网络安全漏洞管理规定

（征求意见稿）

第一条 为规范网络安全漏洞（以下简称漏洞）报告和信息发布等行为，保证网络产品、服务、系统的漏洞得到及时修补，提高网络安全防护水平，根据《国家安全法》《网络安全法》，制定本规定。

第二条 中华人民共和国境内网络产品、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,应当遵守本规定。

第三条 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，应当遵守以下规定：

（一）立即对漏洞进行验证，对相关网络产品应当在 90 日内采取漏洞修补或防范措施，对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；

（二）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，并向工业和信息化部网络安全威胁信息共享平台报送相关漏洞情况。

第四条 工业和信息化部、公安部和有关行业主管部门按照各自职责组织督促网络产品、服务提供者和网络运营者采取漏洞修补或防范措施。

第五条 工业和信息化部、公安部、国家互联网信息办公室等有关部门实现漏洞信息实时共享。

第六条 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，并遵守以下规定：

（一）不得在网络产品、服务提供者和网络运营者向社会或用户发布漏洞修补或防范措施之前发布相关漏洞信息；

（二）不得刻意夸大漏洞的危害和风险；

（三）不得发布和提供专门用于利用网络产品、服务、系统漏洞从事危害网络安全活动的方法、程序和工具；

（四）应当同步发布漏洞修补或防范措施。

第七条 第三方组织应当加强内部管理，履行下列管理义务，防范漏洞信息泄露和内部人员违规发布漏洞信息：

（一）明确漏洞管理部门和责任人；

（二）建立漏洞信息发布内部审核机制；

（三）采取防范漏洞信息泄露的必要措施；

（四）定期对内部人员进行保密教育；

（五）制定内部问责制度。

第八条 网络产品、服务提供者和网络运营者未按本规定采取漏洞修补或防范措施并向社会或用户发布的，由工业和信息化部、公安部等有关部门按职

责依据《网络安全法》第五十六条、第五十九条、第六十条等规定组织对其进行约谈或给予行政处罚。

第九条 第三方组织违反本规定向社会发布漏洞信息，由工业和信息化部、公安部等有关部门组织对其进行约谈，或依据《网络安全法》第六十二条、第六十三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。

第十条 鼓励第三方组织和个人获知网络产品、服务、系统存在的漏洞后，及时向国家信息安全漏洞共享平台、国家信息安全漏洞库等漏洞收集平台报送有关情况。漏洞收集平台应当遵守本规定第六条、第七条规定。

第十一条 任何组织或个人发现涉嫌违反本规定的情形，有权向工业和信息化部、公安部举报。

第十二条 本规定自印发之日起施行。