

中华人民共和国公安部

公信安〔2018〕843号

关于组织撰写第七届全国网络安全 等级保护技术大会论文的函

为贯彻落实中央领导关于网络安全工作的重要指示精神以及《深化简政放权放管结合优化服务改革方案》的有关要求，遵循国家网络安全工作责任制，进一步加强网络安全等级保护制度建设，提升网络安全保障水平，经研究决定，拟于2018年10月在长沙召开“第七届全国网络安全等级保护技术大会”，现将有关事项通知如下：

一、会议主题：网络安全等级保护制度建设与实践。研讨方向：等级保护制度建设与实践、等级保护标准与规范、等级保护与云计算、大数据、物联网、移动互联网、人工智能、区块链等新技术、新应用、新业务、新场景下的等级保护制度建设与实践。

二、会议时间：2018年10月23日—25日（23日报到，24日开会，25日离会）。

三、会议地点：湖南省长沙市（具体地点另行通知）。

四、会议规模：预计参会代表约500人。

五、会议内容：本次会议将围绕网络安全等级保护制度建设与实践，研讨方向：等级保护制度建设与实践、等级保护标准与规范、等级保护与云计算、大数据、物联网、移动互联网、人工智能、区块链等新技术、新应用、新业务、新场景下的等级保护制度建设与实践。

六、会议成果：会议将组织优秀论文评选，优秀论文将推荐至《中国信息安全》、《中国电子报》、《中国公安报》等媒体发表。

七、会议费用：会议不收取会务费，食宿统一安排，费用自理。

八、报名方式：请各参会单位于2018年9月20日前将参会回执发送至邮箱：wgl@ccia.org.cn。

九、联系方式：联系人：王工，电话：010-52997069，手机：13810100000。

息安全信息通报工作开展情况，根据征求意见要求（见附件），组织力量撰写论文，积极投稿。



附件：

第七届全国网络安全等级保护技术大会

征文要求

一、征文范围

(一) 网络安全等级保护整体解决方案。网络安全等级保护是国家对关键信息基础设施实行重点保护的制度，是国家网络安全工作的重要组成部分。随着《网络安全法》的实施，网络安全等级保护制度在落实过程中，如何结合行业特点，构建整体解决方案，成为亟待研究解决的问题。

(二) 网络安全等级保护与云计算、大数据、物联网等新兴技术的融合。

(三) 网络安全等级保护与移动互联网、物联网、工业控制、智慧城市等领域的融合。

(四) 网络安全等级保护与数据安全、个人信息保护、关键信息基础设施保护、网络安全应急响应、网络安全标准、网络安全产品、网络安全服务、网络安全人才等领域的融合。

(五) 网络安全等级保护与网络安全法、数据安全法、个人信息保护法、关键信息基础设施保护法等法律法规的融合。

(六) 网络安全等级保护与网络安全监管、网络安全执法、网络安全事件处置、网络安全应急响应、网络安全标准、网络安全产品、网络安全服务、网络安全人才等领域的融合。

(七) 网络安全等级保护与网络安全法、数据安全法、个人信息保护法、关键信息基础设施保护法等法律法规的融合。

(八) 网络安全等级保护与网络安全监管、网络安全执法、网络安全事件处置、网络安全应急响应、网络安全标准、网络安全产品、网络安全服务、网络安全人才等领域的融合。

(九) 网络安全等级保护与网络安全法、数据安全法、个人信息保护法、关键信息基础设施保护法等法律法规的融合。

(十) 网络安全等级保护与网络安全监管、网络安全执法、网络安全事件处置、网络安全应急响应、网络安全标准、网络安全产品、网络安全服务、网络安全人才等领域的融合。

(十一) 网络安全等级保护与网络安全法、数据安全法、个人信息保护法、关键信息基础设施保护法等法律法规的融合。

(十二) 网络安全等级保护与网络安全监管、网络安全执法、网络安全事件处置、网络安全应急响应、网络安全标准、网络安全产品、网络安全服务、网络安全人才等领域的融合。

(十三) 网络安全等级保护与网络安全法、数据安全法、个人信息保护法、关键信息基础设施保护法等法律法规的融合。

(十四) 网络安全等级保护与网络安全监管、网络安全执法、网络安全事件处置、网络安全应急响应、网络安全标准、网络安全产品、网络安全服务、网络安全人才等领域的融合。

(十五) 网络安全等级保护与网络安全法、数据安全法、个人信息保护法、关键信息基础设施保护法等法律法规的融合。

击分析与防范、软件安全技术等。如何利用虚拟机、沙箱技术、黑白名单技术和产品联动技术加强对重要信息系统的保护。

(四) 网络安全等级保护检测评估技术：标准符合性检测技术、安全基线评估技术、差距分析技术、渗透测试技术、物理向工程评估技术、网络安全漏洞评估等。

(五) 网络安全等级保护的安全监管技术：用于支撑安全监测的数据采集、挖掘与分析技术，用于支撑安全监管的敏感数据保护技术、安全态势评估技术、安全事件关联分析技术、安全态势感知技术、安全事件响应技术、支撑进行设备管理分析、攻击检测与预警、策略配置与告警生成、可视化决策。

（六）网络安全等级保护支撑技术：身份识别、密钥管理、日志、审计、取证分析、恶意代码检测、防火墙、入侵检测、入侵防御、漏洞扫描、安全加固、安全审计、安全评估、安全培训、入网检测技术等。

（七）网络安全等级保护法律制度：网络安全法及其配套法规、行政法规、部门规章、规范性文件、司法解释、地方性法规、地方政府规章、国家标准、行业标准、地方标准、团体标准、企业标准、网络安全等级保护制度、网络安全等级保护工作。

（八）网络安全等级保护：方案设计、评审、建设、运行维护、评估、定级、整改、监督、检查、考核、奖励、惩罚、宣传、教育、培训、激励、考核、评价、总结、经验交流、表彰、奖励、处罚、通报、批评、诫勉、降职、撤职、免职、辞退、开除、移送司法机关处理等。

(九) 国外网络安全基础研究：国外网络安全战略、策

略、管理、法律、技术、标准、评估、检测、应急响应、人才培养等。

（十）其他

（十一）其他

（十二）其他

（十三）其他

（十四）其他

（十五）其他

（十六）其他

（十七）其他

（十八）其他

（十九）其他

（二十）其他

（二十一）其他

（二十二）其他

（二十三）其他

（二十四）其他

（二十五）其他

（二十六）其他

（二十七）其他

（二十八）其他

（二十九）其他

（三十）其他

（三十一）其他

（三十二）其他

（三十三）其他

（三十四）其他

（三十五）其他

（三十六）其他

（三十七）其他

（三十八）其他

（三十九）其他

（四十）其他

（四十一）其他

（四十二）其他

（四十三）其他

（四十四）其他

（四十五）其他

（四十六）其他

（四十七）其他

（四十八）其他

（四十九）其他

（五十）其他

（五十一）其他

（五十二）其他

（五十三）其他

（五十四）其他

（五十五）其他

（五十六）其他

（五十七）其他

（五十八）其他

（五十九）其他

（六十）其他

（六十一）其他

（六十二）其他

（六十三）其他

（六十四）其他

（六十五）其他

（六十六）其他

（六十七）其他

（六十八）其他

（六十九）其他

（七十）其他

（七十一）其他

（七十二）其他

（七十三）其他

（七十四）其他

（七十五）其他

（七十六）其他

（七十七）其他

（七十八）其他

（七十九）其他

（八十）其他

（八十一）其他

（八十二）其他

（八十三）其他

（八十四）其他

（八十五）其他

（八十六）其他

（八十七）其他

（八十八）其他

（八十九）其他

（九十）其他

（十一）其他

（十二）其他

（十三）其他

（十四）其他

（十五）其他

（十六）其他

（十七）其他

（十八）其他

（十九）其他

（二十）其他

（二十一）其他

（二十二）其他

（二十三）其他

（二十四）其他

（二十五）其他

（二十六）其他

（二十七）其他

（二十八）其他

（二十九）其他

（三十）其他

（三十一）其他

（三十二）其他

（三十三）其他

（三十四）其他

（三十五）其他

（三十六）其他

（三十七）其他

（三十八）其他

（三十九）其他

（四十）其他
（四十一）其他
（四十二）其他
（四十三）其他
（四十四）其他
（四十五）其他
（四十六）其他
（四十七）其他
（四十八）其他
（四十九）其他
（五十）其他
（五十一）其他
（五十二）其他
（五十三）其他
（五十四）其他
（五十五）其他
（五十六）其他
（五十七）其他
（五十八）其他
（五十九）其他
（六十）其他
（六十一）其他
（六十二）其他
（六十三）其他
（六十四）其他
（六十五）其他
（六十六）其他
（六十七）其他
（六十八）其他
（六十九）其他
（七十）其他
（七十一）其他
（七十二）其他
（七十三）其他
（七十四）其他
（七十五）其他
（七十六）其他
（七十七）其他
（七十八）其他
（七十九）其他
（八十）其他
（九十一）其他
（九十二）其他
（九十三）其他
（九十四）其他
（九十五）其他
（九十六）其他
（九十七）其他
（九十八）其他
（九十九）其他
（一百）其他

（五）论文提交截止日期：2018年7月30日。

三、联系方式

通讯地址：北京市海淀区北四环中路211号华北计算技术研究所

邮编：100083

联系人：张洁、陈愚

联系电话：010-89055525 18612673323

010-89055529 13810717212