名词术语

一、网络安全事件及其分类

（一）网络安全事件。网络安全事件是指由于人为原因、软硬件缺陷或故障、自然灾害等，对网络和信息系统或者其中的数据造成危害，对社会造成负面影响的事件。

（二）网络安全事件分类。网络安全事件分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设施设备故障、灾害性事件和其他网络安全事件等。

1.有害程序事件分为计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件。

2.网络攻击事件分为拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件。

3.信息破坏事件分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件。

4.信息内容安全事件是指通过网络传播法律法规禁止信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公众利益的事件。

5.设施设备故障分为软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障。

6.灾害性事件是指由自然灾害等突发事件导致的网络安全事件。

7.其他事件是指不能归为以上分类的网络安全事件。

（三）关键信息基础设施。《中华人民共和国网络安全法》规定：“国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定”。

二、重要网络与信息系统

重要网络与信息系统是指所承载的业务与国家安全、社会秩序、经济建设、公众利益密切相关的网络和信息系统。

三、重要敏感信息

重要敏感信息是指不涉及国家秘密，但与国家安全、经济发展、社会稳定，以及企业和公众利益密切相关的信息。这些信息一旦未经授权披露、丢失、滥用、篡改或销毁，可能造成以下后果：

（一）损害国防、国际关系。

（二）损害国家财产、公共利益以及个人财产和人身安全。

（三）影响国家预防和打击经济与军事间谍、政治渗透、有组织犯罪等。

（四）影响行政机关依法调查处理违法、渎职行为，或涉嫌违法、渎职行为。

（五）干扰政府部门依法公正地开展监督、管理、检查、审计等行政活动，妨碍政府部门履行职责。

（六）危害国家关键基础设施、政府信息系统安全。

（七）影响市场秩序，造成不公平竞争，破坏市场规律。

（八）可推论出国家秘密事项。

（九）侵犯个人隐私、企业商业秘密和知识产权。

（十）损害国家、企业、个人的其他利益和声誉。

四、网络和信息系统损失程度划分说明

网络和信息系统损失是指由于网络安全事件对系统的软硬件、功能及数据的破坏，导致系统业务中断，从而给事发组织所造成的损失，其大小主要考虑恢复系统正常运行和消除安全事件负面影响所需付出的代价，划分为特别严重的系统损失、严重的系统损失、较大的系统损失和较小的系统损失，说明如下：

（一）特别严重的系统损失。造成系统大面积瘫痪，使其丧失业务处理能力，或系统关键数据的保密性、完整性、可用性遭到严重破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价十分巨大，对于事发组织是不可承受的。

（二）严重的系统损失。造成系统长时间中断或局部瘫痪，使其业务处理能力受到极大影响，或系统关键数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价巨大，但对于事发组织是可承受的。

（三）较大的系统损失。造成系统中断，明显影响系统使用效率，使重要信息系统或一般信息系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价较大，但对于事发组织是可承受的；

（四）较小的系统损失。造成系统短暂中断，影响系统使用效率，使系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到影响，恢复系统正常运行和消除安全事件负面影响所需付出的代价较小。

五、“六日”“七进”

六日：金融日、法治日、电信日、青少年日、个人信息保护日、校园日

七进：进机关、进军营、进企业、进社区、进校园、进农村、进家庭