CNCA-22-JS01
移动应用程序个人信息安全测试
技能竞赛总结报告

中国网络安全审查技术与认证中心编制

国家市场监管总局认可检测司（认监委）审核批准

二〇二三年三月

目录

1 前言

移动应用程序个人信息安全测试技能竞赛（以下简称：本次竞赛）为国内首次个人信息安全检验检测技能竞赛，由国家认证认可监督管理委员会（简称认监委）主办，由中国网络安全审查技术与认证中心承办。

本次竞赛依据 GB/T 27043-2012《合格评定能力验证的通用要求》、《实验室能力验证实施办法》（市场监督总局 2006 年公告第 9 号）、CNAS-GL002：2018《能力验证结果的统计处理和能力评价指南》、CNAS-GL003：2018《能力验证样品均匀性和稳定性评价指南》、GB/T 28043-2019《利用实验室间比对进行能力验证的统计方法》、GB/T35273-2020《信息安全技术个人信息安全规范》运作实施。

本报告是对本次竞赛结果的总结，由中国网络安全审查技术与认证中心负责起草，国家市场监管总局认可检测司批准发布。

2 竞赛概述

2.1 项目简介

习近平总书记在党的二十大报告中指出“要加快建设网络强国、数字中国，加强个人信息保护”。近年来我国个人信息保护力度不断加大，为落实《网络安全法》、《数据安全法》、《个人信息保护法》等法律关于数据安全管理的规定，规范网络数据处理活动，保护个人、组织在网络空间的合法权益，维护国家安全和公共利益，国务院及其相关部门着手制定相应的规章或规范性文件，个人信息、数据安全的法律保护体系变得更加完善。

移动互联网时代，人们在享受方便快捷的移动网络服务的同时，不可避免地会向网络服务运营者提供更多的个人信息。由于网络服务运营者的个人信息保护能力参差不齐，用户个人信息保护意识有待提高，个人信息保护依旧面临诸多问题和挑战，特别是 App 违法违规收集个人信息问题较为突出。

本次技能竞赛采用理论知识笔试和现场检测实操相结合的考核方式，旨在帮助个人信息安全检验检测机构准确理解和掌握法律法规、标准规范中个人信息的收集要求和测试方法，提高移动应用程序个人信息安全检测结果的一致性，提升个人信息安全检测服务水平；同时大力弘扬劳动精神、工匠精神，积极营造检验检测行业从业人员学习氛围，推动检验检测队伍专业化建设。

2.2 参加机构概况

本次竞赛共有 44 家机构报名参加，通过资格选拔的报名机构有 34 家，其中 2 家因故退出，实际参加机构为 32 家。

参加本次竞赛的检验检测机构来自全国 10 个省/直辖市（详见图 1），其中已获资质认定的机构有 24 家，占比 75%；获得实验室认可的机构有 29 家，占比约 90.6%；获得资质认定且为国家产品质检中心的有 7 家，占比约 21.8%；未获得资质认定或实验室认可的机构有 4 家，占比 12.5%。

图 1 参赛机构地域分布柱状图

2.3 竞赛设计

2.3.1 第一单元——理论知识笔试

考核形式：所有参加机构选派 2 名代表共同使用一台终端通过考试系统在线进行笔试答题。笔试试题类型包括：填空题、单选题、多选题、判断题、简答题和案例分析题，由竞赛专家组出具统一试卷。考试大纲依据：GB/T 35273-2020《信息安全技术 个人信息安全规范》和《中华人民共和国个人信息保护法》相关内容。

考试时间：90 分钟。

试卷分值：试卷总分 100 分。

具体请见附录 A《笔试试卷》。

2.3.2 第二单元——现场检测实操

本次竞赛实操样品为安卓版民生快递 App，由承办单位定制开发并统一提供。所有参加机构选派 1~3 名代表通过在线监控远程方式完成检测。本次竞赛实操方法依据承办单位现场提供的《作业指导书》（依据 GB/T 35273-2020 制定）；实操结束后，参加机构现场填写由承办单位提供的《结果报告单》，作为该参加机构本次竞赛现场检测实操结果。

实操时间：180 分钟。

实操分值：实操总分 100 分。

具体请见附录 B《作业指导书》。

2.4 竞赛评分规则

本次竞赛分为理论知识笔试和现场检测实操两个单元，每个单元满分均为100分。

2.4.1 笔试成绩

理论知识笔试成绩采用系统判卷和人工评价相结合的方式得出评分。

2.4.2 实操成绩

实操成绩由竞赛专家组依据《评价细则》进行分组评分，并通过公议方式确定最终得分。

2.4.3 综合成绩

综合成绩=笔试成绩×50%＋实操成绩×50%。

2.4.4 技能竞赛结果评价

本次竞赛依据各参加机构综合成绩进行排名，详情见附录D。

2.5 日程安排

本次竞赛的日程安排如表1所示：

表1 竞赛日程安排

序号	竞赛阶段	日程安排
1	认监委发布竞赛通知，开始接受报名	2022年9月20日
2	竞赛试卷及实操样品准备与验证	2022年9~12月
3	竞赛准备事项发布，确认参赛人员信息	2022年12月5日
4	竞赛详细日程安排及注意事项发布	2022年12月22日
5	作业指导书发布	2022年12月28日
6	竞赛实施	2022年12月29日
7	完成竞赛总结报告编制	2023年3月

2.6 保密性要求

出于保密的要求，本次竞赛对每个参加机构赋予一个唯一性代码，代码为PQHR01~JWMW34，其中前四位为随机大写英文字母，后两位为递增的阿拉伯数字。在本报告中，凡说明与参加机构有关的竞赛结果和成绩时，均以上述代码表示，总结报告将发送给每一个参加机构。

3 竞赛结果统计分析与评价

3.1 笔试结果统计

本次竞赛中参加机构笔试成绩如图 2 所示：

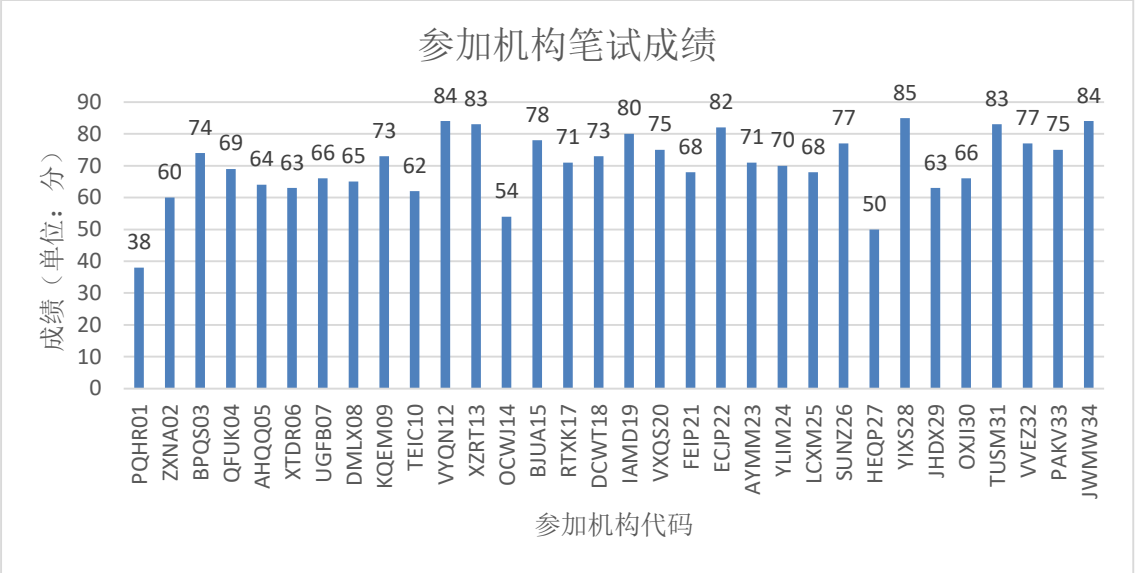

图 2 参加机构笔试成绩柱状图

3.2 实操结果统计

本次竞赛中参加机构实操成绩如图 3 所示：

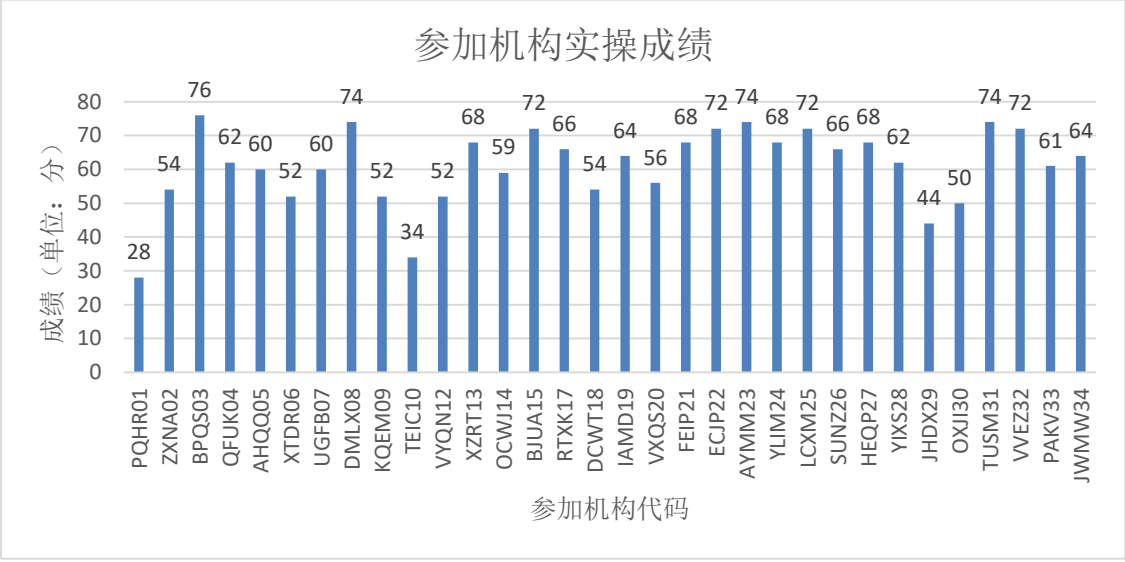

图 3 参加机构实操成绩柱状图

3.3 竞赛结果评价

参加本次竞赛并提交结果的 32 家参加机构中，12 家机构综合成绩≥70 分，

占比 37.5%；12 家机构综合成绩介于 60~70 分之间，占比 37.5%；6 家机构综合成绩介于 50~60 分之间，占比 18.75%；2 家机构综合成绩＜50 分，占比 6.25%。本次技能竞赛最终结果评价见表 2。

表 2 本次竞赛最终结果评价

结果情况	机构代码	合计家数	比例
综合成绩≥70 分	TUSM31、ECJP22、XZRT13、BPQS03、BJUA15、VVEZ32、JWMW34、YIXS28、AYMM23、IAMD19、SUNZ26、LCXM25	12	37.5%
70 分＞综合成绩≥60 分	DMLX08、YLIM24、RTXK17、VYQN12、FEIP21、PAKV33、QFUK04、VXQS20、DCWT18、UGFB07、KQEM09、AHQQ05	12	37.5%
60 分＞综合成绩≥50 分	HEQP27、OXJI30、XTDR06、ZXNA02、OCWJ14、JHDX29	6	18.75%
综合成绩＜50 分	TEIC10、PQHR01	2	6.25%

本次竞赛中参加机构综合成绩如图 4。

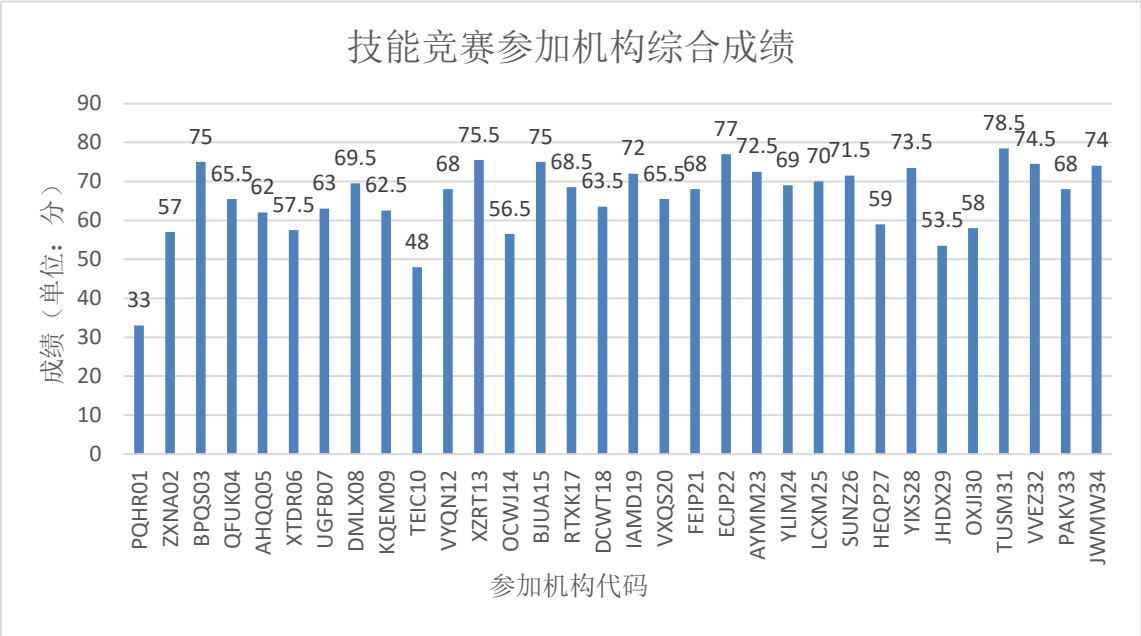

图 4 参加机构综合成绩柱状图

4 技术分析和建议

移动应用程序个人信息安全测试结果受多种因素影响，主要包括标准的理解、检测设备与检测方法的掌握以及团队协作等方面。针对本次竞赛回收的32家参加机构提交的结果报告单和笔试答卷，实施机构从技能竞赛的两个单元进行了汇总分析，以期为参加机构提供理论知识笔试和移动应用程序个人信息安全测试的技术建议。

（一） 加强标准和法律的研究与理解

加强对GB/T 35372标准和《个人信息保护法》的理解与研究。准确地理解并识别个人信息是开展个人信息安全测试的基础条件。在理论知识笔试中，部分机构对个人信息定义的理解不足，例如填空题第1题中关于对个人信息定义的考查，参加机构的答题正确率仅有34.38%。此外，GB/T 35273标准与《个人信息保护法》中对不同敏感程度的个人信息提出了差异化的授权要求，如“授权同意”、“明示同意”和“单独同意”等要求。面对相关知识点的考核，部分参加机构存在概念上的混淆。部分参加机构对“隐瞒收集”与“提前收集”问题定位不清晰，约22%参加机构将提前收集行为视同为隐瞒收集，存在标准理解和问题定位的偏差。仍需进一步研读标准和法律要求，以确保对标准理解的准确性。

（二） 加强自动检测和人工分析相结合的能力

目前移动应用程序检测工具多种多样，不同工具所提供的个人信息检测结果不尽相同，因此个人信息安全测试不能仅依靠工具自动检测出具结果报告，而更多地需要人工进行分析和判断。本次竞赛实操结果反馈中，部分参加机构的检测结果直接采用工具检测结果，存在测试场景分析不足、测试覆盖不全面，或测试不够深入导致未能发现样品预置的全部缺陷的问题。建议开展检测活动前进行充分评估，配备适当的人员和检测工具。多人协作利用自动化检测工具出具检测结果时，应对结果进行人工分析和校验，以确保结果的正确性和充分性。

（三） 重视检测过程的规范性

本次竞赛的作业指导书中明确要求“无论检测结果符合与否，均需充分给出判定理由和证据”。从本次竞赛反馈结果来看，部分参加机构提交的《结果报告单》中存在结论与描述不一致的情况，缺乏图片证据支撑，导致结果无法溯源。建议参加机构在开展检测活动过程重视作业指导文件，规范检测结果描述，以确

保结果的准确性。

（四） 加强团队建设和协作能力的培养

本次竞赛实施期间，新冠疫情给参加机构在人员安排、团结协作等方面带来一定考验。部分机构能够提前做好替补人员的安排，明确任务分工，竞赛当天全员到位，井然有序地完成竞赛考核。部分机构在赛前临时更换了参赛人员，竞赛当天人员配备不足，在规定时间内完成检测任务略显困难。建议参加机构加强检测人员队伍建设和团队协作能力培养，以提高面对不同挑战的应对能力。

5 技能竞赛组织机构和实施机构

5.1 竞赛组织机构

国家市场监管总局认可检测司（认监委）

5.2 竞赛实施机构

中国网络安全审查技术与认证中心

竞赛实施负责人：张晓梅

技术专家：许静慧、袁翠红、陈淑娟

统计专家：袁翠红、杨莉

联络人员：许静慧

电话：010-65994649

邮箱：ccrcptp@isccc.gov.cn

地址：北京市东城区天坛东路 31 号铜牛信息大厦 B 座

6 依据的标准和规范

1、《实验室能力验证实施办法》（市场监督总局 2006 年公告第 9 号）

2、GB/T 27043-2012《合格评定能力验证的通用要求》

3、GB/T 28043-2011《利用实验室间比对进行能力验证的统计方法》

4、CNAS-GL002：2018《能力验证结果的统计处理和能力评价指南》

5、CNAS-GL003：2018《能力验证样品均匀性和稳定性评价指南》

6、GB/T 35273-2020《信息安全技术个人信息安全规范》

附录 A 笔试试卷

“移动应用程序个人信息安全测试”技能竞赛笔试题

（总分 100 分）

姓名：_____所在单位：_____证件号码：_____

一、 填空题（每空 2 分，共 5 空，总分 10 分）

1. 个人信息是以电子或其他方式记录的能够____或者与其他信息结合____特定自然人身份或反映特定自然人活动情况的各种信息，包括个人____信息，如个人生物识别信息、行踪轨迹等。

2. 根据《个保法》规定，收集敏感个人信息前，应取得个人信息主体的_____同意。

3. 收集个人信息前应征得个人信息主体的授权同意。授权同意包括通过积极的行为作出授权即_____同意，或者通过消极的不作为而作出授权。

二、 单选题（每题 2 分，共 10 题，总分 20 分）

4. App 收集的个人信息类型应与实现服务的业务功能有直接关联关系，体现了个人信息安全的哪项基本原则。（）

A、权责一致

B、目的明确

C、最小必要

D、公开透明

5. 日常生活中为了保护个人信息安全，我们不应采取___。（）

A、签收快递后及时撕毁快递包裹上的个人信息

B、为了增加面试机会，大量投递个人简历

C、输入密码时确保无人偷窥

D、使用后及时销毁身份证复印件

6. 下列场景中不属于收集个人信息的是____。（）

A、某 App 自动采集用户的地理位置信息。

B、某 App 注册会员时需要用户输入职业类型。

C、某 App 通过嵌入第三方 SDK 记录用户行为日志。

D、某 App 支持离线地图为用户提供路线规划服务。

7. App 在收集下列各类（）信息时，除了向个人信息主体告知收集、使用个人信息的目的、方式和范围等规则，应征得个人信息主体的明示同意；并确保个人信息主体的明示同意是其在完全知情的基础上自主给出的、具体的、清晰明确的意愿。

A、个人信息主体账号、IP 地址、个人数字证书等。

B、个人学历、社保卡、体检报告等。

C、设备软件列表、网页浏览记录、交易和消费记录等。

D、好友列表、通信记录和内容、行踪轨迹等。

8. 下列哪种情形中，个人信息控制者可以不响应个人信息主体的请求。（）

A、当 App 存在将个人信息非法提供向第三方时，用户向个人信息控制者提出请求撤回授权同意和删除个人信息。

B、当 App 展示的个人信息有错误时，用户向个人信息控制者提出请求更正个人信息。

C、用户向个人信息控制者提出获取个人信息副本请求可能涉及商业秘密。

D、个人信息控制者响应用户的请求将导致个人信息主体或其他个人、组织的合法权益受到严重损害。

9. 某招聘类 App 在明示告知和征得用户同意后采集了本机的 MAC 地址、地理位置信息，注册时用户通过手动填写姓名、电话号码、身份证号码、学历等信息完成注册，则以下关于 App 向用户提供个人信息副本的描述正确的是（）。

A、宜提供姓名、电话号码、身份证号码、学历信息。

B、可不提供 MAC 地址、地理位置。

C、必须提供姓名、电话号码、身份证号码、学历信息、MAC 地址、地理位置。

D、不能将个人信息副本传输给用户指定的第三方。

10. App 运营者（甲）购买了第三方服务提供者（乙）的短信接口服务，从

而实现甲调用乙的短信接口向 App 客户端用户发送短信验证码、通知、广告等信息。甲与乙双方合同约定，乙不得留存或访问向甲提供短信接口服务中涉及的信息内容。请问该场景下甲与乙是以下哪种关系（）。

A、共享

B、转让

C、委托处理

D、共同个人信息控制者

11. A 公司因经营不善将其拥有的全部个人信息卖于 B 公司，且双方通过合同和技术手段确保 A 删除了全部个人信息。请问该场景下 A 与 B 是属于哪种关系（）

A、共享

B、转让

C、委托处理

D、共同个人信息控制者

12. App 在收集个人信息前可采用不同方式向用户进行告知，以下哪种场景的告知方式是不符合规范的（）。

A、某 App 提供的快捷登录功能需要收集用户的指纹识别信息，在首次启动时 App 主动弹出包含个人信息保护政策访问链接的独立界面，通过个人信息保护政策向个人信息主体告知了各项业务功能收集、使用个人信息的目的、方式和范围等规则，并提供了同意或不同意的选择按钮。

B、某 App 的注册、登录功能支持第三方平台账号登录，可通过第三方平台间接获取用户的账号、姓名、电话号码信息；App 在获取个人信息前，通过跳转至第三方平台的申请授权窗口的方式征得个人信息主体明示同意。

C、某 App 的基本业务功能需要收集用户的学历、学位、教育经历、培训经历等信息，在收集不满 14 周岁未成年人用户的个人信息前，通过单独弹窗的方式征得了未成年人或其监护人的明示同意。

D、某 App 提供多项需要收集个人信息的业务功能时，通过首次使用时弹窗形式和提供个人信息保护政策的方式告知了各项业务功能收集、使用个人信息的目的、方式和范围等规则。

13. 根据《个人信息保护法》规定，以下哪些活动属于对个人信息的处理（）。

A、产生、使用、维护、销毁

B、收集、传输、存储、销毁

C、产生、使用、加工、传输

D、收集、使用、加工、删除

三、 多选题（每题 4 分，共 5 题，总分 20 分，选错或少选多选均不得分）

14. 以下关于 App 收集个人信息的情形正确的是____。（）

A、征得授权同意前收集与业务功能有关的必要个人信息

B、征得授权同意后收集与业务功能无关的个人信息

C、征得授权同意后收集与业务功能有关的个人信息

D、征得授权同意后收集与业务功能有关的必要个人信息

15. 为保障敏感个人信息安全，招聘者在网上征集简历时应避免收集以下哪些个人信息：（）

A、手机号码

B、身份证号码

C、宗教信仰

D、生育信息

16. 以下行为中你认为哪些是不合规的：（）

A、某 App 为方便用户快速登录，登录界面默认勾选“我已阅读并同意隐私政策”。

B、App 业务功能中收集的个人信息与隐私政策中告知用户收集的个人信息类型不相符。

C、某 App 在用户同意隐私政策后，在后台持续采集设备软件列表、MAC 地址等个人信息，而隐私政策中未告知用户该种场景。

D、某 App 在用户同意隐私政策前，在后台多次调用 IMEI 接口将 IMEI 信息上传至服务器。

17. 个人信息控制者开展个人信息处理活动应遵循合法、正当、必要的原则，

以下哪些说法是正确的：（）

A、向个人信息主体明示个人信息处理目的、方式、范围等规则，征求其授权同意。

B、以明确、易懂和合理的方式公开处理个人信息的范围、目的、规则等，如涉及商业秘密的，可不接受外部监督。

C、只处理满足个人信息主体授权同意的目的所需的最少个人信息类型和数量。目的达成后，应及时删除个人信息。

D、向个人信息主体提供能够查询、更正、删除其个人信息，以及撤回授权同意、注销账户、投诉等方法。

18. 个人信息控制者在收集个人信息前，应当以显著方式、清晰易懂的语言真实、准确、完整地向个人信息主体告知下列事项。（）

A、个人信息控制者的身份信息

B、个人信息的处理目的、方式、范围以及保存期限

C、个人信息主体的权利和实现方法

D、提供个人信息后可能存在的安全风险

四、 判断题（每题 2 分，共 10 题，总分 20 分，请填写“对”或“错”）

19. 个人信息经匿名化处理后所得的信息不再属于个人信息。

20. 用户画像或特征标签不属于个人信息。

21. 向香港或澳门地区的个人信息处理者提供、传输个人信息，属于个人信息跨境提供。

22. 收集个人生物特征信息前，App 通过隐私政策告知收集、使用个人生物识别信息的目的、方式和范围，以及存储时间等规则，并征得用户的明示同意。

23. 采用泛化、假名化、加密等方法可实现个人信息的去标识化处理。

24. App 用户在申请注销账号操作时，受运营者统一账号管理平台的影响，需要同时注销平台旗下所有 App 相关账号。

25. 当用户拒绝提供 App 所需必要个人信息时，App 不再提供基本业务功能。

26. 某 App 向用户明示告知，为保障改善服务质量、提升使用体验、研发新产品、增强安全性等为由，须收集用户相应的个人信息。

27. 为满足收集个人信息最小必要原则，在设计 App 自动收集个人信息的业务功能时，可根据实际业务场景的需要对个人信息进行多次采集。

28. 用户在使用某 App 的扩展业务功能时，拒绝同意 App 扩展业务功能所必要收集的个人信息，App 可向用户拒绝提供基本业务功能。

五、 简答题（每题 5 分，共 3 题，总分 15 分）

29. 收集个人信息的方式有哪些？

30. 如何判断某款 App 是否存在超范围收集个人信息的行为？

31. 请举例说明明示同意与单独同意的联系与区别。

六、 场景分析题（共 3 题，总分 15 分）

32. （二选一）某教育类 App 需要老师通过后台系统注册填写学生信息后，学生才可以登录使用 App，那么 App 运营方通过哪种收集方式获得了学生个人信息？请给出理由。

33. （二选一）某基金证券类 App 运营者存在基金代销的情况，用户从第三方代销公司购买基金后其个人信息会在该基金公司核心系统留存，那么 App 运

营者通过哪种收集方式获取了个人信息？请给出理由。

34. 某 App 属于社交、电子商务类型，要求注册用户具有虚拟的个人消费账户。App 要求注销账号需满足以下条件之一：1）账号余额为 0；2）可消费卡券余额为 0 或已全部过期失效（等值金额过期默认是 1 年有效期）。

某用户拟注销平台账号时，发现其账号余额（定义见注 1）和可消费卡券余额（定义参考注 2）均大于 0 元，但又不足以购买 App 中相关商品或服务，且等待两月后卡券过期失效。

注 1：“账号余额”是使用货币购买的虚拟资产或退款所得，不支持提现。

注 2：“可消费卡券余额”是参加平台活动获得的等值金额奖励，如积分/消费券/红包等具有人民币价值且可消费的属性类型。

请问平台以上的做法是否符合 GB/T 35273 中关于注销账户的要求？请详细说明理由。

35. 您认为开展个人信息安全测试需具备哪些方面技术能力和哪些类别专业检测工具？贵单位在个人信息安全检测方面有哪些技术优势？

附录 B 作业指导书

中国网络安全审查技术与认证中心

CNCA-22-JS01“移动应用程序个人信息安全测试”技能竞赛作业指导书

各参加机构：

首先感谢贵机构参加本次技能竞赛。“移动应用程序个人信息安全测试”技能竞赛是国家认证认可监督管理委员会（CNCA）组织，中国网络安全审查技术与认证中心承担的能力验证计划（项目编号为：CNCA-22-JS01）。

在本次能力验证计划中，贵机构的代码为_____

为保证本次技能竞赛工作顺利进行，特作如下说明：

1. 样品说明

本次技能竞赛样品为 安卓版民生快递 App，样品编号为： MESD-JS01 ，已通过稳定性测试和其他有关验证。

实施机构将在 2022 年 12 月 29 日 13:30 开始通过腾讯会议聊天功能统一发送样品下载链接至各参加机构。请各机构务必在 12 月 29 日 13:00 准时上线签到，以免延误正式比赛。

各机构在收到样品时，应首先对样品状态进行确认，请在第一时间通过腾讯会议聊天功能派**机构代表**与实施机构**私信反馈样品状态是否良好。如发现样品存在问题，请务必在 30 分钟之内联系实施机构**（联系电话：010-65994649 或加微信：18101226510），**超时未反馈视为样品接收状态正常**。需填写《认监委能力验证项目测试样品接收确认表》(见附件一)，并在测试结束时与其他资料一并提交至实施机构。

2. 检测说明

2.1. 检测时间

实操测试将于 2022 年 12 月 29 日下午 14:00 至 17:00 进行，测试总时长为 3 小时，其中包含测试和结果提交时间。各参加机构须在 2022 年 12 月 29 日

17:00 前向指定邮箱（ccrcptp@isccc.gov.cn ）提交电子版测试结果和相关证明材料，邮件主题命名格式为：“CNCA-22-JS01 技能竞赛结果-机构代码”。未按时提交测试结果的，实施机构将取消该机构的检测实操成绩。

2.2. 检测内容及约束

本次能力验证计划要求按照 GB/T 35273-2020《信息安全技术 个人信息安全规范》部分条款内容（详见 2.3）对能力验证样品进行检测，其他内容不在本次测试范围。注意事项如下：

1) 样品的数据类型及长度限制，不作为此次评价内容。

2) 建议采用市场上主流品牌厂商（华为或小米）的安卓测试手机，并确保操作系统为 Android 6.0 以上版本。

2.3. 检测内容要求

2.3.1. 收集个人信息的合法性

对个人信息控制者的要求包括：

a) 不应隐瞒产品或服务所具有的收集个人信息的功能。

2.3.2. 多项业务功能的自主选择

当产品或服务提供多项需收集个人信息的业务功能时，个人信息控制者不应违背个人信息主体的自主意愿，强迫个人信息主体接受产品或服务所提供的业务功能及相应的个人信息收集请求。对个人信息控制者的要求包括：

a) 应把个人信息主体自主作出的肯定性动作，如主动点击、勾选、填写等，作为产品或服务的特定业务功能的开启条件。个人信息控制者应仅在个人信息主体开启该业务功能后，开始收集个人信息；

b) 个人信息主体不授权同意使用、关闭或退出特定业务功能的，不应频繁征求个人信息主体的授权同意；

c) 个人信息主体不授权同意使用、关闭或退出特定业务功能的，不应暂停个人信息主体自主选择使用的其他业务功能，或降低其他业务功能的服务质量；

2.3.3. 收集个人信息时的授权同意

对个人信息控制者的要求包括：

a) 收集个人生物识别信息前，应单独向个人信息主体告知收集、使用个人生物识别信息的目的、方式和范围，以及存储时间等规则，并征得个人信息主体的明示同意；

b) 收集年满 14 周岁未成年人的个人信息前，应征得未成年人或其监护人的明示同意；不满 14 周岁的，应征得其监护人的明示同意。

2.3.4. 个人信息保护政策

对个人信息控制者的要求包括：

a) 应制定个人信息保护政策，内容应包括但不限于：

1) 个人信息控制者的基本情况，包括主体身份、联系方式；

2) 收集、使用个人信息的业务功能，以及各业务功能分别收集的个人信息类型。涉及个人敏感信息的，需明确标识或突出显示；

3) 个人信息收集方式、存储期限、涉及数据出境情况等个人信息处理规则；

4) 对外共享、转让、公开披露个人信息的目的、涉及的个人信息类型、接收个人信息的第三方类型，以及各自的安全和法律责任；

5) 个人信息主体的权利和实现机制，如查询方法、更正方法、删除方法、注销账户的方法、撤回授权同意的方法、获取个人信息副本的方法、对信息系统自动决策结果进行投诉的方法等；

6) 提供个人信息后可能存在的安全风险，及不提供个人信息可能产生的影响；

7) 遵循的个人信息安全基本原则，具备的数据安全能力，以及采取的个人信息安全保护措施，必要时可公开数据安全和个人信息保护相关的合规证明；

8) 处理个人信息主体询问、投诉的渠道和机制，以及外部纠纷解决机构及联络方式。

b)个人信息保护政策应公开发布且易于访问，例如在网络主页、移动互联网应用程序安装页、附录 C 中的交互界面或设计等显著位置设置链接。

3. 结果反馈说明

1)各参加机构须在 **2022 年 12 月 29 日 17:00 之前**将《被测物品接收状态确认表》、《能力验证结果报告单》签字扫描版发送至邮箱（ccrcptp@isccc.gov.cn）。文件命名规则如下：

■ 《被测物品接收状态确认表》命名格式为“CNCA-22-JS01 状态确认表-机构代码” ，如机构代码为“CCRC01”，则文件名称为“CNCA-22-JS01 状态确认表-CCRC01”。

■ 《能力验证结果报告单》命名格式为“CNCA-22-JS01 结果报告单-机构代码”。

2) 各参加机构应根据每个检测项目给出对应的检测结果，并填写《能力验证结果报告单》（见附件二）。无论检测结果符合与否，均需充分给出判定理由和证据，如篇幅有限可另附文档（例如：截图、录屏等），格式不限。检测结果内容必须明确描述，出现模糊描述（如：部分、等等）将影响本次能力验证评价结果。

3) 各参加机构在测试结束后需拷贝本机录频文件，并以机构代码命名文件夹，通过优盘、光盘等存储介质提交至实施机构，同时在本地留存录频文件以备查。如无故未提交录频或未进行录制的按作弊处理。

各参加机构应在 **2022 年 12 月 29 日 24:00**（以快递单打印为准）之前，按《结果提交清单》（见附件三）要求寄出纸质文档。如无故未按时提交纸质文档的，实施机构视情况采取扣分处理。

4. 保密说明

在本次能力验证计划实施过程中，要求参加机构独立完成检测，**严禁参加机构相互串通结果**。一经发现确认，将采取取消机构成绩的处罚措施。

我中心将对各参加机构的有关信息保密，各机构均以代码表示，能力验证结果信息将由我中心统一汇总并对外发布。

5. 联系方式

联系人：许静慧　　电　话：010-65994649/18101226510

地　址：北京市东城区天坛东路 31 号铜牛信息大厦 B 座

联系邮箱：ccrcptp@isccc.gov.cn

附件一：

被测物品接收状态确认表

项目编号： CNCA-22-JS01 机构代码：

能力验证计划名称	移动应用程序个人信息安全测试		
实 施 机 构	中国网络安全审查技术与认证中心		
联 系 电 话	010-65994649	联系人	许静慧
发 送 状 态	完好 ■ 不完好 □	发 送 人	许静慧
接收机构名称： 联系地址： 邮编： 联系电话： 联系人： 接收人签名： 接收时间：			
接收时，被测物品状态是否良好： 是 □ 否 □			
如需要，对接收状态的详细说明：			
注： 如发现样品下载后无法正常安装及使用，请在 30 分钟内联系实施机构。			

附件二：

CNCA-22-JS01 移动应用程序个人信息安全测试技能竞赛

结果报告单

一、 基本信息

机 构 名 称		机构代码	
地　　址			
认可注册号（如适用）		资质认定证书编号（如适用）	

注：认可注册号和资质认定证书编号栏，未获认可的实验室可不填写。

二、 检测信息

检测时间	**检测人员**
2022 年 12 月 29 日	

检测工具					
序号	工具名称	版本号	序号	工具名称	版本号
1			2		
3			4		
5			6		

三、 检测结果

序号	检测项目（作业指导书对应的章节号/名称）			检测结果	
	章节号	名称	章节号	判定结果	检测详情
1	2.3.1	收集个人信息的合法性	2.3.1 a）	□符合 □不符合	检测结果描述： 证据截图：
2	2.3.2	多项业务功能的自主选择	2.3.2a）	□符合 □不符合	检测结果描述： 证据截图：

序号	检测项目（作业指导书对应的章节号/名称）			检测结果	
	章节号	名称	章节号	判定结果	检测详情
3			2.3.2b）	□符合 □不符合	检测结果描述：
					证据截图：
4			2.3.2c）	□符合 □不符合	检测结果描述：
					证据截图：

<table>
<tr><td rowspan="2">序号</td><td colspan="3">检测项目
（作业指导书对应的章节号/名称）</td><td colspan="2">检测结果</td></tr>
<tr><td>章节号</td><td>名称</td><td>章节号</td><td>判定结果</td><td>检测详情</td></tr>
<tr><td rowspan="2">5</td><td rowspan="4">2.3.3</td><td rowspan="4">收集个人信息时
的授权同意</td><td rowspan="2">2.3.3a）</td><td rowspan="2">□符合 □不符合</td><td>检测结果描述：</td></tr>
<tr><td>证据截图：</td></tr>
<tr><td rowspan="2">6</td><td rowspan="2">2.3.3b）</td><td rowspan="2">□符合 □不符合</td><td>检测结果描述：</td></tr>
<tr><td>证据截图：</td></tr>
</table>

<table>
<tr><td rowspan="2">序号</td><td colspan="3">检测项目
（作业指导书对应的章节号/名称）</td><td colspan="2" rowspan="2">检测结果</td></tr>
<tr><td>章节号</td><td>名称</td><td>章节号</td></tr>
<tr><td>7</td><td rowspan="2">2.3.4</td><td rowspan="2">个人信息保护政策</td><td>2.3.4a）</td><td>□符合 □不符合</td><td>检测结果描述：
证据截图：</td></tr>
<tr><td>8</td><td>2.3.4b）</td><td>□符合 □不符合</td><td>检测结果描述：
证据截图：</td></tr>
<tr><td colspan="2">检测人（签字）：</td><td colspan="2"></td><td>审核人（签字）：</td><td></td></tr>
<tr><td colspan="6">备注：

实验室负责人（签字）：
实验室（盖章）：
年 月 日</td></tr>
</table>

附件三：

CNCA-22-JS01 移动应用程序个人信息安全测试

技能竞赛结果提交清单

电子版提交文档（17:00 之前）：

☐ 被测物品接收状态确认表（签字扫描版）

☐能力验证结果报告单（签字扫描版）

纸质版提交文档（24:00 之前）：

☐报名表盖章版原件（纸质）

☐ 被测物品接收状态确认表（纸质）

☐能力验证结果报告单（纸质）

☐本地录频（光盘/优盘）

☐其他 (请说明)

附录 C 评价细则

C1.《笔试参考答案》

一、填空题　1.单独、识别、敏感 2.单独 3.明示

二、单选题　4-8. CBDDD　9-13.ACBCD

三、多选题　14.CD　15.BCD　16.ABCD　17.ACD　18.ABCD

四、判断题　19-28.对错对错对错对错对错

五、简单题

29.评分参考：（1）由个人信息主体主动提供；（2）通过与个人信息主体交互或记录个人信息主体行为等自动采集；（3）通过共享、转让、搜集公开信息等间接获取个人信息等行为。描述了“主动提供”、“自动采集”、“间接获取”得 3 分，结果描述的完整性得 1-2 分。

30.评分参考：（1）判断 App 收集的必要个人信息是否超出相关服务类型的必要信息范围；（2）判断 App 收集的有关个人信息是否与隐私政策描述一致；（3）判断 App 是否存在收集无关个人信息的情况。答出任意一点得 2 分，答出 3 点得 5 分。

31.评分参考：明示同意和单独同意都是授权同意的一种方式，区别于默示同意。单独同意也是一种明示同意。完整描述明示同意与单独同意存在的联系（2 分）；单独同意是相对于一揽子同意的，明示同意是相对于默示同意的。完整描述明示同意与单独同意的区别（3 分）。

32.答案与分析：属于主动提供或直接获取（2 分）。由于老师与学生均为软件系统（含客户端 App 和后台系统）的用户，属于直接获取个人信息。（3 分）

33.答案与分析：属于间接获取（2 分）。该基金公司（个人信息控制者）通过第三方代销公司（其他个人信息控制者）共享或者委托处理获得个人信息主体的个人信息（3 分）。

34.答案与分析：不符合注销账户相关要求（2 分）。围绕该平台设置的注销账号条件存在不合理和额外增加个人信息主体义务的情况不满足 GB/T 35273 8.5d)的要求进行描述的（3 分）。

35.评分参考：体现了人员对个人信息相关法律法规、标准规范的理解（1 分）；体现了人员技术能力（1 分）；体现了熟悉的工具（1 分）；体现单位情况：规模、项目经验、人员获证情况、管理情况等（2 分）。

C2.《实操评价细则》

序号	作业指导书章节号/名称	检测要求	评分说明	分值
1	2.3.1. 收集个人信息的合法性	a）不应隐瞒产品或服务所具有的收集个人信息的功能。	（1）检测结果包括：判定结果为不符合，得 2 分； **扣分说明：**判定结果为符合，-2 分；	14 分
			（2）检测结果包括：描述了隐瞒收集 Android_ID，且提供充分证据证明，得 4 分； **扣分说明：** 1） 未描述隐瞒收集 Android_ID，-2 分；部分描述隐瞒收集 Android_ID，-1 分。 2） 未提供隐瞒收集 Android_ID 证据，-2 分；提供部分证据，-1 分。	
			（3）检测结果包括：描述了隐瞒收集剪切板内容，且提供充分证据证明，得 4 分； **扣分说明：** 1） 未描述隐瞒收集剪切板内容，-2 分；部分描述，-1 分。 2） 未提供隐瞒收集剪切板内容证据，-2 分；提供部分证据，-1 分。	
			（4）检测结果包括：描述了私自截留第三方服务所需的个人信息（如姓名、电话、地址），且提供充分证据证明，得 4 分。 **扣分说明：** 1） 未描述私自截留第三方服务所需的个人信息，-2 分；部分描述，-1 分。 2） 未提供私自截留第三方服务所需的个人信息证据，-2 分；提供部分证据，-1 分。	

序号	作业指导书章节号/名称	检测要求	评分说明	分值
2	2.3.2. 多项业务功能的自主选择	a）应把个人信息主体自主作出的肯定性动作，如主动点击、勾选、填写等，作为产品或服务的特定业务功能的开启条件。个人信息控制者应仅在个人信息主体开启该业务功能后，开始收集个人信息；	检测结果包括： （1）判定结果为不符合，得 2 分； （2）完整描述了未同意隐私政策前存在收集 MAC 地址，且提供充分证据证明，得 6 分。 **扣分说明：** 1） 判定结果为符合，-2 分； 2） 未描述同意隐私政策前提前收集 Mac 地址，-3 分；部分描述同意隐私政策前提前收集 Mac 地址，-1 分。 3） 未提供同意隐私政策前提前收集 Mac 地址证据，-3 分；提供部分证据，-1 分。	8 分
3		b）个人信息主体不授权同意使用、关闭或退出特定业务功能的，不应频繁征求个人信息主体的授权同意；	检测结果包括： （1）判定结果为符合，得 2 分； （2）描述了未发现 App 存在频繁征求个人信息主体的授权同意或者描述了 App 不存在频繁征求个人信息主体的授权同意，且提供充分证据证明得 12 分。 **扣分说明：** 1） 判定结果为不符合，-2 分； 2） 描述存在频繁征求个人信息主体的授权同意，-8 分；部分描述未频繁征求个人信息主体的授权同意，-2 分。 3） 未提供有关证据，-4 分；提供部分证据，-2 分。	14 分

序号	作业指导书章节号/名称	检测要求	评分说明	分值
4		c)个人信息主体不授权同意使用、关闭或退出特定业务功能的，不应暂停个人信息主体自主选择使用的其他业务功能，或降低其他业务功能的服务质量；	检测结果包括： （1）判定结果为不符合，得 2 分； （2）描述了拒绝提供位置权限，无法正常使用“查询快递”功能，且提供充分证据证明，得 8 分 **扣分说明：** 1） 判定结果为符合，-2 分； 2） 未描述拒绝提供位置权限后无法正常使用“查询快递”功能，-4 分；部分描述拒绝提供位置权限后无法正常使用“查询快递”功能，-2 分。 3） 未提供拒绝提供位置权限后无法正常使用“查询快递”功能相关证据，-4 分；提供部分证据，-2 分。	10 分
5	2.3.3. 收集个人信息时的授权同意	a)收集个人生物识别信息前，应单独向个人信息主体告知收集、使用个人生物识别信息的目的、方式和范围，以及存储时间等规则，并征得个人信息主体的明示同意；	检测结果包括： （1）判定结果为符合，得 2 分； （2）描述了 App 收集人脸信息前，通过《人脸识别协议》单独告知了收集、使用个人生物识别信息的规则，且提供充分证据证明，得 8 分； （3）描述了提供勾选、点击等方式征得明示同意，且提供充分证据证明，得 6 分。 **扣分说明：** 1） 判定结果为不符合，-2 分； 2） 未体现通过《人脸识别协议》单独告知了收集、使用个人生物识别信息的规则，-8 分；未描述单独告知收集、使用个人生物识别信息规则，或未提供有效证据，-4 分；部分描述通过《人脸识别协议》单独告知了收集、使用个人生物识别信息的规则，-2 分；提供部分证据，-2 分。 3） 未体现通过勾选、点击等方式征得明示同意，-6 分；未描述征得明示同意或未提供明示同意有效证据，-3 分，部分描述或提供部分证据，-2 分。	16 分

序号	作业指导书章节号/名称	检测要求	评分说明	分值
6		b）收集年满 14 周岁未成年人的个人信息前，应征得未成年人或其监护人的明示同意；不满 14 周岁的，应征得其监护人的明示同意；	检测结果包括： （1）判定结果为不符合，得 2 分； （2）描述了隐私政策说明了处理未满 14 周岁未成年个人信息的规则，未说明收集年满 14 周岁未成年人个人信息的规则，得 2 分； （3）描述了在“实名认证”时，使用未成年人身份证号进行验证时，并征得明示同意，且提供充分证据证明，得 4 分； （4）描述了使用“学生寄”寄件时存在收集未成年人个人信息情况，未征得未成年人或其监护人的明示同意，且提供充分证据证明，得 4 分。 **扣分说明：** 1） 判定结果为符合，-2 分； 2） 未描述隐私政策说明处理未成年的个人信息规则，-2 分； 3） 未描述使用未成年人身份证号进行验证并征得明示同意，-4 分；描述或证据不充分，-2 分； 4） 未描述存在收集未成年人个人信息情况，未征得未成年人或其监护人的明示同意，-4 分；描述或证据不充分，-2 分。	12 分

序号	作业指导书章节号/名称	检测要求	评分说明	分值
7	2.3.4. 个人信息保护政策	a） 应制定个人信息保护政策，内容应包括但不限于： 1） 至 8）	检测结果包括： （1）判定结果为不符合，得 2 分； （2）描述了隐私政策中未包括个人信息控制者联系方式，询问、投诉的渠道和机制，以及外部纠纷解决机构及联络方式，且提供充分证据证明，得 12 分。 **扣分说明：** 1） 判定结果为符合，-2 分； 2） 未描述隐私政策中未包括个人信息控制者联系方式，询问、投诉的渠道和机制，以及外部纠纷解决机构及联络方式，-6 分；部分描述，-2 分。 3） 未提供有关证据，-6 分；提供部分证据，-2 分。	14 分
8		b） 隐私政策应公开发布且易于访问，例如，在网站主页、移动应用程序安装页、本标准附录 C 中的交互界面或设计等显著位置设置链接。	检测结果包括： （1）判定结果为符合，得 2 分； （2）描述了隐私政策公开发布且易于访问，且提供充分证据证明，得 10 分。 **扣分说明：** 1） 判定结果为不符合，-2 分； 2） 未描述隐私政策公开发布且易于访问，-6 分；部分描述，-2 分。 3） 未提供有关证据，-4 分；提供部分证据，-2 分。	12 分
合计				100 分

附录 D 成绩与排名

参加机构代码	笔试成绩	实操成绩	综合成绩（=50%*笔试成绩+50%实操成绩）	综合排名
TUSM31	83 分	74 分	78.5 分	第 1 名
ECJP22	82 分	72 分	77 分	第 2 名
XZRT13	83 分	68 分	75.5 分	第 3 名
BPQS03	74 分	76 分	75 分	第 4 名
BJUA15	78 分	72 分	75 分	第 4 名
VVEZ32	77 分	72 分	74.5 分	第 6 名
JWMW34	84 分	64 分	74 分	第 7 名
YIXS28	85 分	62 分	73.5 分	第 8 名
AYMM23	71 分	74 分	72.5 分	第 9 名
IAMD19	80 分	64 分	72 分	第 10 名
SUNZ26	77 分	66 分	71.5 分	第 11 名
LCXM25	68 分	72 分	70 分	第 12 名
DMLX08	65 分	74 分	69.5 分	第 13 名
YLIM24	70 分	68 分	69 分	第 14 名
RTXK17	71 分	66 分	68.5 分	第 15 名
VYQN12	84 分	52 分	68 分	第 16 名
FEIP21	68 分	68 分	68 分	第 16 名
PAKV33	75 分	61 分	68 分	第 16 名
QFUK04	69 分	62 分	65.5 分	第 19 名
VXQS20	75 分	56 分	65.5 分	第 19 名
DCWT18	73 分	54 分	63.5 分	第 21 名
UGFB07	66 分	60 分	63 分	第 22 名
KQEM09	73 分	52 分	62.5 分	第 23 名
AHQQ05	64 分	60 分	62 分	第 24 名
HEQP27	50 分	68 分	59 分	第 25 名
OXJI30	66 分	50 分	58 分	第 26 名
XTDR06	63 分	52 分	57.5 分	第 27 名
ZXNA02	60 分	54 分	57 分	第 28 名
OCWJ14	54 分	59 分	56.5 分	第 29 名
JHDX29	63 分	44 分	53.5 分	第 30 名
TEIC10	62 分	34 分	48 分	第 31 名
PQHR01	38 分	28 分	33 分	第 32 名