教　育　部　文　件

教技〔2018〕8号

教育部关于印发《教育系统网络安全事件应急预案》的通知

各省、自治区、直辖市教育厅（教委），新疆生产建设兵团教育局，部属各高等学校，部内各司局、各直属单位，中国教育和科研计算机网网络中心：

根据《中华人民共和国网络安全法》《国家网络安全事件应急预案》的要求，为健全完善教育系统网络安全事件应急工作机制，提高教育系统网络安全应急处置能力，我部制定了《教育系统网络安全事件应急预案》。现印发给你们，请认真贯彻落实。

教　育　部

2018年6月11日

教育系统网络安全事件应急预案

1 总则

1.1 编制目的

根据《国家网络安全事件应急预案》要求，健全完善教育系统网络安全事件应急工作机制，规范网络安全事件工作流程，提高教育系统网络安全应急处置能力，预防和减少网络安全事件造成的损失和危害，维护教育系统安全稳定。

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》等法律法规，《国家突发公共事件总体应急预案》《突发事件应急预案管理办法》《国家网络安全事件应急预案》《关于加强教育行业网络与信息安全工作的指导意见》《信息安全技术信息安全事件分类分级指南》(GB/Z 20986-2007)等文件。

1.3 适用范围

本预案适用于各级教育行政部门及其直属单位（以下简称教育行政部门)、各级各类学校、中国教育和科研计算机网（以下简称教育网)。按照《国家网络安全事件应急预案》规定，本预案所指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，可分为有害程序事件、网络攻击事件、信息破坏事件、设备设施故障、灾害性事件和其他事件。信息内容安全事件的应对，参照有关规定和办法。

1.4 事件分级

参照《国家网络安全事件应急预案》事件分级规定，根据教育系统特点，可能造成的危害，可能发展蔓延的趋势等，教育系统网络安全事件分为四级：特别重大网络安全事件、重大网络安全事件、较大网络安全事件、一般网络安全事件。

（1）符合下列情形之一的，为特别重大网络安全事件（Ⅰ级）：

①教育网全国或多省份范围大量用户无法正常上网。

②.edu.cn 域名的权威系统解析效率大幅下降。

③关键信息基础设施或统一运行的核心业务信息系统（网站）遭受特别严重损失，造成系统大面积瘫痪，丧失业务处理能力。

④网络病毒在全国教育系统或多省教育系统大面积爆发。

⑤关键信息基础设施或统一运行的核心业务信息系统（网站）的重要敏感信息或关键数据丢失或被窃取、篡改。

⑥其他对教育系统安全稳定和正常秩序构成特别严重威胁，造成特别严重影响的网络安全事件。

（2）符合下列情形之一且未达到特别重大网络安全事件的，为重大网络安全事件（Ⅱ级）：

①教育网一个省份大量用户无法正常上网。

②关键信息基础设施或核心业务信息系统（网站）遭受严重系统损失，造成系统瘫痪，业务处理能力受到重大影响。

③网络病毒在一个省的教育系统范围内大面积爆发。

④核心业务信息系统（网站）的重要敏感信息或关键数据发生丢失或被窃取、篡改。

⑤其他对教育系统安全稳定和正常秩序构成严重威胁，造成严重影响的网络安全事件。

（3）符合下列情形之一且未达到重大网络安全事件的，为较大网络安全事件（Ⅲ级）：

①教育网一个单位大量用户无法正常上网。

②重要业务信息系统（网站）遭受较大系统损失，明显影响系统效率，业务处理能力受到影响。

③网络病毒在教育系统多个单位范围内广泛传播。

④重要业务信息系统（网站）的信息或数据发生丢失或被窃取、篡改、假冒。

⑤其他对教育系统安全稳定和正常秩序构成较大威胁，造成较大影响的网络安全事件。

（4）一般网络安全事件（Ⅳ级）：

除上述情形外，对教育系统安全稳定和正常秩序构成一定威胁、造成一定影响的网络安全事件，为一般网络安全事件。

1.5 工作原则

（1）统一指挥、密切协同。教育部网络安全和信息化领导小组（以下简称部网信领导小组）统筹协调教育系统网络安全应急指挥工作，建立与国家网络安全职能部门、专业机构等多方参与的协调联动机制，加强预防、监测、报告和应急处置等环节的紧密衔接，做到快速响应、正确应对、果断处置。

（2）分级管理、强化责任。按照属地化管理原则，省级以下（含省级）教育行政部门在本地党委和政府领导下，负责本地区教育系

统网络安全应急工作。按照“谁主管谁负责、谁运维谁负责”的原则，各级党委（党组）对本地区本单位网络安全工作负主体责任。领导班子主要负责人是网络安全工作第一责任人。

（3）预防为主、平战结合。坚持事件处置和预防工作相结合，做好事件预防、预判、预警工作，加强应急支撑保障能力和安全态势感知能力建设。提高网络安全事件快速响应和科学处置能力，抓早抓小，争取早发现、早报告、早控制、早解决，严控网络安全事件风险和影响范围。

2 组织机构与职责

2.1 领导机构与职责

部网信领导小组统筹协调教育系统全局性网络安全事件应急工作，指导各级教育行政部门、各级各类学校网络安全事件应急处置；发生特别重大网络安全事件时，成立教育系统网络安全事件应急工作组（以下简称工作组），负责组织指挥和协调事件处置，并根据实际情况吸纳相关教育行政部门、业务主管单位和教育网网络中心等参加应对工作。

2.2 办事机构与职责

在部网信领导小组的领导下，教育部网络安全应急办公室（以下简称部网络安全应急办）负责网络安全应急管理事务性工作，对接国家网络安全应急办公室和网络安全职能部门，向部网信领导小组报告网络安全事件情况，提出特别重大网络安全事件应对措施建议，统筹组织网络安全监测工作，指导网络安全支撑单位做好应急处置的技术支撑工作。部网络安全应急办的工作由部网信领导小组

办公室承担。

2.3 教育行政部门和学校职责

省级教育行政部门负责统筹协调组织本地区网络安全事件应急工作，做好网络安全事件的预防、监测、报告和应急工作。省级以下（含省级）教育行政部门、学校按照“谁主管谁负责、谁运维谁负责”的原则，参照本预案制定应急预案，承担各自网络安全责任，全面落实各项工作。

2.4 其他单位职责

教育网网络中心负责教育网网络安全事件应急工作；教育网网络中心、教育部教育管理信息中心等单位负责监测、报告网络安全事件和预警信息，为教育系统的网络安全事件应对提供决策支持和技术支撑。

3 监测与预警

3.1 预警分级

建立教育系统网络安全事件预警制度。按照紧急程度、发展态势和可能造成的危害程度，教育系统网络安全事件预警等级分为四级：由高到低依次用红色、橙色、黄色和蓝色表示，分别对应发生或可能发生教育系统特别重大、重大、较大和一般网络安全事件。

3.2 安全监测

3.2.1 事件监测

部网络安全应急办通过多种渠道监测、发现已经发生的教育系统网络安全事件，将掌握的情况立即通知相关省级教育行政部门。各单位对本地区、本单位网络和信息系统（网站）的运行状况进行

密切监测，一旦发生网络安全事件，应当立即通过电话等方式向上级教育行政部门报告，不得迟报、谎报、瞒报、漏报。

3.2.2 威胁监测

部网络安全应急办组织对教育系统网络安全威胁进行监测，建立多方协作的信息共享机制，通过多种途径监测、汇聚漏洞、病毒、网络攻击等网络安全威胁信息，依托教育系统网络安全工作管理平台实现安全威胁信息的收集、校验、发布、跟踪。各单位加强对本地区、本单位网络和信息系统（网站）的网络安全威胁监测，对发生的威胁及时进行处置和上报。

3.3 预警研判和发布

各级教育行政部门对监测信息进行研判，对发生网络安全事件的可能性及其可能造成的影响进行分析评估，认为需要立即采取防范措施的及时通知有关单位；认为可能发生重大以上（含重大）网络安全事件的信息，应立即向部网络安全应急办报告。

各省级教育行政部门可根据监测研判情况，发布本地区的橙色以下（含橙色）预警。部网络安全应急办研判，提出发布红色预警和涉及多地区预警的建议，报部网信领导小组批准后统一发布。对达不到预警级别但又需要发布警示信息的，部网络安全应急办和各省级教育行政部门可发布风险提示信息。

预警信息包括预警级别、起始时间、可能影响范围、警示事项、应采取的措施、时限要求和发布机关等。

3.4 预警响应

3.4.1 红色预警响应

（1）部网络安全应急办组织预警响应工作，联系有关部门、专业机构和专家，组织对事态发展情况进行跟踪研判，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，重要情况报部网信领导小组。

（2）组织跟踪和分析研判，密切关注事态发展，做好监测分析和信息搜集工作；开展应急处置或准备、风险评估；密切关注舆情动态，加强教育引导，采取有效措施管控风险。

（3）有关单位按照部网络安全应急办要求，实行24小时值守，相关人员保持通信联络畅通。

（4）部网络安全应急办做好与专业机构沟通协调的准备工作；安全技术支撑部门进入待命状态，研究制定应对方案，检查设备、软件工具等，确保处于良好状态。

3.4.2 橙色预警响应

（1）教育部、省级教育行政部门网络安全职能部门启动相应应急预案，组织开展预警响应工作，做好风险评估、应急准备和风险控制工作。

（2）省级教育行政部门及时将事态发展情况报部网络安全应急办。部网络安全应急办密切关注事态发展，有关重大事项及时通报有关单位。

（3）相关应急技术支撑队伍保持联络畅通，检查应急设备、软件工具等，确保处于良好状态。

3.4.3 黄色、蓝色预警响应

各级教育行政部门根据预案，组织做好预警响应工作。

3.5 预警解除

预警发布部门根据实际情况，确定是否解除预警，及时发布预警解除信息。

4 应急处置

4.1 初步处置

网络安全事件发生后，事发单位应立即启动应急预案，立即组织本单位的应急队伍和工作人员根据不同的事件类型和事件原因，采取科学有效的应急处置措施，尽最大努力将影响降到最低，并注意保存网络攻击、网络入侵或网络病毒等证据。经分析研判，初判为特别重大、重大网络安全事件的，应立即报告部网络安全应急办；对于人为破坏活动，应同时报当地网信部门和公安机关。部网络安全应急办组织研判，认定为特别重大网络安全事件的，报部网信领导小组和国家网络安全应急办公室。

4.2 应急响应

网络安全事件应急响应分为Ⅰ级、Ⅱ级、Ⅲ级、Ⅳ级等四级，分别对应教育系统特别重大、重大、较大和一般网络安全事件。由国家网络安全应急办公室研判确定为国家级特别重大网络安全事件的，由国家网络安全应急办公室统一组织应急处置工作，具体要求以国家网络安全应急办公室部署为准。

4.2.1 Ⅰ级响应

发生特别重大网络安全事件，由部网络安全应急办向部网信领导小组提出启动Ⅰ级响应的建议，经批准后，成立工作组。

（1）启动指挥体系

①工作组进入应急状态，履行应急处置工作统一领导、指挥、协调的职责。工作组成员保持24小时联络畅通，部网络安全应急办24小时值守。

②有关单位网络安全职能部门进入应急状态，在工作组的统一领导、指挥、协调下组织人员开展应急处置或支援保障工作，启动24小时值守，并派员参加部网络安全应急办工作。

（2）掌握事件动态

①跟踪事态发展。事发单位与部网络安全应急办保持联系，及时填写《教育系统网络安全事件情况报告》，将事态发展变化情况和处置进展情况上报部网络安全应急办。

②检查影响范围。有关单位立即全面了解本地区、本单位主管的网络和信息系统是否受到事件的波及或影响，并将有关情况及时报部网络安全应急办。

③及时通报情况。部网络安全应急办负责整理上述情况，重大事项及时报工作组和国家网络安全应急办公室，并通报有关单位。

（3）决策部署

工作组组织有关单位、专家组、应急技术支撑队伍等方面及时研究对策意见，对处置工作进行决策部署。

（4）处置实施

①控制事态防止蔓延。采取各种技术措施、管控手段，最大限度阻止和控制事态蔓延。

②消除隐患恢复系统。根据事件发生原因，针对性制定解决方案，备份数据、保护设备、排查隐患。对业务连续性要求高的受破

坏网络与信息系统要及时组织恢复。

③调查取证。事发单位应在保留相关证据的基础上，开展问题定位和溯源追踪工作。积极配合当地网信部门和公安机关开展调查取证工作。

④信息发布。教育部新闻办根据实际，组织网络安全突发事件的应急新闻工作，指导协调各单位开展新闻发布和舆论引导工作。未经批准，其他单位不得擅自发布相关信息。

⑤协调国家支持。处置中需要技术及工作支持的，由部网络安全应急办根据实际，报请工作组批准后，商国家网络安全应急办予以支持。

⑥次生事件处置。对于引发或可能引发其他安全事件的，部网络安全应急办应及时按程序上报。在相关部门应急处置中，部网络安全应急办做好协调配合工作。

4.2.2 Ⅱ级响应

网络安全事件的Ⅱ级响应，由事发单位所在的省级教育行政部门或部网络安全应急办确定并发布。

（1）响应发布单位进入应急状态，按照相关应急预案做好应急处置工作。

（2）事发单位及时填写《教育系统网络安全事件情况报告》，报所在省级教育行政部门，由省级教育行政部门报部网络安全应急办。部网络安全应急办将有关重大事项及时通报部网信领导小组和有关单位。

（3）处置中需要其他单位和网络安全应急技术支撑队伍配合和

支持的，商部网络安全应急办予以协调。

（4）有关单位根据通报，结合各自实际有针对性地加强防范，防止造成更大范围影响和损失。

4.2.3 Ⅲ级和Ⅳ级响应

事件发生单位按相关预案进行应急响应。

4.3 应急结束

4.3.1 Ⅰ级响应结束

部网络安全应急办提出建议，报工作组批准后，及时通报有关单位。

4.3.2 Ⅱ级响应结束

部网络安全应急办和省级教育行政部门根据实际决定Ⅱ级响应的结束。省级教育行政部门结束应急响应应报部网络安全应急办。

4.3.3 Ⅲ级、Ⅳ级响应结束

由事发单位完成应急处置后，自行解除Ⅲ级、Ⅳ级响应状态。

5 调查与评估

特别重大网络安全事件由部网络安全应急办组织有关单位开展调查处理和总结评估工作，并将调查评估结果汇总上报部网信领导小组及国家网络安全应急办公室。重大网络安全事件根据事发单位属性，由部网络安全应急办或省级教育行政部门组织开展调查处理和总结评估工作。省级教育行政部门应将调查评估结果汇总上报部网络安全应急办。较大和一般网络安全事件由事发单位自行组织开展调查处理和总结评估工作。

网络安全事件总结调查报告应对事件的起因、性质、影响、责

任等进行分析评估，提出处理意见和改进措施。网络安全事件的调查处理和总结评估工作应在应急响应结束后5天内完成。

6 预防工作

6.1 日常管理

各单位应做好网络安全事件日常预防工作，根据本预案制定完善相关的专项应急预案和配套的管理制度，建立完善的应急管理体制。按照网络安全等级保护、关键信息基础设施防护等相关要求落实各项防护措施，做好网络安全检查、风险评估和容灾备份，加强信息系统的安全保障能力。

6.2 监测预警和通报

各单位应加强网络安全监测预警和通报，及时发现并处置安全威胁。各省级教育行政部门应全面掌握本地区信息系统（网站）情况，建立本地区的网络安全监测预警和通报机制，并指导、监督本地区教育机构及时修复安全威胁，全面排查安全隐患，提高发现和应对网络安全事件的能力。

6.3 应急演练

部网络安全应急办每年组织针对特别重大网络安全事件的跨地区、跨层级的应急演练，检验和完善预案，提高实战能力。各单位每年至少组织一次应急演练，每年年底前将本年度演练情况报部网络安全应急办。

6.4 宣传教育

各单位应将网络安全教育作为国家安全教育的重要内容，加强突发网络安全事件预防和处置的有关法律、法规和政策的宣传教育。

同时，充分利用网络安全周等各种活动形式和传播媒介，开展网络安全基本知识和技能的宣传活动，提高在校师生的网络安全意识。

6.5　工作培训

各单位应定期组织网络安全培训，将网络安全事件的应急知识列为领导干部和有关人员的培训内容，加强网络安全特别是网络安全事件应急预案的学习，提高网络安全管理和技术人员的防范意识及安全技能。

7 工作保障

7.1　机构和人员

各单位应落实网络安全应急工作责任制，明确网络安全职能处室，并将网络安全应急工作作为重点工作予以部署。按照“谁主管谁负责”的原则，把网络安全应急工作责任落实到具体部门、具体岗位和个人，建立健全应急工作机制。

7.2　技术支撑

各省级教育行政部门、部属高校和有条件的直属单位，应明确或建立网络安全技术支撑单位，加强网络安全应急技术支撑队伍建设和网络安全物资保障，做好网络安全事件的监测预警、预防防护、应急处置、应急技术支援工作。

7.3　专家队伍

教育部建立教育系统网络安全专家组，完善专家研判分析与支撑保障机制，为网络安全事件的预防和处置提供技术咨询和决策建议。各省级教育行政部门根据地方实际，建立本地区的网络安全专家咨询队伍，提高应急保障能力。

7.4　基础平台

教育部加强教育系统网络安全管理平台建设，通过平台通报网络安全事件信息和网络安全威胁信息，增强教育系统网络安全预警和态势感知能力。各省级教育行政部门加强监测通报和应急管理信息化平台建设，并与我部平台实现数据的双向共享，建立教育系统网络安全态势感知体系，做到早发现、早预警、早响应，提高应急处置能力。

7.5　信息共享与应急合作

加强与网络安全职能部门、网络安全专业机构、行业学会和教育网网络中心等单位的合作，建立网络安全威胁的信息共享机制和网络安全事件的快速发现和协同处置机制。

7.6　经费保障

各单位应为网络安全应急工作提供必要的经费保障，利用现有政策和资金渠道，支持网络安全应急技术支撑队伍建设、专家队伍建设、基础平台建设、监测通报、宣传教育培训、预案演练、物资保障等工作开展。

7.7　责任与奖惩

各级教育行政部门可对网络安全事件应急管理工作中作出突出贡献的先进集体和个人给予表彰和奖励；对不按照规定制定预案和组织开展演练，迟报、谎报、瞒报和漏报网络安全事件重要情况或者在应急管理工作中有其他失职、渎职行为的，依照相关规定对有关责任人给予处分；构成犯罪的，依法追究刑事责任。

8 附则

8.1 预案管理

本预案原则上每年评估一次，根据实际情况适时修订。修订工作由部网络安全应急办组织。

各单位要根据本预案制定或修订本单位、本地区的网络安全事件应急预案。各预案要做好与本预案的衔接，并报部网络安全应急办。

8.2 预案解释

本预案由部网络安全应急办负责解释。

8.3 预案实施时间

本预案自印发之日起实施。

（此件依申请公开）

部内发送：有关部领导，办公厅

教育部办公厅　　2018 年 6 月 13 日印发