河南省通信管理局
河南省通信行业协会

豫通局函〔2024〕229号

关于举办2024年国家网络安全宣传周河南省电信日活动暨河南省第七届“天安杯”网络安全职业技能竞赛的通知

省各基础电信运营公司、省铁塔公司、中移在线服务有限公司、联通（河南）产业互联网有限公司，各省辖市通信行业协会，相关单位:

为深入贯彻落实习近平总书记关于技能人才工作的重要指示批示精神，加快推进我省电信和互联网行业网络与信息安全高技能人才队伍建设，根据《河南省人力资源和社会保障厅关于组织开展2024年河南省职业技能竞赛活动的通知》（豫人社函

〔2024〕113号）安排，现就2024年国家网络安全宣传周河南省电信日活动暨河南省第七届“天安杯”网络安全职业技能竞赛（以下简称“竞赛”）有关事项通知如下：

一、指导思想

坚持以习近平新时代中国特色社会主义思想为指导，深入贯彻党的二十大和二十届二中、三中全会精神，落实《网络安全法》《数据安全法》有关要求，进一步促进网络与信息安全人才培养，为信息通信行业职工切磋技艺、提升技能、展现风采搭建平台。通过竞赛培育选拔创新型、技能型网络与信息安全人才，提升网络与信息安全意识，提高网络与信息安全保障能力水平，为网络强省、数字河南建设提供有力的网络与信息安全人才保障。

二、组织机构

本次竞赛为省级行业二类赛，由省通信管理局、省通信行业协会主办，中国电信股份有限公司河南分公司承办，新华三技术有限公司、郑州大学网络空间安全学院提供竞赛技术支撑。竞赛成立组委会，全面负责竞赛的组织领导和统筹决策工作，组委会下设办公室和技术工作委员会，办公室设在河南省通信行业协会，负责竞赛政策制定、组织协调和赛前培训安排等工作。技术工作委员会设在新华三技术有限公司、郑州大学网络空间安全学院，负责大赛相关技术保障工作。

各参赛单位负责牵头组织落实本单位选拔赛事宜，并在竞赛举办过程中接受组委会的指导。组委会办公室负责竞赛宣传报道。

三、竞赛项目

本次竞赛分为个人赛、团队赛。

四、参赛对象

凡在省内各基础电信企业从事网络、信息安全管理和维护等相关岗位工作的在职职工，经本单位选拔后可报名参加。已获得“中华技能大奖”“中原技能大奖”“全国技术能手”“河南省技术能手”等荣誉人员及已取得“河南技术能手”申报资格的人员，不得以选手身份参加省级竞赛活动（国赛省级选拔赛除外）。各参赛单位要认真做好参赛人员身份审核工作。

每单位报领队 1 人（不参与比赛），参赛选手数量见附表。参赛队员身份一经上报，不得更改（报名表见附件 1、2）。参赛单位名单及数量要求如下：

参赛单位	参赛人数
中国移动通信集团河南有限公司	不少于 36 人、12 个队
中国联合网络通信有限公司河南省分公司	不少于 36 人、12 个队
中国电信股份有限公司河南分公司	不少于 36 人、12 个队
中国广电河南网络有限公司	不少于 3 人、1 个队
中国铁塔股份有限公司河南省分公司	不少于 3 人、1 个队
中移在线服务有限公司	不少于 6 人、2 个队
联通（河南）产业互联网有限公司	不少于 3 人、1 个队

五、竞赛内容

竞赛内容涵盖电信网、互联网、大数据、工业互联网、物联

网、5G、云计算等相关网络安全领域，结合典型网络安全问题和事件，围绕监测预警、漏洞挖掘、安全运维、团队协作、系统加固和应急响应等，模拟业务场景，加强实战攻防，重点考察参赛选手的网络攻防能力和在安全工作岗位的技术业务能力。

竞赛试题由组委会办公室组织有关专家统一命制（具体竞赛考试大纲、竞赛规则等详见附件 3）。

六、竞赛安排

（一）竞赛报到时间：2024 年 9 月 10 日 9:00;

（二）竞赛时间：2024 年 9 月 10 日 13:00-9 月 11 日 11:30;

（三）竞赛地址：郑州融通紫荆山宾馆一号楼三楼第一会议室（金水区金水路 8 号）。

七、奖项设置

（一）金卫士个人奖

1. 设一等奖 3 名、二等奖 5 名、三等奖 7 名及优胜奖 10 名，由竞赛组委会颁发获奖证书及奖金。

2. 获奖选手按照有关规定晋升相应职业技能等级。

3. 经竞赛组委会审核后对获奖选手授予“河南信息通信行业技术能手”荣誉称号。

4. 竞赛选手成绩将作为全国行业竞赛选拔赛成绩排名并代表河南参赛。

（二）金卫士团体合作奖

设金奖、银奖、铜奖各 1 名，由竞赛组委会颁发获奖证书。

（三）其他奖项

对企业领导重视、精心组织、文明参赛的单位，由组委会颁发“优秀组织奖”奖牌。

八、有关要求

（一）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。在组委会的统一部署下，认真做好大赛各项组织工作，并紧密结合企业生产实际，加强协调和指导工作。

（二）各参赛单位选拔工作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，充分调动网络信息安全人才的参赛热情，提升网络安全保障能力和水平。

（三）各参赛单位于 8 月 31 日前将报名表发送至组委会指定邮箱，并电话联系组委会办公室确认参赛名单。

九、联系方式

组委会办公室：河南省通信行业协会

联系人：　张南　袁冰儿

联系电话：　0371-63686997　18639551197

邮　箱：hntxhx@163.com

竞赛住宿及会务联系人：苗新新　13653860947

附件：1. 河南省第七届“天安杯”网络安全职业技能竞赛个人参赛报名表

2. 河南省第七届“天安杯”网络安全职业技能竞赛团体参赛报名表

3. 河南省第七届“天安杯”网络安全职业技能竞赛大纲

河南省通信管理局　　河南省通信行业协会

2024年8月21日

附件 1

河南省第七届“天安杯”网络安全职业技能竞赛个人参赛报名表

序号	单位	姓名	性别	联系电话	身份证号码	证件照	是否住宿

附件 2

河南省第七届“天安杯”网络安全职业技能竞赛团体参赛报名表

单位：　　领队姓名：　　联系电话：

序号	队名	团队口号	照片	队伍简介	姓名	性别	联系电话	身份证号码	是否住宿

附件 3

河南省第七届“天安杯”网络安全职业技能竞赛大纲

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。

4.了解《密码法》主要内容，包括：核心密码、普通密码、商用密码、法律责任、密码安全的基本策略等要求。

（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；熟悉数据安全特性，了解数据全生命周期安全威胁类型及安全防护技术。

（五）工业互联网安全

熟悉工业互联网安全体系架构，了解工业互联网的特征及常见安全威胁类型和安全防护技术等。熟悉常见的工控协议、工控安全漏洞、恶意代码病毒、安全威胁信息等，了解常见工业互联网安全防护措施及实现原理，掌握典型工业互联网安全监测、应急处置、安全事件取证、溯源分析等技术。

（六）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。

（七）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。

（八）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。

（九）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。

（十）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。

（十一）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。

（十二）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。

三、参考资料

（一）管理部分

1.中华人民共和国网络安全法

2.中华人民共和国数据安全法

3.中华人民共和国个人信息保护法

4.中华人民共和国密码法

5.关键信息基础设施安全保护条例（国令第745号）

6.信息系统安全等级保护定级指南

7.信息系统安全等级保护实施指南

8.通信网络安全防护管理办法（工信部令第11号）

9.电信和互联网用户个人信息保护规定（工信部令第24号）

10.网络产品安全漏洞管理规定（工信部联网安〔2021〕66号）

11.公共互联网网络安全突发事件应急预案

12.公共互联网网络安全威胁监测与处置办法

13.工业和信息化部关于加强电信和互联网行业网络安全工作的指导意见（工信部保〔2014〕368号）

14.电信网和互联网网络安全防护系列标准

15.通信网络安全管理文件与标准汇编

（二）技术部分

1.黑客攻防技术宝典-Web 实战篇（第 2 版）

2.安全实战之渗透测试

3.黑客攻防从入门到精通实战篇（第 2 版）

4.Python 黑帽子：黑客与渗透测试编程之道（第 2 版）

5.信息安全原理与实践（第 3 版）

6.应用密码学（第 3 版）

7.恶意代码逆向分析基础详解

8.恶意代码原理、技术与防范

9.Android 应用安全实战

10.Android 应用安全测试与防护

11.iOS 应用逆向与安全之道

12.iOS 黑客攻防秘籍（第 2 版）

13.无线网络威胁和移动安全隐私

14.大数据安全：技术与管理

15.物联网安全（第 2 版）

16.云原生安全：攻防实践与体系构建

17.数据安全实践指南

18.数据安全与隐私计算

19.工业互联网安全：架构与技术

20.工业互联网安全：架构与防御

四、竞赛规则

（一）个人赛竞赛规则

1.个人赛由大赛组委会统一集中举行，采用“个人理论赛+个人夺旗赛”的方式，参赛选手在相同比赛环境中根据竞赛系统提示完成相应的关卡考题，通过提交正确答案后获得相应分数，总计3小时。

2.个人理论赛与个人夺旗赛分开进行，个人理论赛在开赛30分钟后关闭答题环境，个人夺旗赛在开赛30分钟后开始，开赛3小时后关闭答题环境。

3.个人赛时长180分钟，包括个人理论赛30分钟和个人夺旗赛150分钟。

个人理论赛

1.个人理论赛环境为线下理论题答题系统，参赛选手需在规定时间内使用各自电脑登录访问答题平台并进行作答。

2.理论赛共50道题，题型覆盖单选题、判断题和多选题。

3.主要内容为：网络安全管理知识、网络安全技术知识、系统安全技术知识、应用安全技术知识、新技术应用知识等。

4.题目每作答一题提交一次答案并计相应分数，未完成赛题提交，以当前系统提交分数为准。各参赛选手需注意点击提交，若未及时提交，需自行承担后果。

个人夺旗赛

1.比赛环境为线下夺旗赛竞技平台。

2.夺旗赛竞技平台由竞赛服务器构建，提供统一的访问IP地

址。

3.每位参赛选手的答题环境均完全相同且互相隔离，选手通过独立账户访问答题环境。

4.闯关竞赛答题需要的电脑终端及可能需要的工具需要参赛选手自行准备。

5.夺旗赛题目类型包含：WEB、MISC、CRYPTO、REVERSE、PWN 等题目类型。

（二）团队赛竞赛规则

1.团队攻防赛采用 AWD 网络混战模式，参赛队伍互相进行攻击和防守，通过漏洞获取相应的 flag 得分，修补己方主机漏洞进行防御避免失分。

2.题目类型涵盖 WEB 类、PWN 类等。

3.每个队伍维护的主机环境完全一致。

4.比赛时长 180 分钟，采用回合制，每回合 10 分钟，每回合更新 flag。

河南省通信管理局办公室　　2024年8月21日印发