公共互联网网络安全突发事件应急预案

1.总则

1.1 编制目的

建立健全公共互联网网络安全突发事件应急组织体系和工作机制，提高公共互联网网络安全突发事件综合应对能力，确保及时有效地控制、减轻和消除公共互联网网络安全突发事件造成的社会危害和损失，保证公共互联网持续稳定运行和数据安全，维护国家网络空间安全，保障经济运行和社会秩序。

1.2 编制依据

《中华人民共和国突发事件应对法》《中华人民共和国网络安全法》《中华人民共和国电信条例》等法律法规和《国家突发公共事件总体应急预案》《国家网络安全事件应急预案》等相关规定。

1.3 适用范围

本预案适用于面向社会提供服务的基础电信企业、域名注册管理和服务机构（以下简称域名机构）、互联网企业（含工业互联网平台企业）发生网络安全突发事件的应对工作。

本预案所称网络安全突发事件，是指突然发生的，由网络攻击、网络入侵、恶意程序等导致的，造成或可能造成严重社会危害或影响，需要电信主管部门组织采取应急处置措施予以应对的网络中断（拥塞）、系统瘫痪（异常）、数据泄露（丢失）、病毒传播等事件。

本预案所称电信主管部门包括工业和信息化部及各省（自治区、直辖市）通信管理局。

工业和信息化部对国家重大活动期间网络安全突发事件应对工作另有规定的，从其规定。

1.4 工作原则

公共互联网网络安全突发事件应急工作坚持统一领导、分级负责；坚持统一指挥、密切协同、快速反应、科学处置；坚持预防为主，预防与应急相结合；落实基础电信企业、域名机构、互联网服务提供者的主体责任；充分发挥网络安全专业机构、网络安全企业和专家学者等各方面力量的作用。

2.组织体系

2.1 领导机构与职责

在中央网信办统筹协调下，工业和信息化部网络安全和信息化领导小组（以下简称部领导小组）统一领导公共互联网网络安全突发事件应急管理工作，负责特别重大公共互联网网络安全突发事件的统一指挥和协调。

2.2 办事机构与职责

在中央网信办下设的国家网络安全应急办公室统筹协调下，在部领导小组统一领导下，工业和信息化部网络安全应急办公室（以下简称部应急办）负责公共互联网网络安全应急管理事务性工作；及时向部领导小组报告突发事件情况，提出特别重大网络安全突发事件应对措施建议；负责重大网络安全突发事件的统一指挥和协调；根据需要协调较大、一般网络安全突发事件应对工作。

部应急办具体工作由工业和信息化部网络安全管理局承担，有关单位明确负责人和联络员参与部应急办工作。

2.3 其他相关单位职责

各省（自治区、直辖市）通信管理局负责组织、指挥、协调本行政区域相关单位开展公共互联网网络安全突发事件的预防、监测、报告和应急处置工作。

基础电信企业、域名机构、互联网企业负责本单位网络安全突发事件预防、监测、报告和应急处置工作，为其他单位的网络安全突发事件应对提供技术支持。

国家计算机网络应急技术处理协调中心、中国信息通信研究院、中国软件评测中心、国家工业信息安全发展研究中心（以下统称网络安全专业机构）负责监测、报告公共互联网网络安全突发事件和预警信息，为应急工作提供决策支持和技术支撑。

鼓励网络安全企业支撑参与公共互联网网络安全突发事件应对工作。

3.事件分级

根据社会影响范围和危害程度，公共互联网网络安全突发事件分为四级：特别重大事件、重大事件、较大事件、一般事件。

3.1 特别重大事件

符合下列情形之一的，为特别重大网络安全事件：

（1）全国范围大量互联网用户无法正常上网；

（2）.CN 国家顶级域名系统解析效率大幅下降；

（3）1 亿以上互联网用户信息泄露；

（4）网络病毒在全国范围大面积爆发；

（5）其他造成或可能造成特别重大危害或影响的网络安全事件。

3.2 重大事件

符合下列情形之一的，为重大网络安全事件：

（1）多个省大量互联网用户无法正常上网；

（2）在全国范围有影响力的网站或平台访问出现严重异常；

（3）大型域名解析系统访问出现严重异常；

（4）1 千万以上互联网用户信息泄露；

（5）网络病毒在多个省范围内大面积爆发；

（6）其他造成或可能造成重大危害或影响的网络安全事件。

3.3 较大事件

符合下列情形之一的，为较大网络安全事件：

（1）1 个省内大量互联网用户无法正常上网；

（2）在省内有影响力的网站或平台访问出现严重异常；

（3）1 百万以上互联网用户信息泄露；

（4）网络病毒在 1 个省范围内大面积爆发；

（5）其他造成或可能造成较大危害或影响的网络安全事件。

3.4 一般事件

符合下列情形之一的，为一般网络安全事件：

（1）1 个地市大量互联网用户无法正常上网；

（2）10 万以上互联网用户信息泄露；

（3）其他造成或可能造成一般危害或影响的网络安全事件。

4.监测预警

4.1 事件监测

基础电信企业、域名机构、互联网企业应当对本单位网络和系统的运行状况进行密切监测，一旦发生本预案规定的网络安全突发事件，应当立即通过电话等方式向部应急办和相关省（自治区、直辖市）通信管理局报告，不得迟报、谎报、瞒报、漏报。

网络安全专业机构、网络安全企业应当通过多种途径监测、收集已经发生的公共互联网网络安全突发事件信息，并及时向部应急办和相关省（自治区、直辖市）通信管理局报告。

报告突发事件信息时，应当说明事件发生时间、初步判定的影响范围和危害、已采取的应急处置措施和有关建议。

4.2 预警监测

基础电信企业、域名机构、互联网企业、网络安全专业机构、网络安全企业应当通过多种途径监测、收集漏洞、病毒、网络攻击最新动向等网络安全隐患和预警信息，对发生突发事件的可能性及其可能造成的影响进行分析评估；认为可能发生特别重大或重大突发事件的，应当立即向部应急办报告；认为可能发生较大或一般突发事件的，应当立即向相关省（自治区、直辖市）通信管理局报告。

4.3 预警分级

建立公共互联网网络突发事件预警制度，按照紧急程度、发展态势和可能造成的危害程度，公共互联网网络突发事件预警等级分为四级：由高到低依次用红色、橙色、黄色和蓝色标示，分别对应可能发生特别重大、重大、较大和一般网络安全突发事件。

4.4 预警发布

部应急办和各省（自治区、直辖市）通信管理局应当及时汇总分析突发事件隐患和预警信息，必要时组织相关单位、专业技术人员、专家学者进行会商研判。

认为需要发布红色预警的，由部应急办报国家网络安全应急办公室统一发布（或转发国家网络安全应急办公室发布的红色预警），并报部领导小组；认为需要发布橙色预警的，由部应急办统一发布，并报国家网络安全应急办公室和部领导小组；认为需要发布黄色、蓝色预警的，相关省（自治区、直辖市）通信管理局可在本行政区域内发布，并报部应急办，同时通报地方相关部门。对达不

到预警级别但又需要发布警示信息的，部应急办和各省（自治区、直辖市）通信管理局可以发布风险提示信息。

发布预警信息时，应当包括预警级别、起始时间、可能的影响范围和造成的危害、应采取的防范措施、时限要求和发布机关等，并公布咨询电话。面向社会发布预警信息可通过网站、短信、微信等多种形式。

4.5 预警响应

4.5.1 黄色、蓝色预警响应

发布黄色、蓝色预警后，相关省（自治区、直辖市）通信管理局应当针对即将发生的网络安全突发事件的特点和可能造成的危害，采取下列措施：

（1）要求有关单位、机构和人员及时收集、报告有关信息，加强网络安全风险的监测；

（2）组织有关单位、机构和人员加强事态跟踪分析评估，密切关注事态发展，重要情况报部应急办；

（3）及时宣传避免、减轻危害的措施，公布咨询电话，并对相关信息的报道工作进行正确引导。

4.5.2 红色、橙色预警响应

发布红色、橙色预警后，部应急办除采取黄色、蓝色预警响应措施外，还应当针对即将发生的网络安全突发事件的特点和可能造成的危害，采取下列措施：

（1）要求各相关单位实行 24 小时值班，相关人员保持通信联络畅通；

（2）组织研究制定防范措施和应急工作方案，协调调度各方资源，做好各项准备工作，重要情况报部领导小组；

（3）组织有关单位加强对重要网络、系统的网络安全防护；

（4）要求相关网络安全专业机构、网络安全企业进入待命状态，针对预警信息研究制定应对方案，检查应急设备、软件工具等，确保处于良好状态。

4.6 预警解除

部应急办和省（自治区、直辖市）通信管理局发布预警后，应当根据事态发展，适时调整预警级别并按照权限重新发布；经研判不可能发生突发事件或风险已经解除的，应当及时宣布解除预警，并解除已经采取的有关措施。相关省（自治区、直辖市）通信管理局解除黄色、蓝色预警后，应及时向部应急办报告。

5.应急处置

5.1 响应分级

公共互联网网络安全突发事件应急响应分为四级：I 级、II 级、III 级、IV 级，分别对应已经发生的特别重大、重大、较大、一般事件的应急响应。

5.2 先行处置

公共互联网网络安全突发事件发生后，事发单位在按照本预案规定立即向电信主管部门报告的同时，应当立即启动本单位应急预案，组织本单位应急队伍和工作人员采取应急处置措施，尽最大努力恢复网络和系统运行，尽可能减少对用户和社会的影响，同时注意保存网络攻击、网络入侵或网络病毒的证据。

5.3 启动响应

I 级响应根据国家有关决定或经部领导小组批准后启动，由部领导小组统一指挥、协调。

II 级响应由部应急办决定启动，由部应急办统一指挥、协调。

III 级、IV 级响应由相关省（自治区、直辖市）通信管理局决定启动，并负责指挥、协调。

启动 I 级、II 级响应后，部应急办立即将突发事件情况向国家网络安全应急办公室等报告；部应急办和相关单位进入应急状态，实行 24 小时值班，相关人员保持联络畅通，相关单位派员参加部应急办工作；视情在部应急办设立应急恢复、攻击溯源、影响评估、信息发布、跨部门协调、国际协调等工作组。

启动 III 级、IV 级响应后，相关省（自治区、直辖市）通信管理局应及时将相关情况报部应急办。

5.4 事态跟踪

启动 I 级、II 级响应后，事发单位和网络安全专业机构、网络安全企业应当持续加强监测，跟踪事态发展，检查影响范围，密切关注舆情，及时将事态发展变化、处置进展情况、相关舆情报部应急办。省（自治区、直辖市）通信管理局立即全面了解本行政区域受影响情况，并及时报部应急办。基础电信企业、域名机构、互联网企业立即了解自身网络和系统受影响情况，并及时报部应急办。

启动 III 级、IV 级响应后，相关省（自治区、直辖市）通信管理局组织相关单位加强事态跟踪研判。

5.5 决策部署

启动 I 级、II 级响应后，部领导小组或部应急办紧急召开会议，听取各相关方面情况汇报，研究紧急应对措施，对应急处置工作进行决策部署。

针对突发事件的类型、特点和原因，要求相关单位采取以下措施：带宽紧急扩容、控制攻击源、过滤攻击流量、修补漏洞、查杀病毒、关闭端口、启用备份数据、暂时关闭相关系统等；对大规模用户信息泄露事件，要求事发单位及时告知受影响的用户，并告知用户减轻危害的措施；防止发生次生、衍生事件的必要措施；其他可以控制和减轻危害的措施。

做好信息报送。及时向国家网络安全应急办公室等报告突发事件处置进展情况；视情况由部应急办向相关职能部门、相关行业主管部门通报突发事件有关情况，必要时向相关部门请求提供支援。视情况向外国政府部门通报有关情况并请求协助。

注重信息发布。及时向社会公众通告突发事件情况，宣传避免或减轻危害的措施，公布咨询电话，引导社会舆论。未经部应急办同意，各相关单位不得擅自向社会发布突发事件相关信息。

启动 III 级、IV 级响应后，相关省（自治区、直辖市）通信管理局组织相关单位开展处置工作。处置中需要其他区域提供配合和支持的，接受请求的省（自治区、直辖市）通信管理局应当在权限范围内积极配合并提供必要的支持；必要时可报请部应急办予以协调。

5.6 结束响应

突发事件的影响和危害得到控制或消除后，I 级响应根据国家有关决定或经部领导小组批准后结束；II 级响应由部应急办决定结束，并报部领导小组；III 级、IV 级响应由相关省（自治区、直辖市）通信管理局决定结束，并报部应急办。

6.事后总结

6.1 调查评估

公共互联网网络安全突发事件应急响应结束后，事发单位要及时调查突发事件的起因（包括直接原因和间接原因）、经过、责任，评估突发事件造成的影响和损失，总结突发事件防范和应急处置工作的经验教训，提出处理意见和改进措施，在应急响应结束后 10 个工作日内形成总结报告，报电信主管部门。电信主管部门汇总并研究后，在应急响应结束后 20 个工作日内形成报告，按程序上报。

6.2 奖惩问责

工业和信息化部对网络安全突发事件应对工作中作出突出贡献的先进集体和个人给予表彰或奖励。

对不按照规定制定应急预案和组织开展演练，迟报、谎报、瞒报和漏报突发事件重要情况，或在预防、预警和应急工作中有其他失职、渎职行为的单位或个人，由电信主管部门给予约谈、通报或依法、依规给予问责或处分。基础电信企业有关情况纳入企业年度网络与信息安全责任考核。

7.预防与应急准备

7.1 预防保护

基础电信企业、域名机构、互联网企业应当根据有关法律法规和国家、行业标准的规定，建立健全网络安全管理制度，采取网络安全防护技术措施，建设网络安全技术手段，定期进行网络安全检查和风险评估，及时消除隐患和风险。电信主管部门依法开展网络安全监督检查，指导督促相关单位消除安全隐患。

7.2 应急演练

电信主管部门应当组织开展公共互联网网络安全突发事件应急演练，提高相关单位网络安全突发事件应对能力。基础电信企业、大型互联网企业、域名机构要积极参与电信主管部门组织的应急演练，并应每年组织开展一次本单位网络安全应急演练，应急演练情况要向电信主管部门报告。

7.3 宣传培训

电信主管部门、网络安全专业机构组织开展网络安全应急相关法律法规、应急预案和基本知识的宣传教育和培训，提高相关企业和社会公众的网络安全意识和防护、应急能力。基础电信企业、域名机构、互联网企业要面向本单位员工加强网络安全应急宣传教育和培训。鼓励开展各种形式的网络安全竞赛。

7.4 手段建设

工业和信息化部规划建设统一的公共互联网网络安全应急指挥平台，汇集、存储、分析有关突发事件的信息，开展应急指挥调度。指导基础电信企业、大型互联网企业、域名机构和网络安全专业机构等单位规划建设本单位突发事件信息系统，并与工业和信息化部应急指挥平台实现互联互通。

7.5 工具配备

基础电信企业、域名机构、互联网企业和网络安全专业机构应加强对木马查杀、漏洞检测、网络扫描、渗透测试等网络安全应急装备、工具的储备，及时调整、升级软件硬件工具。鼓励研制开发相关技术装备和工具。

8.保障措施

8.1 落实责任

各省（自治区、直辖市）通信管理局、基础电信企业、域名机构、互联网企业、网络安全专业机构要落实网络安全应急工作责任制，把责任落实到单位领导、具体部门、具体岗位和个人，建立健全本单位网络安全应急工作体制机制。

8.2 经费保障

工业和信息化部为部应急办、各省（自治区、直辖市）通信管理局、网络安全专业机构开展公共互联网网络安全突发事件应对工作提供必要的经费保障。基础电信企业、域名机构、大型互联网企业应当安排专项资金，支持本单位网络安全应急队伍建设、手段建设、应急演练、应急培训等工作开展。

8.3 队伍建设

网络安全专业机构要加强网络安全应急技术支撑队伍建设，不断提升网络安全突发事件预防保护、监测预警、应急处置、攻击溯源等能力。基础电信企业、域名机构、大型互联网企业要建立专门的网络安全应急队伍，提升本单位网络安全应急能力。支持网络安全企业提升应急支撑能力，促进网络安全应急产业发展。

8.4 社会力量

建立工业和信息化部网络安全应急专家组，充分发挥专家在应急处置工作中的作用。从网络安全专业机构、相关企业、科研院所、高等学校中选拔网络安全技术人才，形成网络安全技术人才库。

8.5 国际合作

工业和信息化部根据职责建立国际合作渠道，签订国际合作协议，必要时通过国际合作应对公共互联网网络安全突发事件。鼓励网络安全专业机构、基础电信企业、域名机构、互联网企业、网络安全企业开展网络安全国际交流与合作。

9.附则

9.1 预案管理

本预案原则上每年评估一次，根据实际情况由工业和信息化部适时进行修订。

各省（自治区、直辖市）通信管理局要根据本预案，结合实际制定或修订本行政区域公共互联网网络安全突发事件应急预案，并报工业和信息化部备案。

基础电信企业、域名机构、互联网企业要制定本单位公共互联网网络安全突发事件应急预案。基础电信企业、域名机构、大型互联网企业的应急预案要向电信主管部门备案。

9.2 预案解释

本预案由工业和信息化部网络安全管理局负责解释。

9.3 预案实施时间

本预案自印发之日起实施。2009 年 9 月 29 日印发的《公共互联网网络安全应急预案》同时废止。