传 真 电 报

单位：福建省信息通信行业协会　　核稿：
盖章：　　日期：8.5　　拟稿：张兴丽

等级：传真流水号：闽信通行协转传[2022]21号　　总页数：21页

发往单位：各会员单位
抄送：

转发《关于举办“2022年第三届电信和互联网行业职业技能竞赛暨第十一届信息通信网络安全管理员职业技能竞赛”的通知》

各会员单位：

为深入贯彻习近平总书记对技能人才工作的系列重要指示和致首届全国职业技能大赛贺信精神，认真落实《网络安全法》《数据安全法》相关要求，在全社会更好地弘扬劳模精神、劳动精神、工匠精神，加快培养和选拔电信和互联网行业网络安全高技能人才，保障网络安全工作持续有效开展，进一步提升我国通信网络安全的防护水平和应急能力，中国通信企业协会、中国国防邮电工会全国委员会和中国信息通信研究院决定联合举办“2022年第三届电信和互联网行业职业技能竞赛暨第十一届信息通信网络安全管理员职业技能竞赛”。具体赛事内容请参阅附件。请各会员单位积极报名参加。

联系人：王牧风
电　话：010-68094555，13381270717
邮　箱：cacenssc@163.com
附　件：通企【2022】124号 关于举办“2022年第三届电信和互联网行业职业技能竞赛暨第十一届信息通信网络安全管理员职业技能竞赛”的通知

发出时间：2022年8月5日　时　分	福建省信息通信行业协会传真室

中国通信企业协会
中国国防邮电工会全国委员会 文件
中国信息通信研究院

通企〔2022〕124 号

关于举办“2022 年第三届电信和互联网行业职业技能竞赛暨第十一届信息通信网络安全管理员职业技能竞赛”的通知

各省、自治区、直辖市通信管理局，（信息）通信行业协会，基础电信运营企业，互联网企业，网络安全企业，相关高等院校、职业院校（含技工院校）及会员等有关单位：

为深入贯彻习近平总书记对技能人才工作的系列重要指示和致首届全国职业技能大赛贺信精神，认真落实《网络安全法》《数据安全法》相关要求，在全社会更好地弘扬劳模精神、劳动精神、工匠精神，加快培养和选拔电信和互联网行业网络安全高技能人才，保障网络安全工作持续有效开展，进一步提升我国通信网络安全的防护水平和应急能力，中国通信企业协

会、中国国防邮电工会全国委员会和中国信息通信研究院决定联合举办“2022年第三届电信和互联网行业职业技能竞赛暨第十一届信息通信网络安全管理员职业技能竞赛”（以下简称“竞赛”），由中国通信企业协会通信网络安全专业委员会承办。现将有关事项通知如下：

一、组织领导

为保证此次竞赛活动组织有序，大赛方式公平公正，竞赛专门成立全国组委会和执行委员会（名单详见附件1）。

全国组委会是竞赛的最高领导决策机构，负责统筹协调竞赛各项工作推进实施与组织管理工作，由竞赛主办单位与基础电信运营企业等单位的相关领导、专家组成。

执行委员会在全国组委会领导下开展工作，负责具体的赛事组织与管理。执行委员会下设办公室、监审委员会、技术工作委员会，负责审定竞赛方案、决策竞赛期间重大事项协调、指导和监督竞赛全过程、发布竞赛结果等相关事宜。

二、参赛对象

（一）职工组：从事网络与数据安全管理等相关专业或职业的企业职工，各类高等院校和职业院校（含技工院校、高职高专、中职等，下同）教师。

（二）学生组：各类高等院校和职业院校在校学生。

在往届竞赛（含往届电信和互联网行业网络安全管理职业

技能竞赛）中获得前5名且为职工身份的人员不得参赛；具有全日制学籍的在校创业学生不得以职工身份参赛。

三、竞赛内容

（一）竞赛内容：聚焦5G安全、数据安全等领域技术发展趋势，结合近期常见的网络安全重点热点问题，构建电信运营企业典型业务场景等竞赛环境。通过安全风险点定位和排查、安全事件取证和追溯、安全攻击处置和反制等竞赛形式，考查参赛选手多方面安全技能，达到行业网络安全人才技术交流和练兵的目标。

（二）竞赛命题标准：以理论知识和技能操作相结合，总成绩中理论考试成绩占20%、实际操作成绩占80%。

竞赛将积极吸收与借鉴国内外职业技能大赛命题方法和考核内容，适当增加相关新知识、新技术、新技能内容，同时结合企业职业岗位对人才培养需求，并参照相关国家职业标准制定。（见附件4《竞赛大纲》）

四、竞赛实施

竞赛按照“广泛发动、积极参与、自下而上、层层比赛、以赛促学、注重实效”的原则，分为选拔赛和全国总决赛。

（一）选拔赛阶段：2022年10月30日前完成

1.省级选拔赛：以各省、直辖市、自治区为单位组织选拔赛，每个省可推荐3名优秀选手和1支参赛队伍进入全国总决

赛。

2. 基础电信运营企业集团选拔赛：由基础电信运营企业（主要为：中国电信、中国移动、中国联通、中国铁塔）集团公司自行选拔，中国电信、中国移动、中国联通集团可推荐 45 名优秀选手和 15 支参赛队伍进入全国总决赛，中国铁塔集团可推荐 24 名优秀选手和 8 支参赛队伍进入全国总决赛）。

3. 全国组委会选拔赛：面向省级选拔赛未覆盖的地区和单位的网络安全从业人员和在校学生，由全国组委会统一组织开展选拔赛，并根据报名人数另行确定推荐进入全国总决赛名额；全国组委会选拔赛时间等具体事宜另行通知。

（二）全国总决赛阶段：2022 年 12 月 31 日前完成

由全国组委会统一组织全国总决赛；比赛形式包含安全卫士个人赛和安全卫士团队赛，并根据参赛选手单位不同类型分为基础电信运营企业赛场、综合赛场（统称为职工组）和学生赛场（学生组）。其中：

安全卫士个人赛：分别由职工组两个赛场与学生组一个赛场独立进行，成绩分别排名。

安全卫士团队赛：分别由职工组两个赛场与学生组一个赛场独立进行，成绩分别排名；包含“经典网络安全场景攻防”、“热点网络安全场景挑战”、“数据资产保护和安全事件分析”三大赛项。

全国总决赛时间、地点等具体事宜另行通知。

（三）闭幕仪式

全国总决赛结束后举办竞赛闭幕仪式，邀请指导和组织竞赛的单位及相关单位领导出席参加，为获奖选手颁奖。

五、竞赛报名

（一）由各省、集团公司自行组织安排的选拔赛，报名以各省主办单位、基础电信运营企业集团公司通知为准；

（二）请组织选拔赛的省份、集团公司向全国组委会推荐竞赛工作联络负责人，并于2022年8月30日之前将加盖公章的电子扫描PDF版和word版《联络人推荐表》（见附件2）发送至全国组委会竞赛邮箱：cacenssc@163.com；

（三）请参加全国组委会选拔赛的单位和院校于2022年8月30日之前将加盖公章的电子扫描PDF版和word版《全国组委会选拔赛报名意向确认表》（见附件3）发送至全国组委会竞赛邮箱：cacenssc@163.com。

六、竞赛奖励

（一）全国总决赛中安全卫士个人赛的三个赛场分别设有特等和一、二、三等奖，奖项名额为特等奖1名，一、二、三等奖获奖比例分别为10%、15%和25%，获奖人员由主办单位颁发奖杯和荣誉证书。

（二）全国总决赛中安全卫士团队赛的三个赛场分别设有

特等和一、二、三等奖，奖项名额为特等奖1名，一、二、三等奖获奖比例分别为10%、15%和25%，获奖人员由主办单位颁发奖杯和荣誉证书。

（三）其他奖励：

1.对贡献突出的承办、协办单位和技术支持单位，由竞赛组委会颁发“突出贡献奖”奖杯和荣誉证书。

2.对省级选拔赛组织工作表现突出的单位，由竞赛组委会颁发“优秀组织奖”奖杯和荣誉证书。

3.对在全国总决赛组织工作中表现突出的个人，由竞赛组委会颁发“优秀工作者”奖杯和荣誉证书。

各企业（集团）、院校及省级选拔赛主办单位可制定本单位或本赛项奖励办法，具体以各赛区或赛项通知为准。

七、有关要求

（一）落实责任，做好防控

竞赛前，建立以预防为主、防控结合、科学应对的新冠肺炎疫情防控方案及应急处置机制，明确疫情防控领导小组成员，强化组织领导，落实竞赛承办单位“一把手”负责制，细分任务、明确责任人，确保竞赛活动期间防控工作落到实处。在竞赛活动期间，提高快速反应和应急处理能力，落实各项疫情防控措施，确保竞赛活动顺利举行；保护参赛选手、领队、教练员、裁判员和工作人员的身体健康与生命安全，认真落实消防、

人身、公共卫生等安全责任。

（二）提高认识，精心组织

各参赛单位要高度重视，加强协作，精心组织，务求实效；利用各种宣传手段突出宣传“重视技能，尊重技能人才”理念。把竞赛当成岗位练兵的重要举措，促进全体技术人员提高学习热情和技能，同时也作为发现人才、选拔人才的重要参考。请各地人社、教育、科技、工会、信息通信行业（协会）和相关部门，在组委会的统一部署下，认真做好大赛各项组织工作，并紧密结合当地企业生产和院校教学工作实际，加强协调和指导工作。

（三）公平公正，注重实效

各参赛单位及选拔赛组委会要加强技术评判工作，使竞赛做到科学、严谨、公平、公正。竞赛工作要聚焦高技能人才培养，突出岗位练兵，突出实战实用，争取实现网络安全人才能力水平的有效提高，使职业技能竞赛在培养、选拔和激励高技能人才等方面发挥最大功效。对竞赛中可能出现的问题，要及时与竞赛执行委员会办公室联系。

附件：1.“2022年（第十一届）信息通信网络安全管理员职业技能竞赛”全国组委会名单

2.联络人推荐表

3.全国组委会选拔赛报名意向确认表

4.竞赛大纲

中国通信企业协会　　中国国防邮电工会全国委员会　　中国信息通信研究院

2022年7月27日

（联系方式：

全国竞赛执行委员会办公室

联系人：王牧风

电　话：010-68094555，13381270717

邮　箱：cacenssc@163.com）

附件 1

2022 年第三届电信和互联网行业职业技能竞赛暨第十一届信息通信网络安全管理员职业技能竞赛全国组委会名单

一、全国组委会

（一）主任

苗建华　　中国通信企业协会会长

（二）副主任

黄敬平　　中国国防邮电工会全国委员会一级巡视员

赵中新　　中国通信企业协会副会长兼秘书长

魏　亮　　中国信息通信研究院副院长

刘桂清　　中国电信集团有限公司副总经理

李慧镝　　中国移动通信集团有限公司副总经理

梁宝俊　　中国联合网络通信集团有限公司副总经理

高春雷　　中国铁塔股份有限公司党委副书记、工会主席

（三）委员

赵俊渥　　中国通信企业协会副秘书长

姜玉波　　中国国防邮电工会全国委员会电信工作部部长

谢　玮　　中国信息通信研究院安全研究所所长

宋桂香　　中国电信集团有限公司集团工会副主席

张　侃　　中国电信集团有限公司网络和信息安全管理部

副总经理

李　丽　中国移动通信集团有限公司集团工会副主席

袁　捷　中国移动通信集团有限公司信息安全管理与运行中心副总经理

赵全燕　中国联合网络通信集团有限公司集团工会副主席

谢　攀　中国联合网络通信集团有限公司信息安全部副总经理

叶　臻　中国铁塔股份有限公司信息技术研究院院长、业务支撑部总经理

范晓青　中国铁塔股份有限公司工会副主席、党群工作部主任

二、执行委员会办公室

主要负责竞赛整体的协调和组织筹备工作。

（一）主任

孟　楠　中国通信企业协会通信网络安全专委会秘书长/中国信息通信研究院安全研究所副所长

（二）副主任

王牧风　中国通信企业协会通信网络安全专委会人才建设发展部主任

（三）成员

刘亚天　中国电信集团有限公司网络和信息安全管理部

网络与数据安全管理处处长

张　峰　中国移动通信集团有限公司信安中心研究支撑中心经理

郑　涛　中国联合网络通信集团有限公司网络部网络安全室总监

王江峰　中国铁塔股份有限公司信息技术研究院总监

三、监审委员会

主要负责保障竞赛整体流程安排的公平公正。

（一）主任

冯志宏　中国通信企业协会综合业务发展部副主任

（二）委员

董爱刚　中国电信集团有限公司集团工会经济技术部主任

刘忠信　中国移动通信集团有限公司工会经济工作部主任

葛　然　中国联合网络通信集团有限公司网络部网络安全室业务主管

程　赓　中国铁塔股份有限公司业务支撑部总监

四、技术工作委员会

主要负责制定竞赛题目和规则，筹建选拔赛和全国总决赛竞赛环境，提供竞赛期间相关技术安排和保障等工作。

（一）主任

崔　涛　　中国信息通信研究院安全研究所网安部副主任

（二）委员

吴威震　　中国信息通信研究院安全研究所网安部工程师

张　鹏　　中国信息通信研究院安全研究所网安部工程师

董　悦　　中国信息通信研究院安全研究所网安部工程师

刘　凯　　中国信息通信研究院安全研究所网络安全检测评估中心工程师

代长生　　中国信息通信研究院安全研究所网络安全检测评估中心工程师

附件 2

联络人推荐表

单位名称			
姓名		部门及职务	
联系电话		联系邮箱	
2022 年本省网络安全竞赛组织计划、方案等情况简介	（本省今年竞赛的组织领导机构、规格或级别、开展过程、参赛人员情况和特色亮点等情况介绍，可另作附件）		
推荐单位意见 （盖章）			

附件 3

全国组委会选拔赛报名意向确认表

单位名称			
联络人姓名		部门及职务	
联系电话		联系邮箱	
参赛组别	□职工组　　□学生组		
推荐单位意见 （盖章）			

附件 4

竞赛大纲

一、管理部分

（一）法律

1．了解《网络安全法》主要内容，包括：网络运行安全、关键信息基础设施安全、网络信息安全、监测预警与应急处置等要求。

2．了解《数据安全法》主要内容，包括：数据安全与发展、数据安全制度、数据安全保护义务、政务数据安全与开放、法律责任等要求。

3．了解《个人信息保护法》主要内容，包括：个人信息处理规则、个人信息跨境提供的规则、个人在个人信息处理活动中的权利、个人信息处理者的义务等要求。

（二）法规

1．了解《通信网络安全防护管理办法》（工信部令第 11 号）主要内容，包括：通信网络安全防护范围、管理主体、责任主体、同步要求、分级备案要求、符合性评测要求、风险评估要求、应急演练要求等内容。

2．了解《关键信息基础设施安全保护条例》（国令第 745 号）主要内容，包括：关键信息基础设施认定、运营者责任义务、保障和促进、法律责任等内容。

3．了解《电信和互联网用户个人信息保护规定》（工信

部令第 24 号）主要内容，包括：用户个人信息的收集和使用规范要求、安全保障措施、责任和义务等内容。

4．了解《网络产品安全漏洞管理规定》（工信部联网安〔2021〕66 号）主要内容，包括：管理对象、管理职责、主体责任、漏洞发布要求、漏洞收集平台相关要求等内容。

（三）政策文件

1．了解通信网络安全防护工作总体思路、基本原则、主要任务、实施及监督检查要求、安全服务机构管理等政策文件。

2．熟悉通信网络安全防护定级范围、评审要求、备案等政策要求，熟悉通信网络单元安全防护定级方法、定级对象命名规则、定级报告内容、定级备案相关信息等。

3．了解通信行业网络和数据安全管理体系相关工作。

（四）通信网络安全防护标准

1．熟悉各专业网络单元安全防护标准中技术要求内容。

2．了解安全风险评估要素及关系、工作形式、不同生命周期要求和实施要点等要求。

3．了解灾难备份原则、灾难备份资源要素、实施过程、灾难恢复预案等要求。

4．了解安全管理制度、安全管理机构、人员安全管理、安全建设管理、安全运维管理等内容。

5．了解安全风险评估工作的国际标准名称（ISO/IEC TR 13335、ISO/IEC 17799、ISO/IEC 27001 等），了解《信息系

统安全等级保护定级指南》、《信息系统安全等级保护实施指南》等国家标准总体情况。

二、技术部分

（一）操作系统安全检测与防护

了解操作系统（Windows、Linux、Unix 等）的常规安全防护机制。熟悉系统日志、应用程序日志等溯源攻击途径。掌握系统账号、权限、文件系统、文件共享、网络参数、端口和服务、日志审计、漏洞补丁等项目的安全检测与安全加固方法；掌握系统加密、系统防火墙、安全策略、杀毒软件的安装和配置方法。

（二）数据库安全检测与防护

了解数据库（Mssql、Mysql、Oracle、MongoDB、Redis 等）的库表管理、数据访问、权限控制等基础安全防护机制。熟悉数据存储加密不当、数据库访问与权限管理配置不当、SQL 注入攻击、数据库漏洞攻击等常见安全问题。掌握数据库运维管控、数据存储加密、数据脱敏、风险发现、日志审计等安全防护方法。

（三）网络层攻击与防护

了解网络层的网络架构、传输方式、传输协议和控制措施；了解针对有线和无线的攻击方式和安全防护机制。熟悉常见的网络层攻击，包括：DoS 和 DDoS、窃听、假冒/伪装、重放攻击、篡改、针对 DNS 的工具（欺骗、投毒和劫持）、ARP 攻击、

DHCP 攻击以及无线攻击等。掌握通过使用网络层安全工具和设备（如：NMAP、防火墙、Web 防火墙、IDS/IPS、抗拒绝服务攻击系统、网络扫描器、SOC、SIEM、EDR 等）发现和阻断网络层攻击的方法和技术；掌握对网络层设备（如：路由器、交换机等）的安全配置和加固技术；掌握验证各种安全防护手段（如密码强度、访问控制）有效性和强度的方法。

（四）数据安全与保护

了解电信和互联网行业数据分级分类方法；了解同态加密、安全多方计算、联邦学习、差分隐私等隐私计算技术；熟悉容灾备份、持续数据保护等技术和应用方法；熟悉数据安全的全流程管控、追溯技术，以及动态行为分析和数据安全加密保护技术。

（五）Web 应用安全

了解 Web 应用安全架构，风险分析及常规防护思路。熟悉框架和组件漏洞、权限绕过、弱口令、注入、跨站、文件包含、非法上传、非法命令执行、任意文件读取和下载等常见安全问题。掌握常见 Web 环境的安全配置方法和检测方法和安全防护手段。

（六）渗透测试技术

熟悉渗透基本思路、方法和流程，熟悉各种常见渗透测试工具。掌握常规的渗透测试技术，包括：信息收集、漏洞发掘、常规漏洞利用、常见应用入侵、服务器提权、远程溢出攻击、

内网渗透、身份隐藏、暗网挖掘等。

（七）应急响应与恢复

熟悉应急响应与恢复的基本方法和流程。掌握应急响应和恢复的调查、取证、恢复等相关技术，包括：入侵取证分析、日志审计分析、反取证技术、文件删除恢复、中毒文件恢复等。

（八）软件开发安全

了解软件安全开发生命周期、软件安全架构和设计、软件威胁建模原理和方法；了解常见编程环境（C/C++、JAVA、PHP、JSP 等）的构建以及语言的编写。熟悉常见的软件安全漏洞的产生原理和加固方法；熟悉软件安全开发过程中有关参数化查询、输入验证、输出编码、访问控制、身份验证、安全日志、API 接口安全、使用安全的第三方组件等安全开发规范；熟悉代码审计（包括人工审计和工具审计）和代码加固技术。

（九）恶意代码与逆向

熟悉恶意代码的分类、特点和运行机制，熟悉常见的恶意代码，包括：后门、僵尸网络、启动器、感染病毒、勒索病毒、远程控制木马、Rootkit 等。熟悉发现、隔离、清除常见恶意代码的相关工具及技术手段。熟悉常见的恶意代码保护措施以及清除手段。熟悉对常见恶意代码进行静态与动态的分析、源定位以及修复的方法。

（十）移动应用安全

了解智能终端操作系统（安卓系统、苹果 IOS）的安全机

制；了解移动应用软件的安全机制和调试分析、代码审计技术。熟悉移动互联网联网应用和应用商店的架构组成与技术实现；熟悉移动应用软件的越权访问、信息泄露、上传漏洞、业务逻辑错误等安全问题的检测与处理技术；熟悉针对移动应用程序的安全防护技术。掌握移动互联网恶意程序的监测与处置方法。

（十一）新技术应用安全

1．了解云计算的概念及特征。熟悉云计算常见的安全问题，包括：虚拟机安全、容器安全、应用程序安全、数据安全、网络隔离、微隔离、接口安全等。

2．了解大数据的概念及特征。熟悉利用大数据分析技术提升网络系统安全隐患发现和防护能力。

3．了解物联网的概念及相关基础技术，了解智能摄像头、ID/IC 卡、智能卡、智能家居、可穿戴智能设备等常见安全威胁，熟悉物联网应用环境中典型的安全攻击，如 RFID 攻击等。

4．了解 5G 技术的概念及特征。熟悉 5G 网络架构和关键技术，了解 5G 关键技术存在的安全风险以及安全框架。

5．了解车联网的概念及特征。熟悉车联网体系架构，了解车联网安全威胁类型和安全防护技术。

中国通信企业协会秘书处　　2022 年 7 月 27 日印发