中华人民共和国公安部

公信安〔2016〕679号

关于组织撰写第五届全国信息安全等级保护技术大会论文的通知

为进一步贯彻落实国家信息安全等级保护制度，深入推进信息安全等级保护技术实施和工作开展，由我局指导，公安部第三研究所承办的第五届全国信息安全等级保护技术大会（ICSP'2016）将于2016年8月召开。会议拟邀请信息安全领域的院士、资深专家，公安网安等保部门以及重点行业网络安全部门专家领导，围绕网络安全保护策略、机制、新技术新应用、信息安全产品、国外网络安全政策标准和等级保护技术体系等各类热点问题开展交流，为信息安全职能部门、专家学者、行业用户和信息安全企业提供一个开放的技术交流平台，分享等级保护的技术、方法和实践最新研究成果。届时，作为会议的一项重要成果，将出版大会论文集，其中，经专家评选的部分优秀论文，将推荐至国家核心期刊发表。

为做好此次技术大会的论文征集工作，请各单位高度重视，精心组织，结合本行业、本部门信息安全等级保护工作

和信息安全通报工作开展情况，根据征文要求（见附件），认真研究、积极撰写论文并按时投稿。

附件：第五届全国信息安全等级保护技术大会征文要求

公安部第十一局

2016年3月11日

附件：

第五届全国信息安全等级保护技术大会

征文要求

一、征文范围

（一）安全保护策略：由于云计算和大数据技术结合，使得信息网络[redacted]

（四）新技术应用的等级保护管理和技术：下一代互联网（IPv6）、云计算、物联网、移动互联网、大数据、工业控制系统的信息安全等级保护建设和管理内容。如何确定定级对象、如何确定安全保护级别、如何开展安全建设、如何开展等级测评、如何构建安全保护[redacted]

防护的工作思路及技术防护策略。新技术新应用的等级保护基本要求、安全设计技术要求、等级测评要求等安全标准研究。

（五）信息安全等级保护安全建设技术：信任体系模型与构建技术、可信计算技术、密码技术、灾难恢复与备份技术、主动防御技术、漏洞检测技术、网络攻击分析与防范、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。

（六）信息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、安全绩效评估技术等。如何利用大数据技术、审计措施进行设备关联分析、日志存储与分析，解决网络攻击的可发现、可追溯问题。

（七）信息安全等级保护测评技术：标准符合性检验技术、安全基准检查技术、无损检测技术、渗透测试技术、逆向工程剖析技术、源代码安全分析技术等。

（八）应急与事件处置技术：态势感知技术、安全监测技术、通报预警技术、安全事件检测（识别）响应技术、应急处置技术、灾难备份技术

（十）**信息安全产品研究：** 产品检测策略、技术，国内外信息安全产品性能比较，产品的安全性检测技术，国外新技术、新产品研究等。

（十一）**国外网络安全基础研究：** 国外网络安全发展战略、策略、管理等研究，国外网络安全新技术研究，国外信息安全新标准研究。

二、投稿要求

（一）来稿内容应属于作者的科研成果，数据真实、可靠，未公开发表过，引用他人成果已注明出处，署名无争议，论文摘要及全文不涉及保密内容。

（二）会议只接受以 Word 排版的电子稿件，稿件一般不超过 10 页（5000 字）。

（三）稿件以 Email 的方式发送到会议征稿邮箱 pxb@cspec.org.cn。

（四）凡投稿文章被录用且未作特殊声明者，视为已同