

不忘初心，牢记使命
构筑网络安全自信，建设网络强国新时代

教育部科技司 2017.11

CONTENTS 目录

- 1 充分认识网络安全工作的极端重要性
- 2 教育系统网络安全工作的体制机制
- 3 教育系统网络安全工作及面临的新形势
- 4 新时期教育系统网络安全工作思考

**充分认识网络安全工作的
极端重要性**

01



以习近平同志为核心的党中央高度重视网络安全工作

成立一个领导小组

中央网络安全和信息化领导小组，加强统一领导

提出一个重要论述

“没有网络安全就没有国家安全，没有信息化就没有现代化”

召开一次座谈会

发表4·19重要讲话，六个方面的问题

建设一个强国

党的十九大报告，再次提及建设网络强国





国家的长治久安，党的前途命运

互联网是我们面临的“最大变量”。

过不了互联网这一关,就过不了长期执政这一关。

坚持总体国家安全观。 统筹发展和安全，增强忧患意识，做到居安思危，是我们党治国理政的一个重大原则。必须坚持国家利益至上，以人民安全为宗旨，以政治安全为根本，统筹外部安全和内部安全、国土安全和国民安全、传统安全和非传统安全、自身安全和共同安全，完善国家安全制度体系，加强国家安全能力建设，坚决维护国家主权、安全、发展利益。

教育网络安全离国家安全远吗？





网络空间不是“法外之地”

网络空间是虚拟的，但运用网络空间的主体是现实的，大家都应该遵守法律，明确各方权利义务。要坚持**依法治网、依法办网、依法上网**，让互联网在法治轨道上健康运行。

2016年11月7日，十二届全国人大常委会第24次会议审议通过
2017年的6月1日，正式实施



中华人民共和国 网络安全法

含草案说明

中国法制出版社

宣传 教育



第一集 《透明的时代》

第二集：《隐秘的威胁》

第三集 《真实的较量》

大数据时代，所行所思、消费习惯、行程安排、关系网络，数字巨头比你更了解你自己，获取便利的同时也签署条约共享个人信息。

光缆的尽头是宝藏，数据引来贪婪的窥探者。

一组代码，可能导致个人倾家荡产，国家基础设施瘫痪，风险隐于键盘之上。

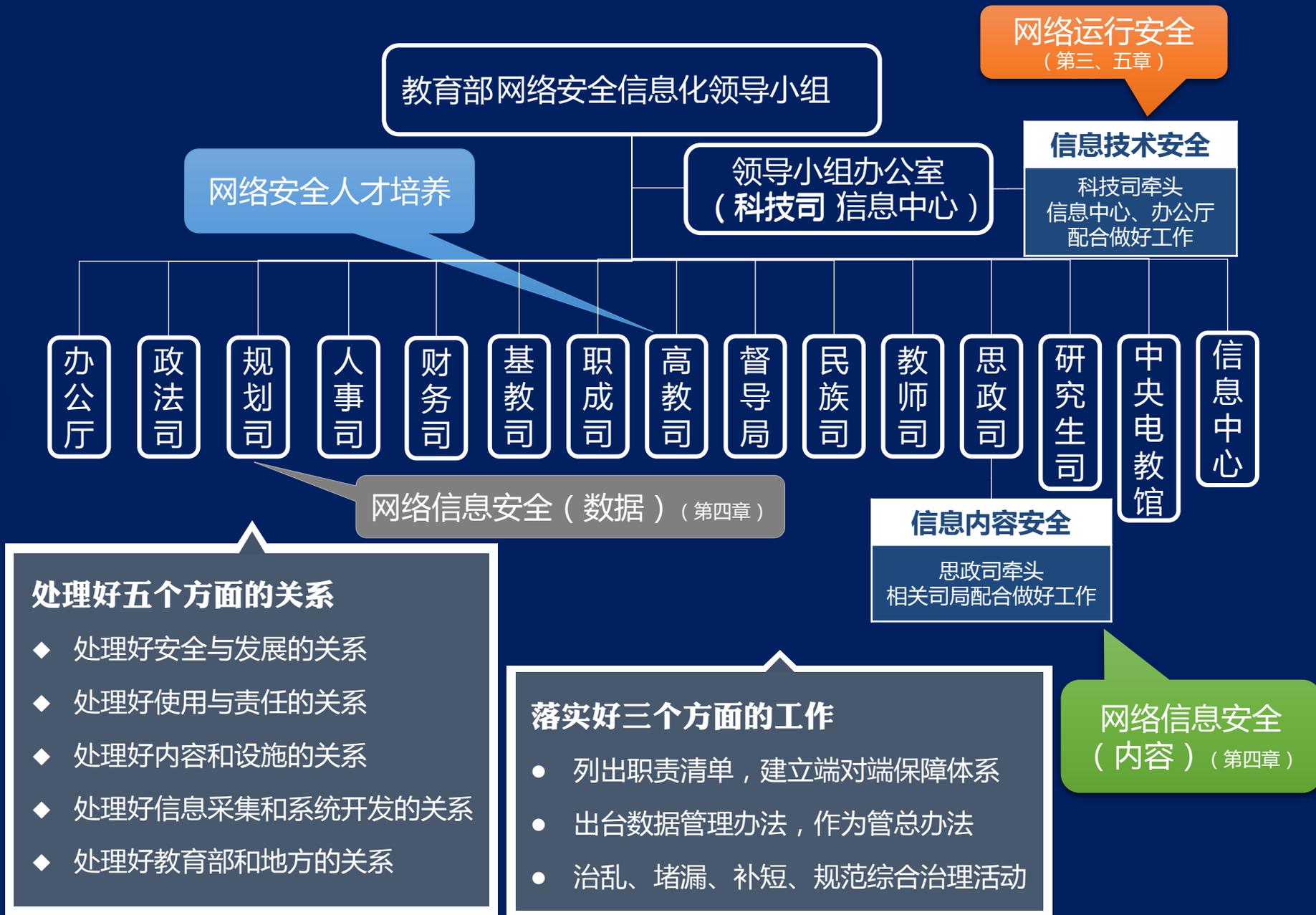
网络空间成为继陆地、海洋、天空、外空之外的第五空间。虚拟空间和现实世界深度融合，面对不断涌现的各种已知和未知的网络安全威胁，我们能够找到守护人类命运共同体的密钥吗？

**教育系统网络安全工作的
体制机制**

02



领导体制





责任 机制





政策体系

加强教育行业网络与信息安全工作的指导意见

领导体系 (第八条)

成立教育部网络安全和信息化领导小组

分级管理，逐级负责，明确责任分工

主体责任、领导责任、信息系统安全责任

管理制度 (第21、32、52条)

联合公安部全面推进信息安全等级保护制度

组织开展部属单位信息安全等级保护工作

教育行业信息系统安全等级保护定级工作指南

等级保护制度 (第三章)

安全防护能力 (第21、25、34条等)

漏洞、病毒、攻击、侵入、灾备、加密

教育信息化专项经费支持软硬件建设

监测应急处置 (第五章)

建立网络安全通报机制

启动信息系统安全监测预警

发布信息技术安全事件报告与处置流程

人员培训 (第19、34条)

2015、2017年组织网络安全培训班

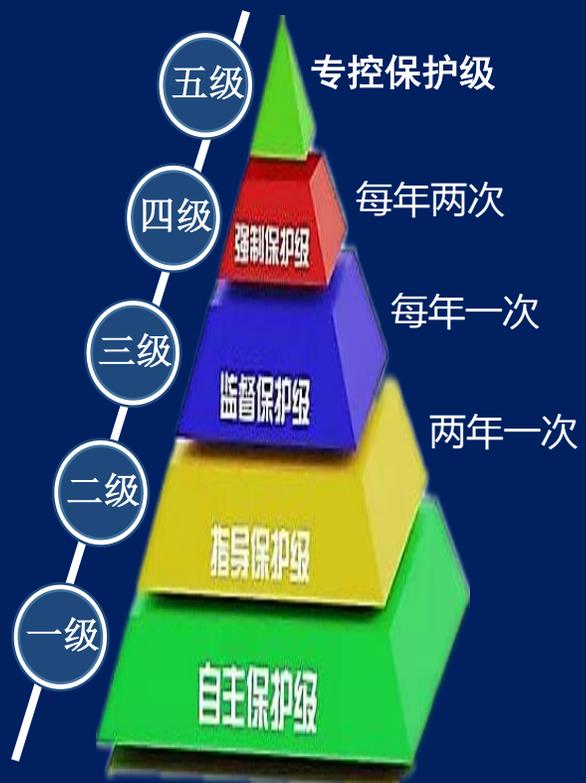
标准规范 (第15条)

教育业务管理信息系统建设子项目管理细则

教育行业网络安全应急预案



等保制度



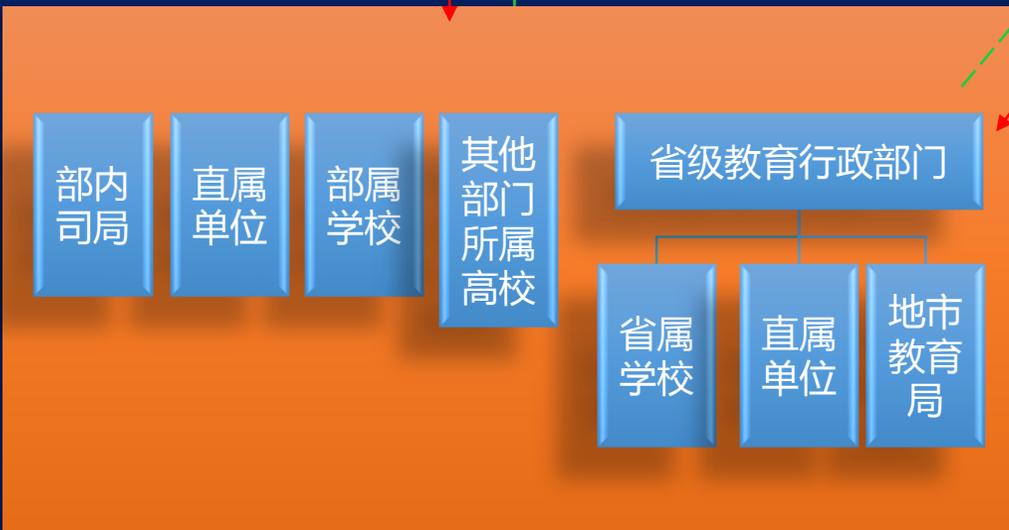
关键信息基础设施



监测制度

网络安全威胁

- 漏洞监测
- 后门监测
- 暗链监测
- DOS攻击监测
- 钓鱼网站监测



校园及周边治安综合治理网络安全方面考核评价



评价制度

序号	内容	工作要求	评分标准	分值
1	建立网络安全通报机制	应明确本单位的网络安全分管负责人、职能处室和联络员，网络安全技术支撑单位和联络员。相关信息应上传至教育行业信息技术安全工作管理平台，相关信息变更应及时更新。	已上传相关信息：不扣分； 未上传相关信息：扣5分； 上传信息不准确：扣1分。	5
2	建立网络安全责任制	主要负责人应签订《教育行业网络安全承诺书》，主要负责人发生变更，应重新签订《教育行业网络安全承诺书》。	签订安全承诺书：不扣分； 未签订安全承诺书：扣5分。	5
3	等级保护定级备案工作	应在6月1日前完成本单位信息系统（网站）的定级备案工作。	按时全部完成定级备案工作：不扣分； 按时完成定级但未完成备案工作：每个系统扣1分； 未按时完成定级备案工作，每个系统扣3分。	30
4	网络安全威胁通报工作	对于通报的安全威胁，包括漏洞、后门、暗链、弱口令等，应在通报函件印发日起15天内完成修复工作，	按时处置安全威胁：不扣分； 未按时处置安全威胁：一个扣1分。	25
5	重要时期网络安全保障工作	重要时期应按照统一部署，每天履行报平安制度，有事件报事件，无事件报平安。	按时报平安：不扣分； 未按时报平安：一天扣0.5分。	15
6	网络安全事件处置	发生网页篡改事件，应按照《信息技术安全事件报告与处置流程》的要求，自启动通报程序15分钟内完成紧急处置，切断涉事系统的网络访问。	未发生安全事件，或发生安全事件及时处置：不扣分； 发生安全事件，处置不及时：一次扣10分。	20



培训 制度

培训期数：4期，管理人员培训两期，由教育部科技司负责；技术人员培训两期，由教育部教育管理信息中心负责。

培训对象：管理人员培训的对象为省级教育行政部门、部内司局、直属单位、部属高校的信息技术安全分管负责人和职能处室负责人，中国教育和科研计算机网络网络信息中心相关负责同志。

技术人员培训的对象为省级教育行政部门、直属单位、部属高校、中国教育和科研计算机网络网络信息中心的信息技术安全支撑部门相关负责人和业务骨干。

培训时间：4月至6月期间，在国家教育行政学院、中国石油大学（华东）、武汉移动培训基地、浙江省杭州市举办。

网络培训：会同国家教育行政学院，9月至11月开展，3000人

**教育系统网络安全工作
及面临的新形势**

03

总体工作部署

1-8月

网络安全综合治理行动

为服务保障党的十九大网络安全工作奠定基础。

为服务保障党的十九大网络安全做冲刺准备

服务保障党的十九大通知

8月

9月

做好重要时期保障的通知

做好党的十九大召开期间的重要时期保障工作

针对召开期间的情况再次强调重点要求

做好关键节点保障的通知

10月

网络安全综合治理行动

治理网站乱象

- 1.规范网站标识工作；
- 2.规范网站内容发布；
- 3.规范网站域名工作。

01

补齐等保短板

- 1.完成等级保护定级备案工作；
- 2.开展等保测评工作。

03

堵塞安全漏洞

- 1.持续推进网络安全监测工作；
- 2.开展通用软件检测工作

02

规范安全管理

- 1.规范数据管理
- 2.规范关键信息基础设施管理；
- 3.规范应急管理。

04



综合治理行动成效

总数：1+32
挂标：1+26
比例：81%

统一标识

整改网站：
10000个
涉及个人隐私
信息发布

信息发布

调查：
3200个单位
结果：
2/3境外域名

域名清理

总数：27024
漏洞：18426
后门：2766
暗链：5832

监测预警

调查：
340所学校
38%事件有关
筛选10个系统

检测风险

总数：
53+265
结果：6月1日
全部完成

定级备案

总数：53个
完成：29个

测评整改

编制《教育部
数据管理办法》

数据管理

部直属机关
拟定：28个
行业拟定：
136个

关键信息基础设施

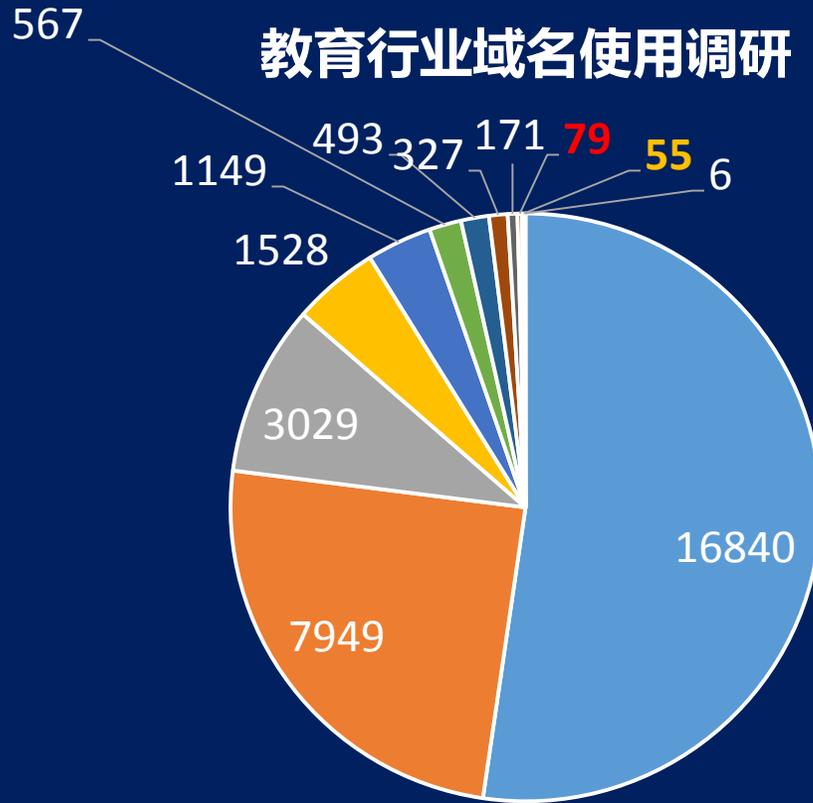
处置：36起
编制：行业网
络安全事件应
急预案

应急响应

网站域名清理

域名	教育行政部门	学校	总计
.com	316	16524	16840
.cn	268	7681	7949
.net	188	2841	3029
edu.cn	29	1499	1528
com.cn	48	1101	1149
gov.cn	411	156	567
.org	26	467	493
net.cn	32	295	327
org.cn	4	167	171
.me	0	79	79
.cc	4	51	55
.info	2	4	6

教育行业域名使用调研



- .com
- .cn
- .net
- edu.cn
- com.cn
- gov.cn
- .org
- net.cn
- org.cn
- .me
- .cc
- .info

.me是黑山共和国的顶级域名，.cc是科科斯群岛的顶级域名

通用软件检测

前期准备：

选取300多个教育机构作为调研对象，进行摸底调查。

调研分析：

85%的学生管理系统，87%的办公系统，89%的教务系统，97%的财务系统使用了通用软件。

事件分析：

38%的反共黑客事件与通用软件漏洞未及时修复升级有关。

检测选择：

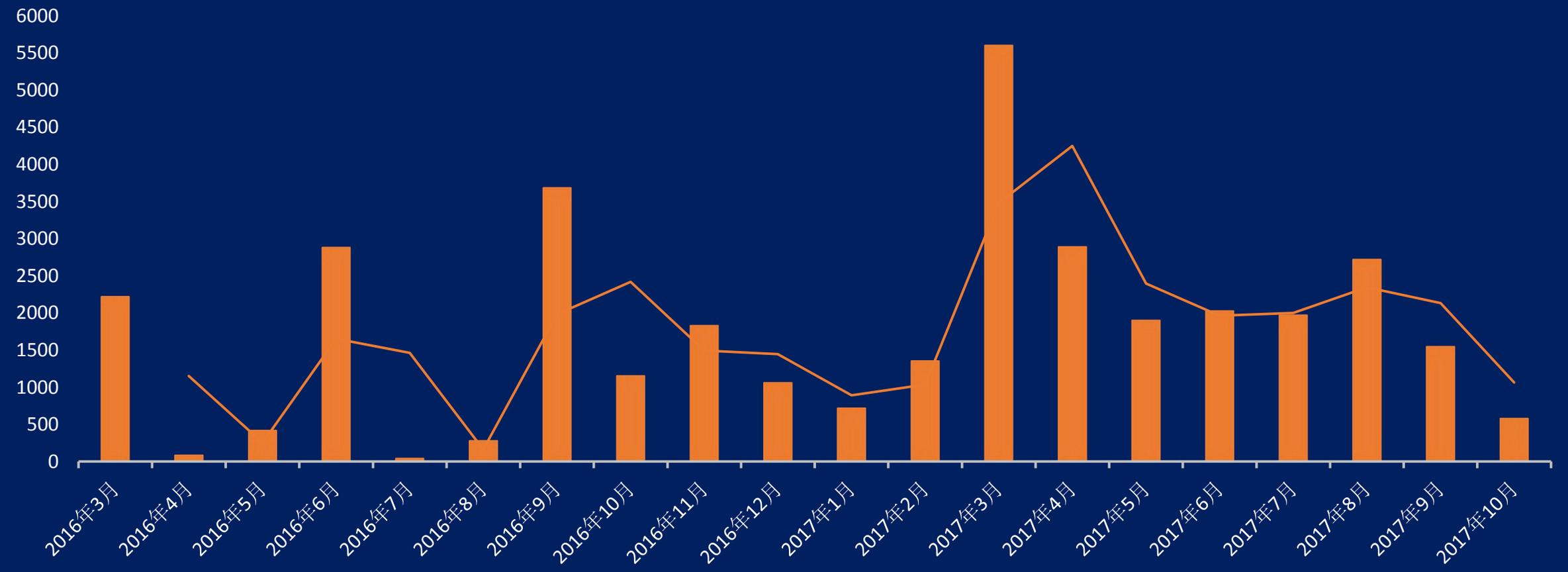
多次通报高危漏洞或发生安全事件，且市场占有率位居前三的9家厂商的10款通用软件产品。

合作机构：

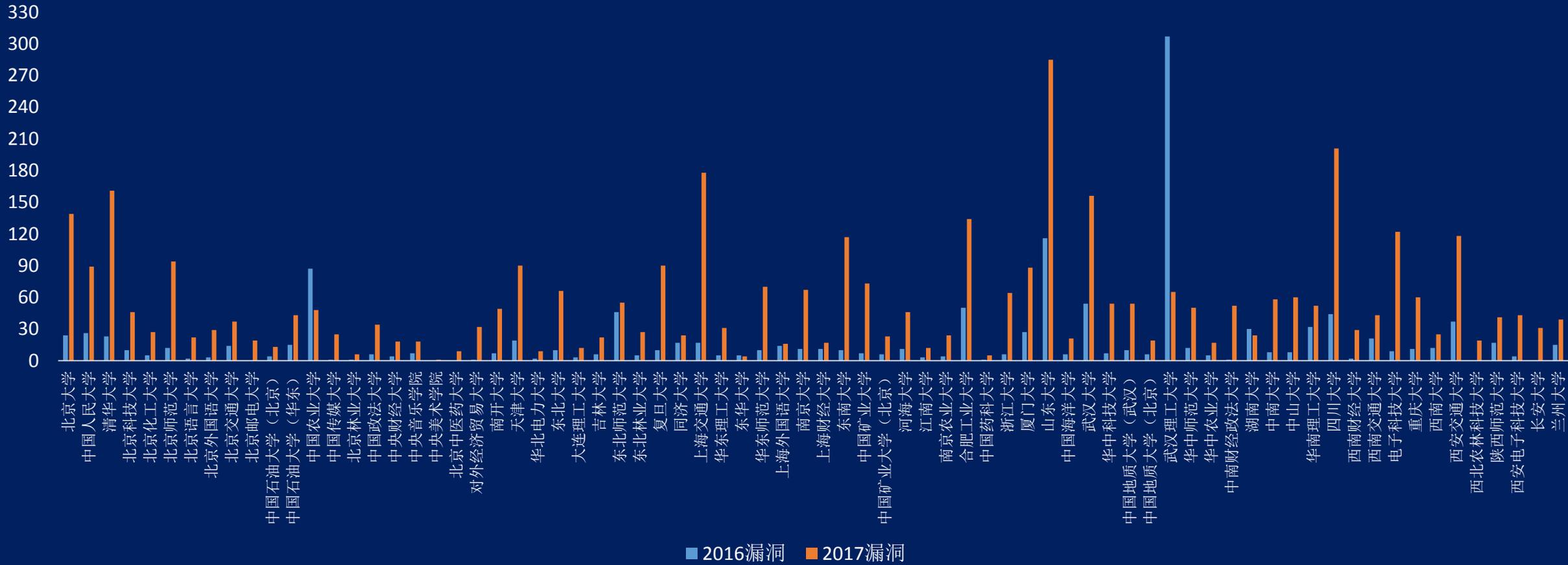
国家信息安全测评中心

类别	公司	产品
迎新系统	浙江正方软件股份有限公司	迎新管理信息系统
财务系统	上海复旦天翼计算机有限公司	天翼财务管理系统
学生系统	浙江正方软件股份有限公司	学生工作管理信息系统
邮件系统	北京亿中邮信息技术有限公司	亿邮电子邮件系统
图书系统	江苏汇文软件有限公司	OPAC书目检索系统
教务系统	湖南青果软件有限公司	青果教务网络管理系统
学生系统	江苏金智教育信息股份有限公司	研究生管理信息系统
档案系统	南京大学档案馆	南大之星档案管理系统
期刊系统	北京玛格泰克科技发展有限公司	期刊稿件远程处理系统
一卡通系统	哈尔滨新中新电子股份有限公司	新中新校园一卡通

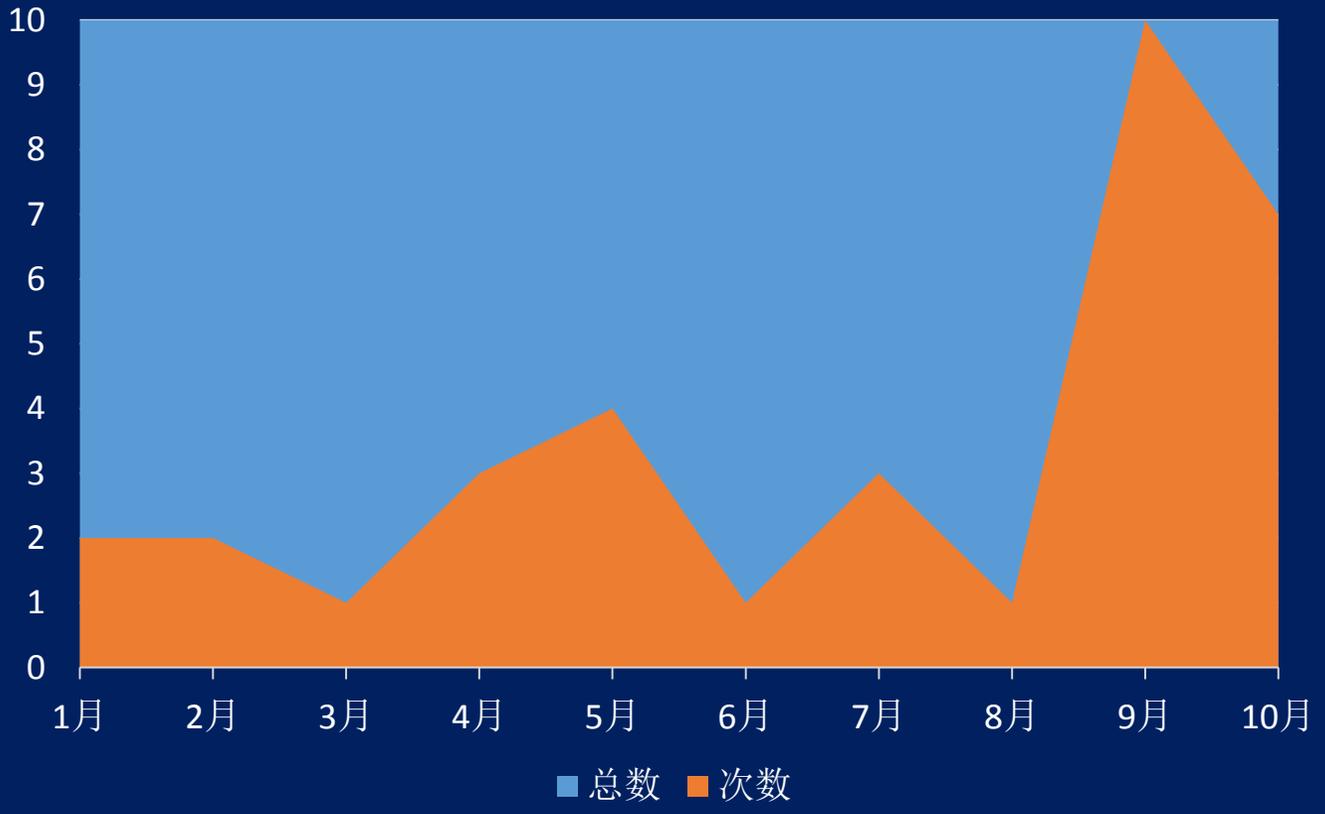
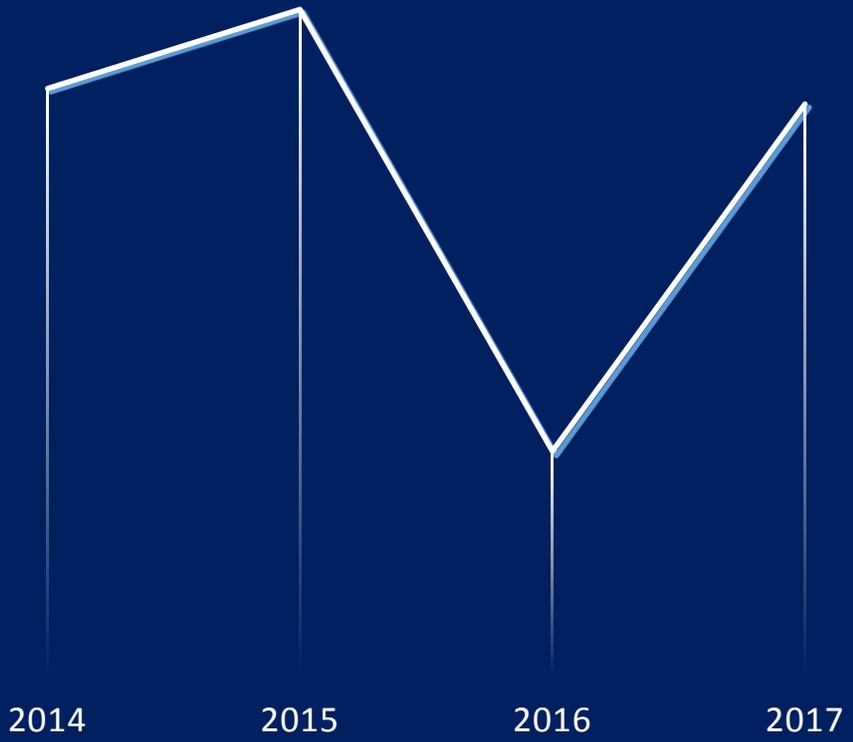
威胁监测预警



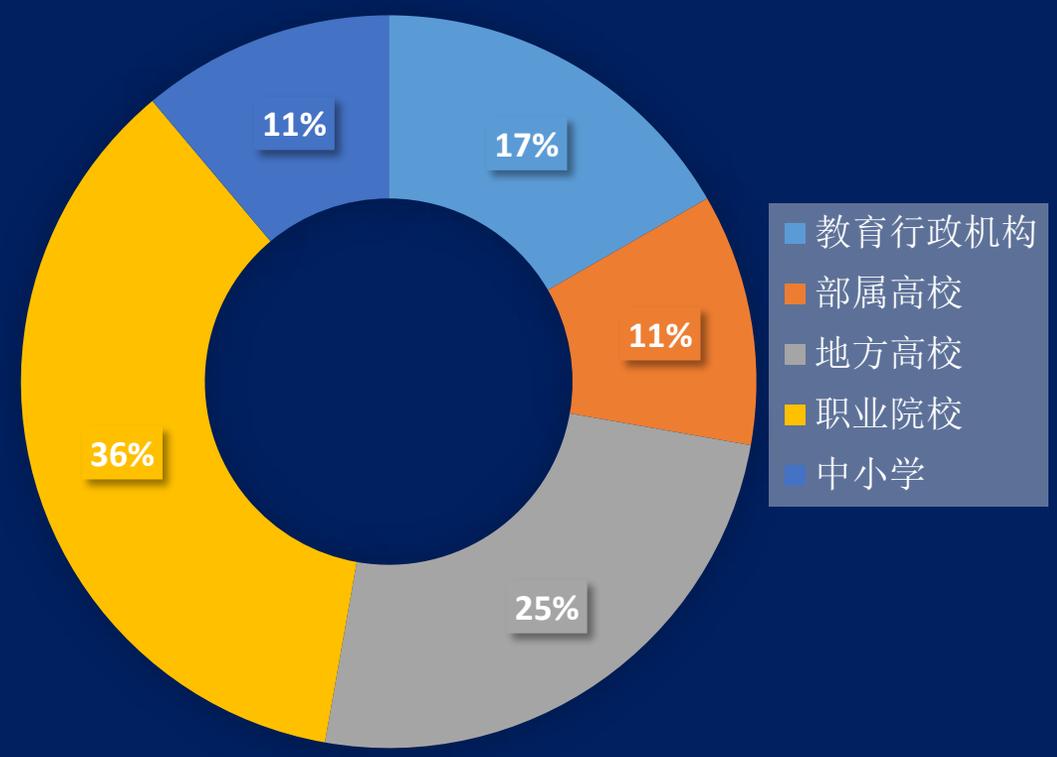
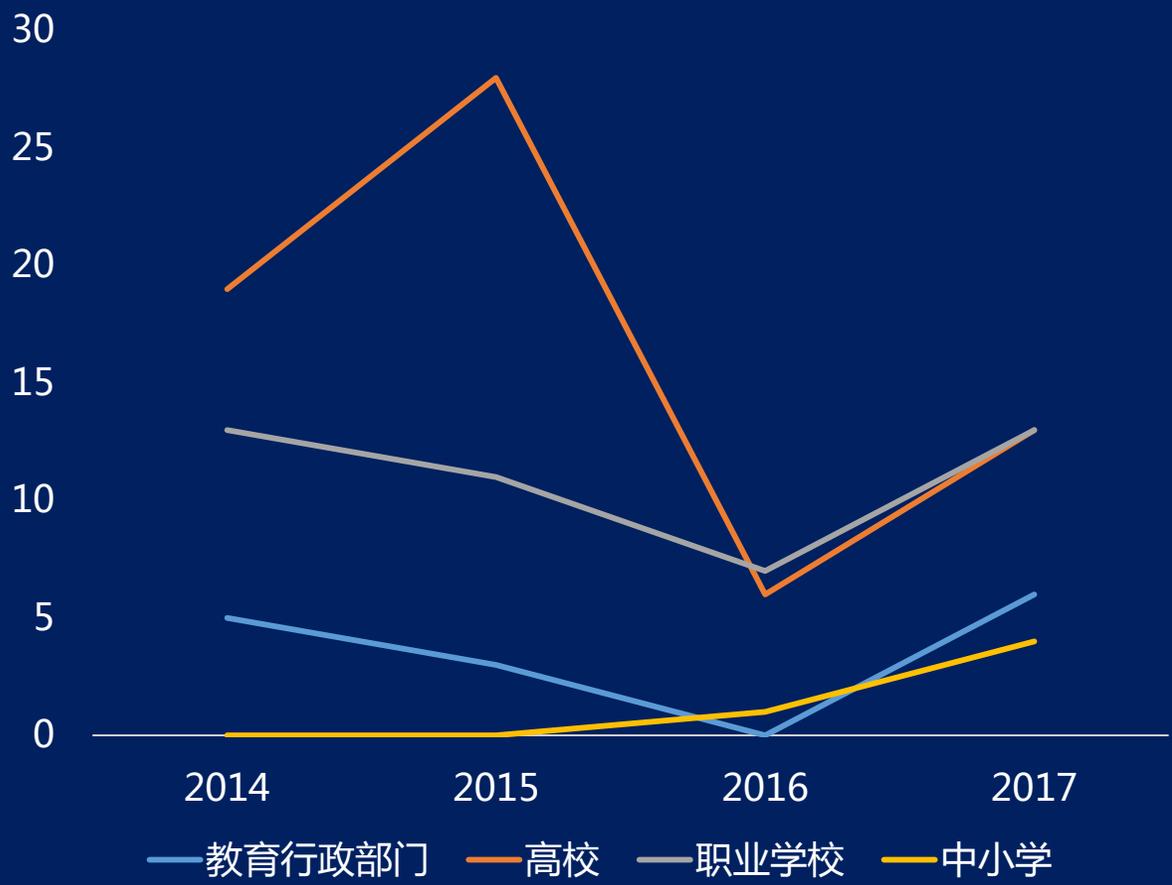
部属高校漏洞



网络安全事件



网络安全事件



四川违反《网络安全法》第一案 启动监管处罚新时代

7月22日，宜宾市翠屏区“教师发展平台”网站因网络安全防护工作落实不到位，导致网站存在高危漏洞，造成网站发生被黑客攻击入侵的网络安全事件。

宜宾网安部门在对事件进行调查时发现，**该网站自上线运行以来，始终未进行网络安全等级保护的定级备案、等级测评等工作，未落实网络安全等级保护制度，未履行网络安全保护义务。**

根据《网络安全法》第五十九条第一款之规定，决定给予翠屏区教师培训与教育研究中心**法定代表唐某某**行政处罚决定，对翠屏区教师培训与教育研究中心处一万元罚款，对法人代表唐某某处五千元罚款。



中华人民共和国 网络安全法

含草案说明

中国法制出版社

学校网站未履行网络安全保护义务 分管副县长被约谈

8月12日，安徽省蚌埠怀远县教师进修学校网站因网络安全防等级保护制度落实不到位，遭黑客攻击入侵。

蚌埠市公安局网安支队调查案件时发现，该网站自上线运行以来，始终未进行网络安全等级保护的定级备案、等级测评等工作，未落实网络安全等级保护制度，未履行网络安全保护义务。

根据《网络安全法》第五十六条之规定，省公安厅网络安全保卫总队约谈怀远县教师进修学校法定代表人、怀远县人民政府**分管副县长**。

《网络安全法》实施以来，首次由省级人民政府公安部门履行网络安全监督管理职责，约谈网络运营者的法定代表人及相关责任人。



中华人民共和国 网络安全法

含草案说明

中国法制出版社

四川多名副校长参与倒卖学生信息被捕

2017年5月初，绵阳网安民警在工作中，发现绵阳本地有人长期通过网络非法获取、贩卖四川省中小學生学籍信息的案件线索，且十分接近信息泄露源头。由于案情重大，绵阳市公安局立即成立了专案组侦办此案，并上报公安部督办。

5月10日、12日，专案组在绵阳将嫌疑人陈某某、龙某某抓获，并从其笔记本电脑中查获学生学籍信息800余万条，这些信息包含了电话、住址、身份证等隐私信息，内容详尽细致。经深入侦查，警方随后抓获了他们的上线李某某，并于5月25日在江苏省镇江市抓获了利用黑客技术入侵教育系统管理平台窃取学生学籍信息的张某。



中华人民共和国 网络安全法

含草案说明

中国法制出版社

**新时期教育系统网络安全
工作思考**

04



不忘初心，牢记使命

构筑网络安全自信，建设网络强国新时代

不忘初心：努力让每个孩子都能享受到公平而优质的教育，办好人民满意的教育

指导思想：习近平新时代中国特色社会主义思想，习近平关于网络安全的系列重要讲话

时代使命：建设教育强国，建设网络强国

总体目标：服务国家安全，保障教育现代化建设，维护师生权益，构筑网络自信

主要矛盾：广大师生对互联网的需求与网络完全和信息化发展不平衡、不充分的矛盾

基本要求：战略思维、辩证思维、法制思维、底线思维、创新思维

主要任务：加强党对网络安全的领导，加强网络安全责任体系建设，加强网络安全制度建设

加强网络安全防护能力，加强网络安全宣传教育

近期重点推进的任务

进一步强化网络安全责任制

1

加强教育系统网络安全制度建设

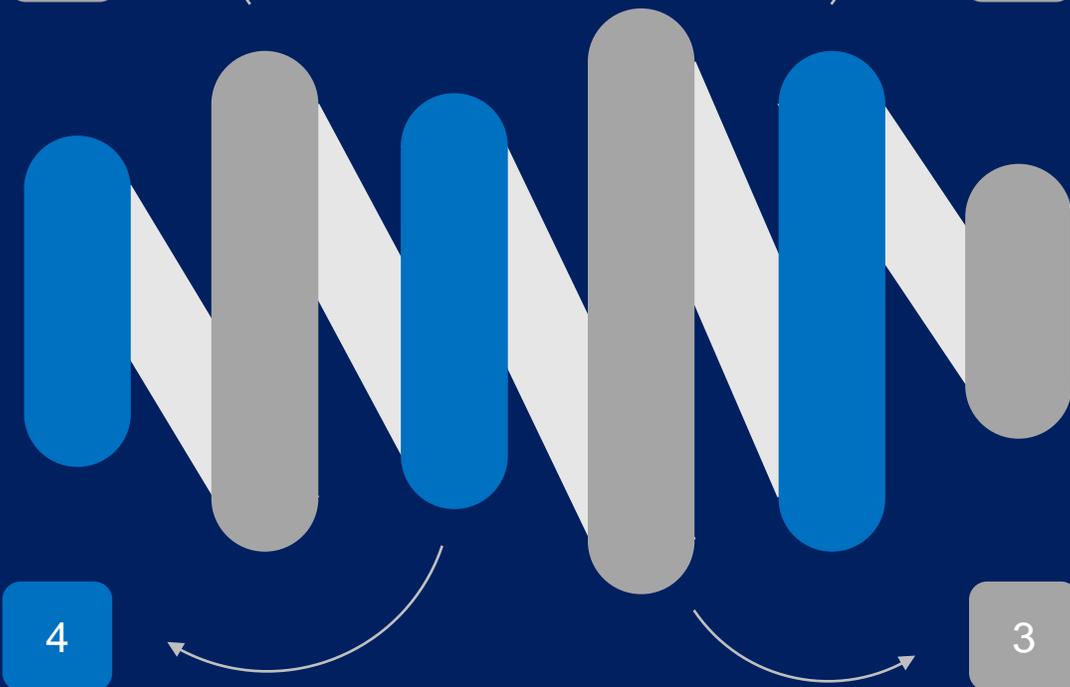
2

深化监测预警与应急处置水平

4

深入实施网络安全等级保护和关键信息基础设施制度

3



感谢聆听