附件 3

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：商用密码应用及管理、检测与认证、使用与评估等。

（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。

5.了解《商用密码管理条例》（国令第760号）主要内容，包括：管理范围、检测认证、电子认证、使用及评估、监督管理等。

（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（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）基础安全检测与防护

了解操作系统安全、数据库安全、中间件安全、web 及移动应用安全、网络协议安全、代码安全，熟悉常见的攻击方式和防御机制，掌握检测验证、配置加固、逆向分析、攻击监测、告警分析、应急处置等技能。

了解关键信息基础设施的安全防护技术要求，能够评估关基的风险及防护措施，掌握对关基的安全检测与加固方法。

（二）算力安全

了解算力安全的关键技术，包括算力基础设施的安全概念、硬件安全与软件安全的融合、防御机制的设计、算法安全性分析。能够熟练评估算力系统的安全配置及防护措施，掌握对计算中心、云计算平台、大数据处理系统等关键算力资源的安全检测与加固方法，以及应对算力攻击的策略和日志分析与事件监控技巧。

（三）信创安全

了解自主可控技术在安全保障中的重要性，掌握国产软硬件

的安全评估标准与流程。能够熟练识别信创环境中的安全风险，应用相关工具和策略进行安全检测与加固，确保技术的安全性和兼容性。

（四）漏洞挖掘

熟悉漏洞识别与利用的常规技术，包括漏洞扫描工具的使用、渗透测试方法与技巧，包括信息收集、漏洞扫描、静态代码分析、动态应用测试、渗透测试、漏洞利用等。能够有效地进行系统及应用的漏洞检测，掌握漏洞报告与修复流程，提升系统整体的安全性。

（五）社会工程学

了解社会工程学的基本概念与攻击手法，包括钓鱼攻击、预文本等。能够识别社会工程学攻击的迹象，掌握防范措施与应急响应策略，提升对人性弱点的识别与防护能力。

（六）网络威胁研判

掌握网络攻击趋势与模式的分析技能，能够有效评估潜在的网络威胁及其对业务的影响。熟练应用网络情报分析工具，进行安全事件的研判与预警，提升网络防护能力。

（七）数字取证技术

了解数字取证的基本概念与流程，掌握数据提取、证据保全与分析技能。能够熟练使用取证工具，进行安全事件后的证据分析，确保取证过程的合规性与有效性。

（八）隐匿技术与反追踪

掌握隐匿技术的基本原理与应用，包括使用 VPN、加密通讯等

手段。能够识别和应对追踪技术，熟练应用反追踪策略，提升个人与组织的信息安全。

（九）APT 攻击技术分析

了解 APT 攻击的特点与攻击手法，掌握其攻击阶段与工具的分析技能。能够熟练识别 APT 攻击的迹象，评估其威胁并制定相应的防护策略。

（十）应急响应处置

掌握网络安全事件的应急响应流程，包括事件识别、隔离与恢复。能够熟练应用应急响应工具与策略，提升团队协作能力，确保在安全事件发生后的快速响应与业务连续性。

中国通信企业协会秘书处　　2024 年 10 月 25 日印发