附件6：

2024年网络安全企业填报表填写说明

1. 企业中文名称：请填写贵企业在研究项目评估结果上展现的名称，推荐使用集团名称。
2. 企业性质：请从“国有”、“非国有”两种性质中选一项填写。“国有”包括国有及国有控股企业、国有实际控制企业。具体可参照国务院国有资产监督管理委员会公布的《企业国有资产交易监督管理办法》中第一章第四条。
3. 营业收入：包括企业的主营业务和其他业务收入、境内和境外的收入。不含营业外收入，不含增值税。
4. 网络安全业务收入：企业通过开展网络安全业务实现的收入。网络安全业务涉及的常见产品及服务详见文末分类表。
5. 网络安全业务研发费用：指企业研究开发网络安全领域新产品、新业务、新技术所发生的各项费用，包括新产品设计费、原型系统开发设计、技术图书资料费、研究机构人员工资、研究设备折旧、技术研究有关的其他经费以及委托其他单位进行科研试制的费用。包括当年发生的，计入当期损益的研究阶段的支出，以及已经资本化的开发阶段的支出。
6. 网络安全业务营业利润：以网络安全业务的营业收入为基础，减去相关营业成本、营业税金及附加、销售费用、管理费用、财务费用、资产减值损失，加上公允价值变动收益（减去公允价值变动损失）和投资收益（减去投资损失），计算得到营业利润。
7. 网络安全业务净利润：以网络安全业务利润总额为基础，减去对应所得税费用，计算出净利润（或净亏损）。
8. 纳税总额：企业在我国境内实际缴纳的所有税款合计金额。计算范围包括全部税种。
9. 网络安全业务员工总数：涉及网络安全业务的年度平均从业人数（含合并财务报表合并范围中所有企业的人数之和）。
10. 网络安全业务研发人数：涉及网络安全业务的年度平均主要从事研究和开发活动的从业人员数量（含合并财务报表合并范围中所有企业的研发人员人数之和）。
11. 企业简介：简要介绍企业基本情况，该内容主要用于网络安全企业评估结果向社会发布时，介绍入选企业使用。
12. 各项业务开展情况：企业认为所有可以展现本企业在2023年业务发展情况的信息均可在此填写，此处填写的内容在评选时会予以考虑。
13. 科技创新认可和奖励情况：指在2023年国家级、省部级单位的创新评比中获奖情况，如试点示范等，应包含奖项及发布单位，并提供证明材料，如无相关获奖情况则填写“无”。
14. 社会贡献：展现企业2023年在各个领域中的突出社会贡献，领域包含且不限于在国家级和省部级单位平台进行的漏洞共享、参加的国家级和省部级重保活动以及其他主流价值观宣传、正能量传播、灵活就业、碳中和、乡村振兴、共同富裕、劳动者权益保障、适老化建设、环境保护、社会公益、人才培养（与高校联合搭建实验室，牵头举办国家级、省级赛事等）、行业自律以及参与部委重点工作任务等。介绍材料需标明贡献所属领域。
15. 行业表彰：企业在2023年受到省部级单位的行业表彰情况，应包含奖项名称、发布单位及发布时间。
16. 行政处罚：指行政机关或其他行政主体依法定职权和程序对违反行政法规尚未构成犯罪的相对人给予行政制裁的具体行政行为。
17. 拥有发明专利权（项）：截至2023年底，企业持有的由我国或外国专利主管机关授予的，尚处于在法定保护期限内的**发明专利权**数量。特别注意：本项**只统计**发明专利数量，**不包含**实用新型、外观设计专利数量，**也不包含**版权（如软件著作权）数量。
18. 企业客户数：指在2023年内，与填报企业签订涉及网络安全业务的合同（或处于合同存续期内），并与填报企业正常开展业务的企业客户数。企业用户指在工商注册的企业级单位，**不包含**商户或个人。单位为“个”。
19. 产品、服务评定认证情况：统计由事业单位、社会组织或其他权威专业机构出具的有效期内的网络安全产品或服务评定、认证情况。企业提交材料中应包含且不限于认证时间、认证单位、认证产品、性能功能认证结果等。
20. 产品能力实效：指企业优势产品的实效及竞争力情况。填报时需在文末“安全产品及服务分类表”的“安全产品分类”部分选择3-5项优势产品，提供可量化的产品能力评价指标及本公司产品对应的性能、功能参数。参数需有测评结果等实际证明材料。
21. 网络安全产品及服务名称：企业提供的网络安全主要产品或服务，以及推广的主要业务品牌。填报时按在营业收入的占比由大到小排列。“简介”请简要填写该产品的主要功能、特点等内容。

网络安全产品及服务分类表

|  |  |
| --- | --- |
| **网络安全产品分类** | |
| **细分领域** | **具体产品** |
| **终端安全** | 主机监控与审计  主机/服务器加固  主机检测/入侵防范  终端安全管理  终端检测与响应  恶意代码防护  蜜罐/蜜网  漏洞检测与管理  保密检查  可信计算  其他 |
| **数据安全** | 数据库安全  安全数据库  数据防泄漏  数据备份与恢复  文档安全  数据脱敏  敏感数据发现与监控  数据溯源  大数据保护  数据安全管控平台  数据分类分级  隐私计算  个人信息保护  其他 |
| **应用安全** | Web应用防火墙  下一代防火墙（NGFW）  Web应用扫描与监控  网页防篡改  邮件安全  API安全  业务安全与反欺诈  域名安全  软件成分分析  安全开发流程  源代码安全  静态安全测试  动态/模糊安全测试  交互式安全测试  沙箱  内容安全  支付安全  勒索软件防护  应用软件安全  云原生安全  视频监控安全  其他 |
| **网络安全** | 防火墙  入侵检测与防御  网络隔离与交换系统  防病毒  上网行为管理  网络准入控制  虚拟专用网络  负载均衡  网络接入安全  网络访问控制  网络流量采集与分析  僵木蠕监测  UEBA  抗DDoS  APT高级威胁防护  零信任  SASE  欺骗防御  拟态防御  动态防御  其他 |
| **身份安全与权限管理** | 身份认证  4A系统  堡垒机  IDaaS  身份识别与访问管理  其他 |
| **密码技术及应用** | 加密机  数字证书  数字防伪  加解密  秘钥管理  其他 |
| **其他安全支撑技术** | 安全审计  威胁情报  病毒库/引擎  AI安全  其他 |
| **安全管理系统** | 安全日志与审计（SIEM）  安全运营中心（SOC）  风险评估与管理  安全基线与配置管理  资产扫描与发现  资产测绘  安全编排与自动化响应（SOAR）  合规管理与检查  攻击面管理  其他 |
| **安全监测与分析系统** | 威胁情报分析  安全监测预警和处置  态势感知  攻击溯源与电子取证  网络空间资产测绘  安全检测（系统/平台/工具）  XDR  其他 |
| **网络安全服务分类** | |
| **细分领域** | **具体服务** |
| 安全管理与检测服务 | 风险评估服务  渗透测试服务  应急响应服务  安全托管服务  安全运维服务  安全审计服务  合规检测服务  数据安全治理服务  其他 |
| 安全培训服务 | 安全培训  实战培训  攻防演练  其他 |
| 安全咨询与集成服务 | 安全咨询与规划  安全设计与集成  其他 |
| 其他服务 | 测评与认证  应急响应与重保服务  网络安全保险  其他 |