 8519 1739	Email:zhutong@junhe.com
Ziyu JIA	Associate	Tel: 86 10 8540 8702	Email:jiazy@junhe.com

This document is provided for and only for the purposes of information sharing. Nothing contained in this document constitutes any legal advice or opinion of JunHe Law Offices.. For more information, please visit our official website at www.junhe.com or our WeChat public account “君合法律评论”/WeChat account “JUNHE_LegalUpdates”.

。