网络信息安全周报

【2017】第 34 期

党委宣传部
信息网络中心 编

2017 年 12 月 21 日

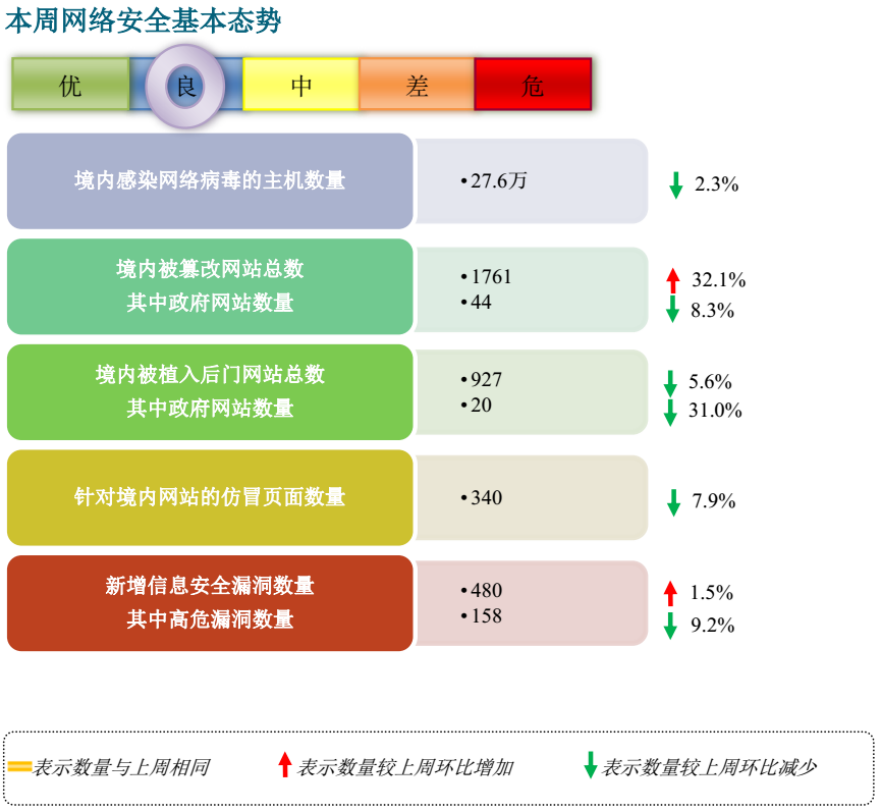
本期要目

- 【权威发布】全国网络安全信息与动态（2017 年 12 月 4 日—10 日）
- 【城院 IT】综合业务管理平台统计信息(2017 年 12 月 11 日—17 日)
- 【学习中国】习近平为“不忘初心、牢记使命”主题教育立规矩

全国网络安全信息与动态

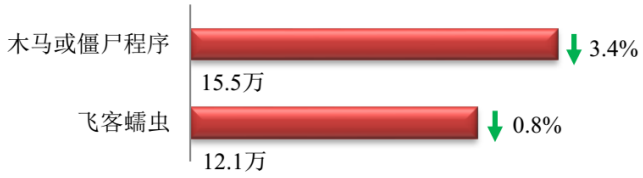
（2017 年 12 月 4 日-12 月 10 日）

根据国家互联网应急中心最新公告数据：



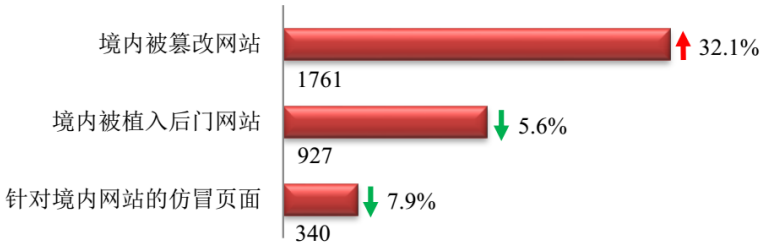
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 27.6 万个，其中包括境内被木马或被僵尸程序控制的主机约 15.5 万以及境内感染飞客（conficker）蠕虫的主机约 12.1 万。



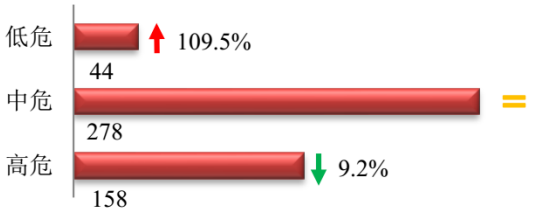
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1761 个；境内被植入后门的网站数量为 927 个；针对境内网站的仿冒页面数量为 340。



本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 480 个，信息安全漏洞威胁整体评价级别为中。



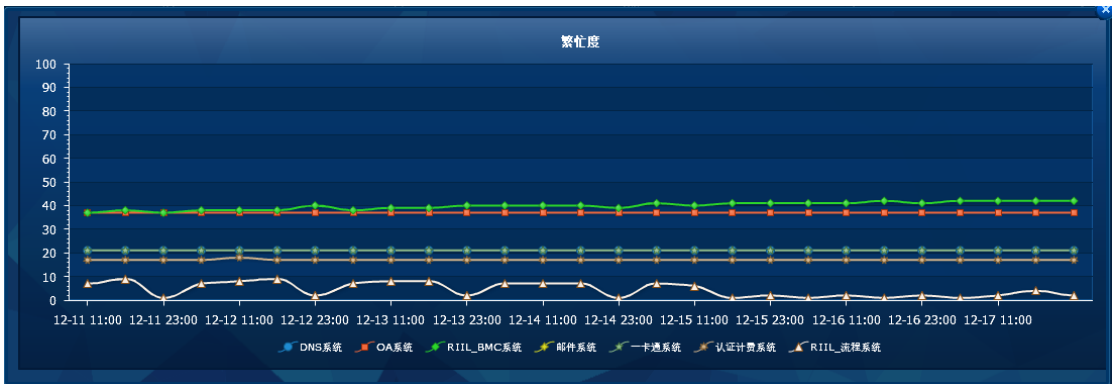
本周事件处理情况

本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 590 起，其中跨境网络安全事件 153 起。

城院 IT 综合业务管理平台统计信息

(2017 年 12 月 11 日—12 月 17 日)

主要业务服务繁忙度



网站集群网页更新情况统计

站点名称【站点帐号】	发布		站点名称【站点帐号】	发布
兰州城市学院	55		发展规划处	
马克思主义学院	9		甘肃省高等学校外语教学指导委员会	
文史学院	8		甘肃文化翻译中心	
就业服务网	7		甘肃张芝书法院	
地理与城乡规划学院	6		国有资产管理处	
传媒学院	5		后勤管理处	
教育学院	5		机关党委	
化学与环境工程学院	4		机械工程学院	
廉政网	4		基本建设处	
路易艾黎研究中心	3		教师发展中心	
音乐学院	3		教学质量监测与评估中心	
教务处	2		卡务中心	
旅游学院	2		科学研究处	
商学院	2		兰州城市学院校医院	
电子与信息工程学院	1		美术与设计学院	
人事处	1		膳食处	
石油工程学院	1		审计	
信息网络中心	1		实训中心	
幼儿师范学院	1		数学学院	
保卫处			体育学院	
城市社会心理研究中心			团委	
城市信息与系统科学研究所			外国语学院	
创新创业学院			网络报修	
档案馆			心理咨询中心	
党委（校长）办公室			信息技术教育与应用研究所	
党委宣传部			学位办公室	
党委学生工作部			音乐研究中心	
党委组织部			招生网	
电子信息科学与技术研究所			职业技能鉴定所	

站群系统应用防火墙入侵防护记录

序号	入侵位置	入侵者IP	归属地	详细信息	入侵方式	入侵时间
191334	站点名称：体育学院	198.204.225.114	美国	含有非法请求参数	SQL注入	2017-12-18 07:04:48
191333	站点名称：体育学院	198.204.225.114	美国	含有非法请求参数	SQL注入	2017-12-18 07:04:48
191332	站点名称：体育学院	198.204.225.114	美国	含有非法请求参数	SQL注入	2017-12-18 07:04:47
191331	站点名称：卡务中心	118.180.5.174	甘肃省兰州市 网宿科技电信CDN节点	含有非法请求参数	SQL注入	2017-12-15 01:10:56
191330	站点名称：卡务中心	118.180.5.174	甘肃省兰州市 网宿科技电信CDN节点	含有非法请求参数	SQL注入	2017-12-15 01:10:56
191329	站点名称：卡务中心	118.180.5.174	甘肃省兰州市 网宿科技电信CDN节点	含有非法请求参数	SQL注入	2017-12-15 01:10:50
191328	站点名称：路易艾黎研究中心	117.25.54.215	福建省福州市 电信	含有非法请求参数	跨站脚本注入	2017-12-13 23:55:33
191327	站点名称：路易艾黎研究中心	117.25.54.215	福建省福州市 电信	含有非法请求参数	跨站脚本注入	2017-12-13 23:55:11
191326	站点名称：路易艾黎研究中心	117.25.54.215	福建省福州市 电信	含有非法请求参数	跨站脚本注入	2017-12-13 23:53:22
191322	站点名称：路易艾黎研究中心	117.25.54.215	福建省福州市 电信	含有非法请求参数	跨站脚本注入	2017-12-13 09:20:11
191321	站点名称：路易艾黎研究中心	117.25.54.215	福建省福州市 电信	含有非法请求参数	跨站脚本注入	2017-12-13 09:19:51
191320	站点名称：路易艾黎研究中心	117.25.54.215	福建省福州市 电信	含有非法请求参数	跨站脚本注入	2017-12-13 09:17:54
191319	站点名称：信息网络中心	42.92.180.12	甘肃省 电信	含有非法请求参数	SQL注入	2017-12-12 21:12:09
191318	站点名称：信息网络中心	42.92.180.12	甘肃省 电信	含有非法请求参数	SQL注入	2017-12-12 21:12:09
191317	站点名称：信息网络中心	42.92.180.12	甘肃省 电信	含有非法请求参数	SQL注入	2017-12-12 21:12:09
191316	站点名称：信息网络中心	61.178.98.70	甘肃省兰州市 电信	含有非法请求参数	SQL注入	2017-12-12 17:11:47
191315	站点名称：信息网络中心	61.178.98.70	甘肃省兰州市 电信	含有非法请求参数	SQL注入	2017-12-12 17:11:47
191314	站点名称：信息网络中心	61.178.98.70	甘肃省兰州市 电信	含有非法请求参数	SQL注入	2017-12-12 17:11:47
191312	站点名称：信息网络中心	61.178.98.70	甘肃省兰州市 电信	含有非法请求参数	SQL注入	2017-12-12 12:41:09
191311	站点名称：信息网络中心	61.178.98.70	甘肃省兰州市 电信	含有非法请求参数	SQL注入	2017-12-12 12:41:09
191310	站点名称：信息网络中心	61.178.98.70	甘肃省兰州市 电信	含有非法请求参数	SQL注入	2017-12-12 12:41:09
191309	站点名称：信息网络中心	61.178.98.70	甘肃省兰州市 电信	含有非法请求参数	SQL注入	2017-12-12 12:41:08
191308	站点名称：信息网络中心	61.178.98.70	甘肃省兰州市 电信	含有非法请求参数	SQL注入	2017-12-12 12:41:08

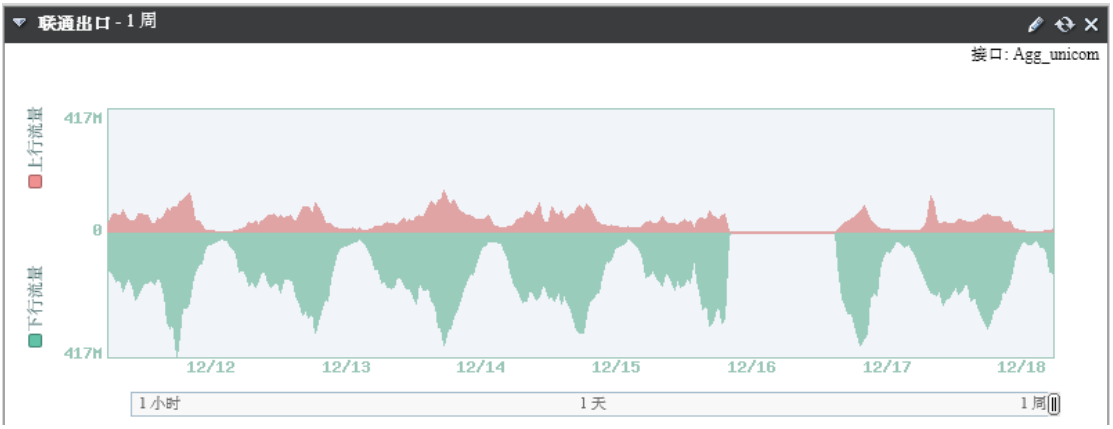
站群系统应用防火墙网站访问 IP 封禁记录

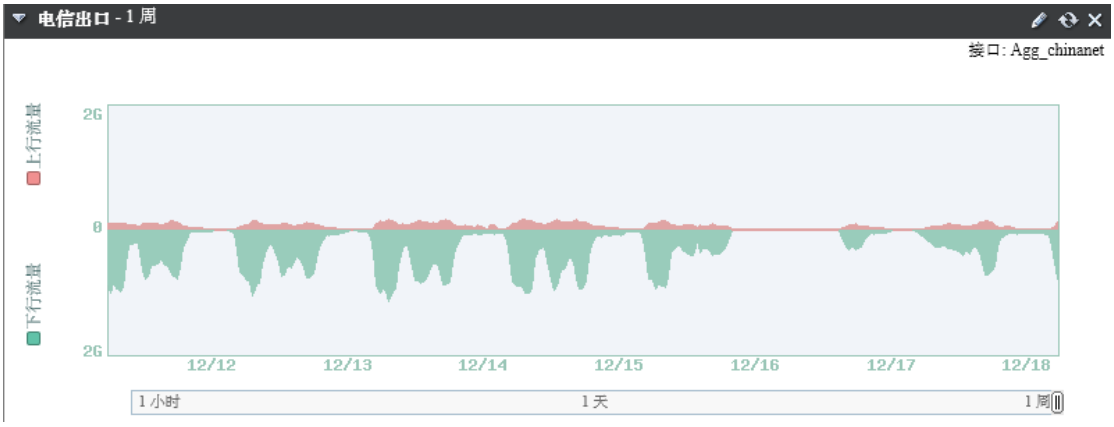
封禁IP	封禁IP归属地	封禁开始时间 ▼
198.204.225.114	美国	2017-12-18 07:04:48
118.180.5.174	甘肃省兰州市 网宿科技电信CDN节点	2017-12-15 01:10:56
117.25.54.215	福建省福州市 电信	2017-12-13 23:55:33
117.25.54.215	福建省福州市 电信	2017-12-13 09:20:11
42.92.180.12	甘肃省 电信	2017-12-12 21:12:09
61.178.98.70	甘肃省兰州市 电信	2017-12-12 17:11:47
61.178.98.70	甘肃省兰州市 电信	2017-12-12 12:41:09
61.178.98.70	甘肃省兰州市 电信	2017-12-12 12:41:09
61.178.98.70	甘肃省兰州市 电信	2017-12-12 12:41:09

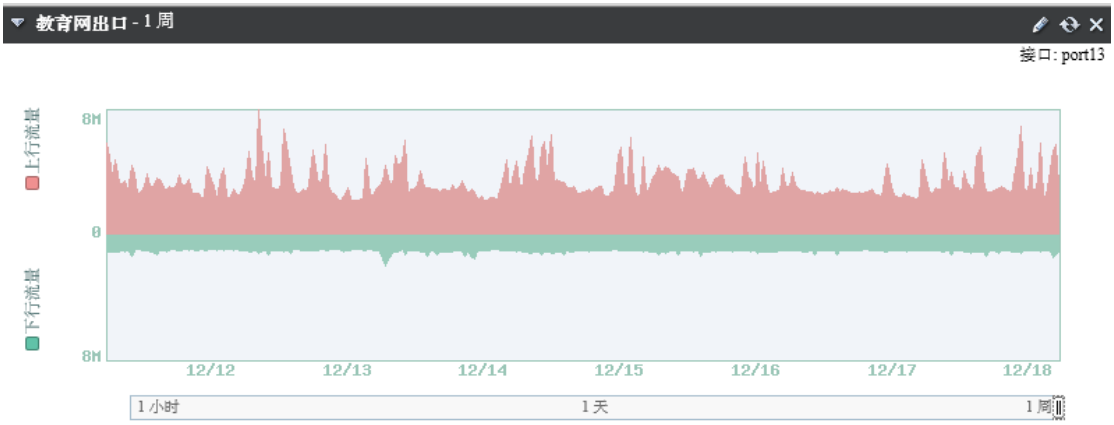
站群系统应用防火墙网站危险文件扫描记录

序号	路径	类型
1	E:\VSB9\manager\system_owners\lyxy_webprj\content.jsp	恶意js引用
2	E:\VSB9\manager\system_owners\lzcsxy_webprj\cheng_2.jsp	恶意js引用
3	E:\VSB9\manager\system_owners\lzcsxy_webprj\content.jsp	恶意js引用
4	E:\VSB9\manager\system_owners\lzcsxy_webprj\dh_jianjie.jsp	恶意js引用
5	E:\VSB9\manager\system_owners\lzcsxy_webprj\index.jsp	恶意js引用
6	E:\VSB9\manager\system_owners\lzcsxy_webprj\list.jsp	恶意js引用
7	E:\VSB9\manager\system_owners\lzcsxy_webprj\list_1.jsp	恶意js引用
8	E:\VSB9\manager\system_owners\lzcsxy_webprj\list_2.jsp	恶意js引用
9	E:\VSB9\manager\system_owners\lzcsxy_webprj\new_list_1.jsp	恶意js引用
10	E:\VSB9\manager\system_owners\lzcsxy_webprj\xiaobao.jsp	恶意js引用
11	E:\VSB9\manager\system_owners\lzcsxy_webprj\xinxiang.jsp	恶意js引用
12	E:\VSB9\manager\system_owners\lzcsxy_webprj\xr_lingdao.jsp	恶意js引用
13	E:\VSB9\manager\system_owners\sxy_webprj\index.jsp	恶意js引用
14	E:\VSB9\manager\system_owners\sygcxy_webprj\index.jsp	恶意js引用
15	E:\VSB9\manager\system_owners\zsw_webprj\index.jsp	恶意js引用

网络出口带宽情况统计





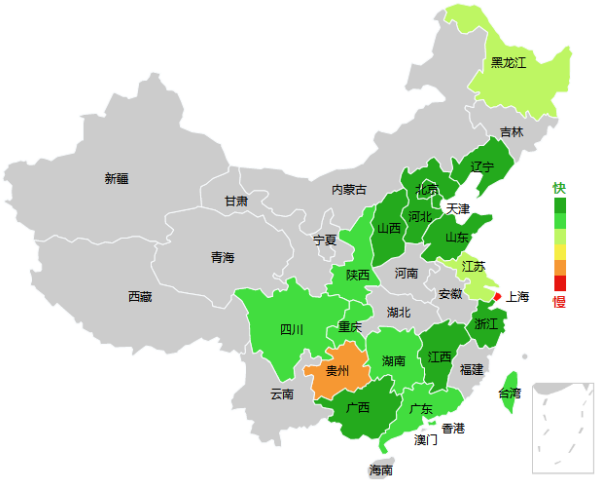


APT统计

防火墙统计

恶意	2401
检测到0-day恶意软件变种	0
可疑文件	0
安全文件	81447468

360 网站测速（http://www.lzcu.edu.cn）



平均速度排行		
名次	省份	平均速度(KB/s)
1	陕西	1,170.53
2	山西	504.94
3	天津	484.77

北京					
监测点	运营商	总耗时/ms	解析时间/ms	连接时间/ms	下载时间/ms
北京市	电信	232.59	26.67	31.56	174.36

360 网站评分（http://www.lzcu.edu.cn）

360 网站 DNS 检测（http://www.lzcu.edu.cn）

输入源IP	归属地
219.246.21.192	甘肃兰州教育网

解析结果IP	所用DNS	所属运营商
219.246.21.192	101.226.4.6(上海电信) 114.114.114.114(114DNS.COM114DNS.COM) 8.8.8.8(GOOGLE.COMGOOGLE.COMlevel3.com) 121.28.148.33(河北石家庄联通) 168.95.1.1(台湾cht.com.tw) 125.71.5.51(四川成都电信)	电信 其他 其他 联通 其他 电信

网站安全检测一（360 网站安全检测）

注：存在“服务器配置信息泄露”风险，“发现 robots.txt 文件”。

监控对象	类型	监测点	响应时间	访问成功率
OA办公主页【http://oa.lzcu.edu.cn】	源站监控	3 1	409.01 ms	75 %
OA办公主页【http://oa.lzcu.edu.cn】	源站监控	3 1	406.04 ms	75 %
WEB【http://www.lzcu.edu.cn】	源站监控	2 1	164.81 ms	66.67 %
WEB【http://www.lzcu.edu.cn】	源站监控	2 1	3257.46 ms	66.67 %

网站安全检测二（百度云观测）

http://www.lzcu.edu.cn　　更新时间：2017-12-17 20:23:47

指数评价

34.0

所属行业：教育培训

32.82% ↓

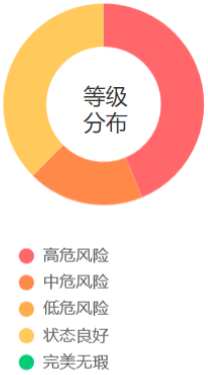
战胜了全国 **0.00%** 的网站

关联网站安全

关联网站数	最低指数评价
16	4.0 高危

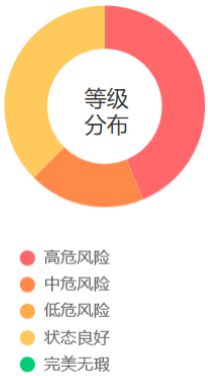
查看更多>>

该网站安全指数评价 高危 但是仍存在改进空间。建议 开启云观测服务>> ，查看评价详情，获取最新网站安全报警，及时修复以免被搜索引擎风险标识或降权。



域名	指数评价	操作
alumni.lzcu.edu.cn	80 良好	查看详情>>
bf.lzcu.edu.cn	4 高危	查看详情>>
cj.lzcu.edu.cn	49 中危	查看详情>>
ecard.lzcu.edu.cn	41.2 中危	查看详情>>
jpkc2.lzcu.edu.cn	90 良好	查看详情>>
jpkc.lzcu.edu.cn	14 高危	查看详情>>
jwc.lzcu.edu.cn	34 高危	查看详情>>
lzcu.edu.cn	80 良好	查看详情>>
nic.lzcu.edu.cn	90 良好	查看详情>>
oa.lzcu.edu.cn	84 良好	查看详情>>

当前 1 / 2 页　首页　上一页　下一页　尾页



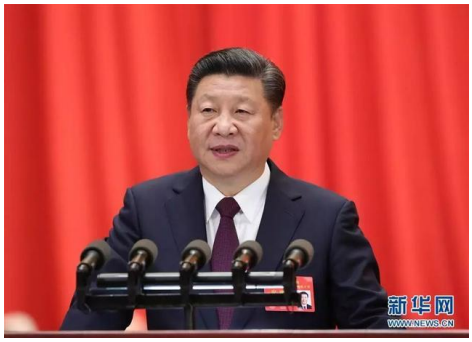
域名	指数评价	操作
old.lzcu.edu.cn	44 中危	查看详情>>
pop.lzcu.edu.cn	10 高危	查看详情>>
smtp.lzcu.edu.cn	10 高危	查看详情>>
syzz.lzcu.edu.cn	4 高危	查看详情>>
test.lzcu.edu.cn	84 良好	查看详情>>
www2.lzcu.edu.cn	4 高危	查看详情>>

当前 2 / 2 页　首页　上一页　下一页　尾页

【学习中国】习近平为“不忘初心、牢记使命”主题教育立规矩

学习中国 2017-12-13 00:00:00

不忘初心，方得始终。党的十九大提出，“以县处级以上领导干部为重点，在全党开展‘不忘初心、牢记使命’主题教育”。如何保证主题教育取得成功？习近平近日作出重要指示强调：“在即将开展的‘不忘初心、牢记使命’主题教育中，要力戒形式主义，以好的作风确保好的效果。”请随“学习中国”小编一起学习。



2017 年 10 月 18 日，中国共产党第十九次全国代表大会在北京人民大会堂开幕。习近平代表第十八届中央委员会向大会作报告。

一、力戒形式主义

形式主义是指片面注重表面形式而不顾实质内容的思想作风和工作方法。其特点是无实事求是之意，有哗众取宠之心，夸大事物的表面形式，不讲实际内容和实际效果。我们党内，形式主义在一定程度上仍然存在，在一些地方和单位问题还比较突出。习近平指出：“在形式主义方面，主要是知行不一、不求实效，文山会海、花拳绣腿，贪图虚名、弄虚作假。”

“不忘初心、牢记使命”主题教育作为党内教育的形式，极有可能出现形式主义现象。习近平曾经列举了形式主义的具体表现，其中提到：“有的不认真学习党的理论和做好工作所需要的知识，学了也是为应付场面，蜻蜓点水，浅尝辄止，不求甚解，无心也无力在实践中认真运用。有的习惯于以会议落实会议、以文件落实文件，热衷于造声势、出风头，把安排领导出场讲话、组织发新闻、上电视作为头等大事，最后工作却不了了之。”新的形势下，形式主义可能出现一些新表现。如，在贯彻落实方面，有的领导干部对贯彻落实中央重大决策部署表态调门高，但行动少落实差，虚多实少，仅仅满足于“轮流圈阅”“层层转发”“安排部署”，个别领导干部说一套做一套，我行我素。在会议方面，一些地方无论什么会议都要层层重复开，一个接一个，检查评比走马灯，导致干部疲于应付，没有时间抓落实。在改进文风方面，有的地方写文件、制文件机械照搬照抄，出台制度规定“依葫芦画瓢”，内容不是来自调查研究，而是源自抄袭拼凑。以上这些表现，要坚决反对。

力戒形式主义，是“不忘初心、牢记使命”主题教育的基本要求。主题教育能不能取得成功，反对形式主义的成效是检验的重要标准之一。反对形式主义，不是反对形式本身。内容很重要，形式也很重要，没有形式，也难有实效。“不忘初心、牢记使命”主题教育要有内容，也要有形式，重要的是做到内容与形式的统一。习近平指出：“当前，全党全国上下正在深入学习宣传贯彻党的十九大精神，开会发文是传达精神的必要方式，营造浓厚氛围也是必要的，但要防止出现以会议落实会议、以文件落实文件的现象，不能空喊口号、流于形式。”

2013 年 3 月 1 日，中央党校建校 80 周年庆祝大会暨 2013 年春季学期开学典礼在北京举行，中共中央总书记、中共中央军委主席习近平出席并发表重要讲话。

二、在做实上下功夫

实事求是，是我们党的思想路线。在“不忘初心、牢记使命”主题教育中，要坚持学用结合，知行合一，坚持问题导向，注重实效，以好的作风确保好的效果。

学风要实。好学才能上进，好学才有本领。开展“不忘初心、牢记使命”主题教育，就是要用党的光荣历史和革命传统涵养党性、用习近平新时代中国特色社会主义思想武装全党。学习贯彻党的十九大精神，学好领会习近平新时代中国特色社会主义思想，学好新党章，就是要在学懂、弄通、做实上下功夫，用党的创新理论武装头脑、指导实践、推动工作。要发扬理论联系实际的马克思主义学风，带着问题学，针对问题改，把解决问题贯穿主题教育全过程。习近平指出：“中央强调要转变工作作风，能不能多一点学习、多一点思考，少一点无谓的应酬、少一点形式主义的东西，这也是转变工作作风的重要内容。”

过程要实。中央将对主题教育的指导思想、目标任务、基本原则、方法步骤等作出明确规定，要严格按照党中央的精神和部署开展主题教育。“认认真真走过场”是最大的形式主义。开展“不忘初心、牢记使命”主题教育，要坚持实事求是、求真务实，力戒形式主义，防止走过场，做表面文章，要认认真真地把每一个“规定动作”做扎实、做到位。

效果要实。“空谈误国，实干兴邦。” 既然开展主题教育，当然要取得成效，而且成效越多越好。开展“不忘初心、牢记使命”主题教育，根本目的是增强工作本领、提高解决实际问题的水平。要真正把心思用在干事业上，把功夫下到察实情、出实招、办实事、求实效上。实效要体现在对中国共产党人的初心和使命的正确认识上；体现在从实际出发，找准靶子，有的放矢，解决实际问题上；体现在突出经常性教育，实现主题教育常态化、长效化上。

“不忘初心、牢记使命”主题教育是全党在思想、作风、党性上进行的又一次集中“补钙”和“加油”。主题教育能不能取得预期效果，反对形式主义是重要一环，要把反对形式主义贯穿于主题教育的全过程，一寸不能让，一刻不放松。

抄送：校领导