

附件:

## 第二届全国信息安全等级保护技术大会

### 征文需求

#### 一、征文范围

(一) 信息安全学理论、信息安全与业务的安全融合与业务融合应用、安全管理运营体系建设、业界案例实践、大型系统安全保障案例等。

(二) 信息安全保障体系、等级保护实施案例、信息安全保障体系中的风险评估、风险评估与整改、风险评估与应急响应、安全监测预警机制等。

(三) 信息安全保障体系中的等级保护实施案例、下一代互联网(IIPv6)、云计算、大数据、物联网、工业互联网、区块链、人工智能

等应用。

(四) 信息安全保障体系中的等级保护实施案例、下一代互联网(IIPv6)、云计算、大数据、物联网、工业互联网、区块链、人工智能等应用。信息安全保障体系中的等级保护实施案例、下一代互联网(IIPv6)、云计算、大数据、物联网、工业互联网、区块链、人工智能等应用。信息安全保障体系中的等级保护实施案例、下一代互联网(IIPv6)、云计算、大数据、物联网、工业互联网、区块链、人工智能等应用。信息安全保障体系中的等级保护实施案例、下一代互联网(IIPv6)、云计算、大数据、物联网、工业互联网、区块链、人工智能等应用。信息安全保障体系中的等级保护实施案例、下一代互联网(IIPv6)、云计算、大数据、物联网、工业互联网、区块链、人工智能等应用。

(六) 等级保护测评技术：标准符合性检验技术、安全基准验证技术、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。

(七) 应急与事件处置技术：态势感知预警技术、安全监测技术、安全事件检测（识别）响应技术、应急处置技术、应急处置策略技术、风险评估技术、入侵检测技术等。

(八) 工控系统安全防护技术：工控系统的安全威胁分析，等级保护支撑性技术和具体实践等。

(九) 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，国外新产品研究等。

(十) 国内外网络安全态势：网络安全态势感知、态势感知与应急响应网络安全的影响，国外网络安全新技术研究、国外网络安全安全标准研究。

## 二、投稿要求

(一) 本期刊物应属于作者的科研成果，数据真实、可靠，未在公开渠道，其他他人或媒体上刊出过，未在公开过，未在公开渠道发表过。

(二) 稿件须按模板 Word 格式上传电子稿件，稿件一律不标注页码（900 字）。

(三) 稿件以 Email 的方式发送至组委会征稿邮箱 [qjhlh@compas.gov.cn](mailto:qjhlh@compas.gov.cn)。

(四) 凡投稿文章被录用且作者特殊声明者，视为已同

意授权出版。

(五) 论文提交截止日期： 2013 年 5 月 15 日

### 三、联系方式

通讯地址：北京市海淀区阜成路 58 号新洲商务大厦 708