2024年全国网民网络安全感满意度

行业治理与企业合规

专题调查报告

发起单位：全国135家网络社会组织及相关机构（网安联）

联合发起单位：全国228家网安联志愿服务机构及相关志愿服务团队

牵头单位：北京网络空间安全协会

承办单位：北京关键信息基础设施安全保护中心

国源天顺科技产业集团有限公司

广州华南检验检测中心有限公司

2024年10月

本报告数据来源于2024网民网络安全感满意度调查活动，任何组织和个人引用本报告中的数据和内容须注明来源出处。

组委会欢迎有关研究机构合作，深入挖掘调查数据价值，有需要者请与组委会秘书处联系。

报告查询(总报告及区域、专题、行业报告):网络安全共建网:www.iscn.org.cn“网安联”公众号:

2024年全国网民网络安全感满意度

行业治理与企业合规

专题调查报告

北京关键信息基础设施安全保护中心

国源天顺科技产业集团有限公司

广州华南检验检测中心有限公司

2024 年 10 月

课题组成员

课题组组长：　陆　臻　公安部网络安全等级保护评估中心

课题组副组长：　袁　静　公安部网络安全等级保护评估中心

程晓峰　北京关键信息基础设施安全保护中心

课题组成员：　胡安勇　广州华南检验检测中心

崔　颖　广州华南检验检测中心

梁洁超　国源天顺科技产业集团有限公司

施　念　重庆信息安全测评中心

侯孟伶　国家互联网数据中心产业技术创新战略联盟

目　　录

一、前言

百年变局起风云，万众同心闯难关。2024年是承前启后的一年，既是新中国建国七十五周年，也是互联网进入中国三十周年，更是我国进入新发展阶段关键的一年。在这一年里，以习近平同志为核心的党中央团结带领全党全国各族人民迎难而上，进一步深化改革开放，加大宏观调控力度，着力调整结构，扩大内需，提振信心，取得明显效果。我国经济总体回升向好，以新质生产力为代表的新动能不断推动经济高质量发展，全面建设社会主义现代化国家迈出坚实步伐。与此同时国际局势风云变幻，地域政治冲突加剧，大国博弈日趋激烈，冲突风险加剧。另外人工智能等新科技取得突破性进展，人类社会正面临一场深刻的技术革命。随着新一代智能化浪潮席卷全球，网络空间成为博弈的重要领域。因此，加强网络空间治理，有效地防范网络安全风险，维护网络空间安全，提升全民网络安全素质，已经成为我们必须面对的问题和挑战。

筑牢网络安全屏障，助推网络强国建设，走出一条具有中国特色的用网治网之道是我国网络空间治理的重要课题和任务。提升网络空间治理水平事关国家长治久安，事关经济社会发展和人民群众福祉。开展网民网络安全感满意度调查，旨在进一步贯彻落实习近平总书记有关网络强国的重要思想，增强全体国民的网络安全意识和防范能力，筑牢可信可控的数字安全屏障，不断增强网络空间安全防御能力和治理能力，推动我国网络空间治理水平的提升。

网民网络安全感满意度调查的宗旨就是以人为本，广大网民是网络活动的直接参与者。调查活动直接面向网民大众，通过问卷调查的方式为大家提供表达诉求的渠道，让政府主管部门可以直接倾听广大网民对网络安全治理的感受和了解现存的网络安全治理问题，更好地倾听民声、尊重民意、顺应民心。同时也向广大网民宣传网络安全的相关政策、法规和知识，提升公众网络安全素养，自觉抵制网上不良信息和网络违法行为，共同守护好清朗的网络空间。

维护网络安全是全社会的共同责任，需要营造全社会共筑网络安全防线的浓厚氛围。为充分发挥网络安全社会组织在网络空间建设中的桥梁作用，切实履行网络社会组织的社会责任，全面提升社会组织服务国家及地方政府网络安全建设的能力和水平，促进全国网络安全事业的发展，从2018年开始由全国多家网络安全社会组织联合发起了每年一度的全国网民网络安全感满意度调查活

动。调查活动及其报告引起社会巨大反响，全国各地联动，有力地推动各地网络安全宣传教育和治理措施的落实。

建设网络强国是我国重要发展战略，在新时代推动高质量发展的背景下，开展2024年度全国网民网络安全感满意度调查别具意义。调查活动通过收集人民群众对网络安全治理的意见和建议，为网络空间治理提供方向和依据，既贯彻落实了“网络安全为人民，网络安全靠人民”的重要思想，又深刻体现了网络安全中的“人民性”。本年度调查活动由全国135家网络安全行业协会及相关社会组织联合发起，公安、网信等各级政府网络安全主管部门对活动给予了强有力的指导和支持。同时，业务主管部门也提供了充分的关心和支持，各参与单位和企业、机构等密切配合，为活动的成功举办打下了坚实的基础。

2024年7月，以“网络安全为人民，网络安全靠人民”为活动主题的2024网民网络安全感满意度调查活动正式启动，7月17日开始全国各大网络平台同步开通线上采集通道，正式对外采集数据，至7月26日24时结束。

本次调查活动收回问卷总数为323.9805万份（主问卷+专题问卷），其中公众网民版问卷为272.9930万份，网络从业人员版问卷50.9875万份。经过数据清洗后，有效问卷总数为206.4726万份，其中，公众网民版问卷173.6912万份，网络从业人员版问卷32.7814万份。丰富的数据量为课题研究打下坚实基础。

本报告由课题组基于2024年度网民网络安全感满意度调查活动收集回来的有效问卷数据，经过对调查数据进行整理、统计、初步分析后编写形成。报告力求真实、客观地反映参与调查的网民群体的网络安全感和满意度的感受，揭示网络安全的态势和网民的关注点和痛点，为有关各方进行网络空间安全治理研究和实践提供参考。

本报告主要基于从业人员版A专题问卷——行业治理与企业合规专题的调研结果，关注网络安全等级保护制度、关键信息基础设施安全保护制度、商用密码应用制度的实施情况，网络运营者和网络产品、服务提供者等履行网络安全主体责任的措施落实情况。

A专题问卷面向网络安全从业人员，调查问卷主要就有关行业指导、措施落实、等保实施、测评服务、关保实施、商密应用、合规措施等方面的问题开展调查，多角度了解从业人员的关注、期望、对治理的评价，探讨推进行业治理与企业合规专题工作的策略和建议。

二、“行业治理与企业合规”专题调查结论

根据总体国家安全观，网络安全和数据安全是国家安全的重要组成部分。网络安全等级保护、关键信息基础设施安全保护、商用密码应用安全是国家落实网络空间安全的重要基石和保障。2023年颁布实施的《商用密码管理条例》和2024年新颁布的《网络数据安全管理条例》与之前颁布实施的《网络安全法》、《密码法》、《数据安全法》、《个人信息保护法》和《关键信息基础设施安全保护条例》共同形成了我国“四法三条例”的网络空间安全法律法规体系，也为推进网络空间安全行业治理提供了法律依据。GB/T 39204-2022《关键信息基础设施安全保护要求》也和以GB/T 22239-2019《网络安全等级保护基本要求》为核心的网络安全等级保护2.0系列标准、以GB/T 39786-2021《信息系统密码应用基本要求》为核心的密码应用系列标准一起形成了我国网络空间安全行业治理的标准体系雏形。随着后续网络安全等级保护、关键信息基础设施安全保护、商用密码应用相关标准的陆续颁布实施，我国网络空间安全行业治理体系的可落地性将进一步完善。

2021年国资委发布施行的《中央企业负责人经营业绩考核办法》第四十八条明确指出企业法定代表人及相关负责人因违反国家法律法规和规定，导致发生较大及以上网络安全事件时要进行责任追究处理。2022年国资委发布施行的《中央企业合规管理办法》中明确要求“企业经营管理行为和员工履职行为符合国家法律法规、监管规定、行业准则和国际条约、规则，以及公司章程、相关规章制度等要求”，并要求所有中央企业设立合规委员会和首席合规官来落实企业合规专项工作。以上两份办法不仅在我国中央企业，还在地方国有企业和其他类型企业得到重点关注和引发广泛遵从意愿。GB/T 35770-2022《合规管理体系要求及使用指南》也成为建立我国企业合规管理体系的基础性标准。

在中国共产党第二十次全国代表大会的报告中，习近平总书记指出要“强化国家安全工作协调机制，完善国家安全法治体系、战略体系、政策体系、风险监测预警体系、国家应急管理体系，完善重点领域安全保障体系和重要专项协调指挥体系，强化经济、重大基础设施、金融、网络、数据、生物、资源、核、太空、海洋等安全保障体系建设”。本次A专题问卷调查对摸清当前网络空间安全行业治理工作落实情况发挥重要作用。

本次A专题问卷主要涉及网络安全从业人员对政府部门网络安全监管工作的评价、网络安全等级保护、关键信息基础设施安全保护、商用密码应用等实施情况、企事业单位网络安全合规工作落实情况以及发生网络安全事件后的处理和报警处置情况。

经过统一数据规整，2024年度A专题问卷有效样本数量为74,382 份。经过课题组对调查数据统计、初步分析后，有以下主要发现：

2.1. 网络安全行业监管水平持续上升

经过连续五年的调查，我国网络安全从业人员对于网络安全重要性认识、网络安全监管力度、政府部门网络安全服务成效等主要评价指标的正面评价呈现持续上升的趋势。特别值得一提的是，作为今年新加入的行业主管部门密码应用指导已经有约69%的从业人员所在行业具备密码应用行业指导意见，这一比例与等级保护、关键信息基础设施安全保护的行业指导水平相当。这一数据充分表明，我国网络安全监管部门在整体网络安全状况、网络安全监管力度等方面的工作取得了显著成效，值得肯定和继续发扬。期待我国网络空间安全行业治理工作继续努力，为广大网民创造更加安全、稳定、可靠的网络空间。

2.2. 企业网络安全合规体系仍需完善

随着“四法三条例”的施行，以及《党委（党组）网络安全工作责任制实施指南》的解密和《中央企业合规管理办法》的发布，我国已初步构建了一套较为全面的网络安全合规体系，用以满足企业在网络安全领域的合规需求。此外，随着ISO/IEC27001：2022《信息安全管理体系》的最新修订和GB/T35770-2022《合规管理体系要求及使用指南》的发布，为我国构建具有中国特色的企业网络安全合规管理体系提供了明确的方向。

然而，通过本次调查的结果显示，仍有近80%的受访者所在单位还未遵循已发布施行多年的《数据安全法》、《密码法》和《关键信息基础设施安全保护条例》。对2023年颁布实施的《商用密码管理条例》的遵循程度相比去年仅上升了约1.5个百分点，仅达到16.98%。虽然，网络安全经费落实比例止住了2023年下降的趋势，在部分区段有所回升，但所在单位网络安全管理满意度相比2023年有一定幅度的下降，并有数十位被访者明确提出希望加强企业网络安

全合规体系建设和合规管理水平的建议，可见建立完善企业网络安全合规工作还有很长的路要走。

2.3. 网络安全等级保护制度发挥重要作用

在过去的一年中，我国网络安全领域在网络安全等级保护制度的护航下，保持了稳健的发展态势。据统计，已有约70%的行业制定了网络安全等级保护工作的指导意见，相较于去年，开展等级保护安全建设整改、等级测评和安全自查的单位数量平均增长了5%—10%。值得注意的是，那些尚未了解或实施等级保护的单位比例均显著下降。参与调查的从业人员普遍认为，网络安全等级保护制度在推动我国网络空间安全方面发挥了重要作用。

此外，各单位从业人员对网络安全等级测评工作的满意度也持续上升，达到了78.63%。这一数据表明，等级测评机构在解决过去存在的问题方面取得了显著进步，得到了被测评单位的广泛认可。然而，我们仍需关注当前存在的各类不足问题。根据多年调查对于等级测评工作不满意的首要原因已经连续两年均为“对测评机构人员专业能力的欠缺”。

2.4. 关键信息基础设施安全保护初见成效

2021年国务院正式颁布《关键信息基础设施安全保护条例》。2023年GB/T39204-2022《关键信息基础设施安全保护要求》也开始正式生效。近一年来关键信息基础设施边界确定、安全测评、安全能力指标体系、网络安全应急框架、供应链安全要求等多份国家标准正起草编制征求已经。根据本次调查数据，对于关键信息基础设施安全保护工作的认知度和实施情况有所下降。相较于2023年的42.98%，今年已经实施了关键信息基础设施安全保护工作的调查对象人数比例略有下降至41.09%。不容忽视的是仍有近60%的调查对象对此项工作表示不清楚、不了解或尚未实施，显示出在关键信息基础设施安全保护方面的认知度和落实程度仍需进一步提升。

但值得肯定的是，关键信息基础设施安全保护的两项核心工作——核心岗位人员管理要求和供应链安全管理方面，相比去年均略有上升。而且对于关键信息基础设施保护总体实施情况的满意度也达到了70%以上。说明随着我国关键信息基础设施安全保护工作的深入，依据相关法律法规和国家标准，逐步开展的分析识别、安全防护、检测评估、监测预警、主动防御、事件处置等落地

工作，有效加强了网络安全从业人员对关键信息基础设施安全保护的培训和指导，一定程度提高广大从业人员对关键信息基础设施安全保护工作的认知度和实施能力。

2.5. 商用密码应用工作任重道远

2019年《密码法》的颁布实施，首次在国家法律层面明确了密码应用对于保障网络与信息安全，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益的重要作用。同时也区分了核心密码、普通密码和商用密码的不同适用场景。其中商用密码用于保护不属于国家秘密的信息，公民、法人和其他组织可以依法使用商用密码保护网络与信息安全。2023年的《商用密码管理条例》更进一步明确商用密码的应用场景和管理要求。但是，通过本次调查显示，以上两部法律法规在了解程度仍然处在不足20%的较低水平，远低于《网络安全法》，甚至距离2021年颁布的《关键信息基础设施安全保护条例》也有近5%的差距。

但是值得肯定的是，在密码应用满足安全需求程度、商用密码安全性评估满意度均达到70%，这也说明当前我国密码应用能够满足大部分行业对于网络安全保障的需求，其安全性评估满意度也在一个较高的水平。当然相比网络安全等级保护测评的满意度仍然有10%以上的差距，说明还有进一步提升的空间。同时，通过本次调查也收集到对于密码应用安全性评估工作时间过长、评估人员技术能力不足、过程监督和管理有待加强等不足问题。在密码技术升级改造过程中也普遍存在资金管理不到位、政策支撑不足等问题。共有约35名被调查对象明确提出“推广商用密码技术”“加强密码管理”的建议。因此，商用密码应用推广和管理工作在落地实施过程中有待进一步探索和完善。

三、专题调查结果分析

3.1. 行业监管状况

3.1.1. 行业分布

经过对本次专题调查参与者的行业背景进行分析，我们发现公共通信和信息服务的从业人员在本次调查中占据较大比例，其占比由2023年的19.24%稳步增长至21.08%。与此同时，体育和娱乐行业的参与度也呈现出积极变化,较2023年相比，提升了1.11个百分点。然而，我们也注意到教育行业的参与度有所下降，较2023年相比下降了4.76个百分比。

从柱状对比图中可以直观地看出，2024年专题参与者的行业分布相较于2023年更趋均衡。各行业在网络安全行业治理与企业合规专题上的参与度均有所提升，这表明本次调查的结果具有更广泛的代表性。这一变化不仅反映了各行业对网络安全和企业合规问题的日益关注，也为我们提供了更为全面、深入的调查数据，为相关决策和研究提供了有力支持。

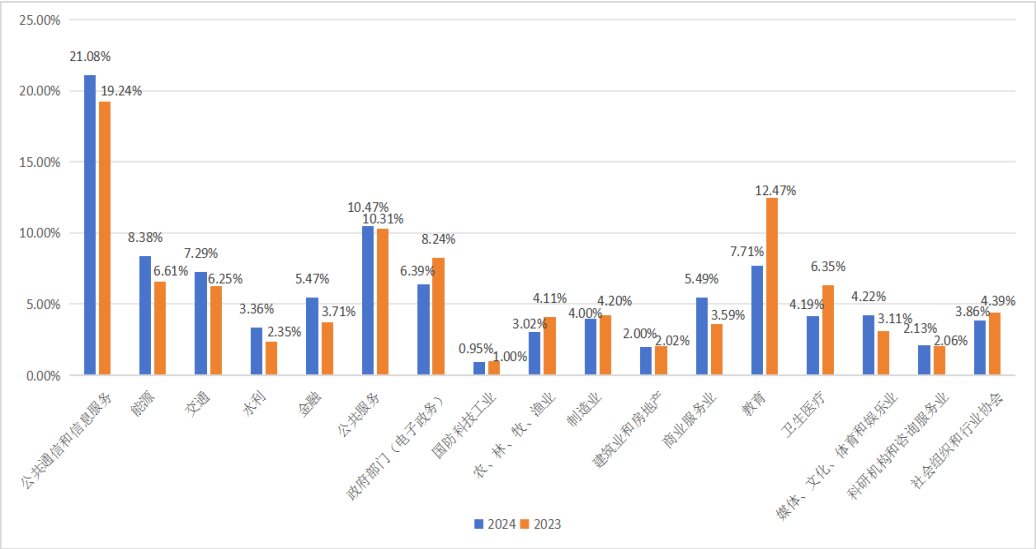

图3-1：调查对象行业分布对比

数据来源：从业人员专题A版问卷行业治理与企业合规专题第1题：您单位所在的行业领域是？

3.1.2. 工作单位性质

经过对本次专题调查参与者的工作单位性质进行分析，结果显示参与调查的从业人员中有51.47%的所在单位属于一般单位（非关键或重保单位），关键信息基础设施运营单位占比达到25.15%，而重要信息系统运营单位（重保单位）

占比为23.38%。从这些数据可以清晰地看出，超过半数的参与者所在单位属于一般单位。

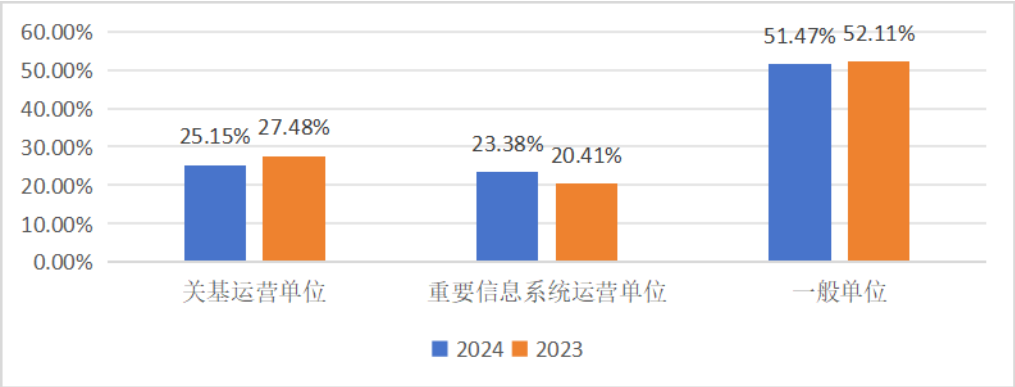

图3-2：调查对象工作单位性质对比

数据来源：从业人员专题A版问卷行业治理与企业合规专题第1.1题：所在单位是否属于以下类型?

3.1.3. 对网络安全重要性认识

经过对参与本次专题调查的从业人员所在单位对网络安全重要性的认识程度进行统计分析，结果显示，有45.81%的从业人员认为网络安全非常重要，29.40%的从业人员认为重要，而认为一般的从业人员占比19.52%。另外，有4.00%和1.27%的从业人员分别表示网络安全不重要和完全不重要。综合这两类从业人员，占比达到5.27%。与2023年相比，无太大变化，这表明网络安全从业人员对网络安全重要性的认识在不断提升。然而，仍有小部分从业人员的网络安全意识有待加强，需要进一步提高他们对网络安全重要性的认识。

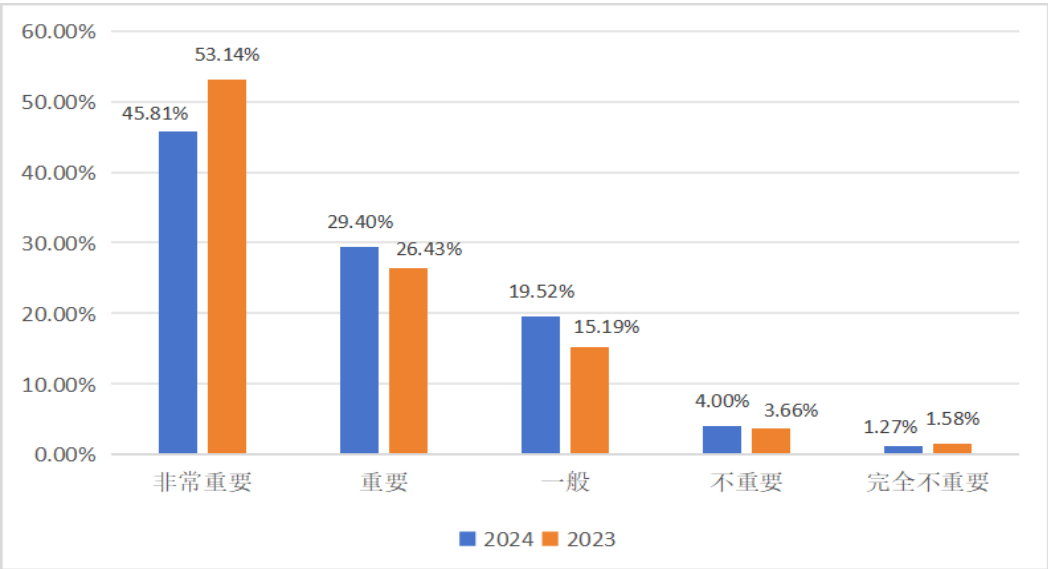

图3-3：对网络安全重要性认识对比

数据来源：从业人员专题A版问卷行业治理与企业合规专题第2题：您认为网络安全对您所在单位来说重要吗？

3.1.4. 行业主管部门对网络安全工作指导

3.1.4.1. 主管部门对等级保护指导

根据本次专题调查的结果，参与调查的从业人员中有33.28%表示其所在单位所在行业已经出台了网络安全等级保护工作的指导意见，但认为这些指导意见较为简单；36.39%的从业人员则表示指导意见明确且细致，相比于2023年增长了4.16%，有14.9%的从业人员表示其所在单位所在行业尚未出台相关指导意见，对比2023年下降9.77%，说明行业治理对比23年有显著效果；经调查有2.47%的人不需要指导。有12.97%的从业人员则表示对此情况不了解，虽比2023年增长3.53%，但本次参与调查的从业人员较去年增加了超过五万人次，这表明此次调查引起了更为广泛的关注和重视。

综合以上数据，我们可以看出，大部分（69.67%）从业人员所在单位所在行业已经制定了网络安全等级保护工作的指导意见，这反映了当前企事业单位对网络安全合规工作的重视。然而，仍有27.86%的从业人员表示其单位所在行业未出台相关指导意见或对此情况不了解，虽比23年下降6.25%，但还需在行业治理的合规之路继续努力。

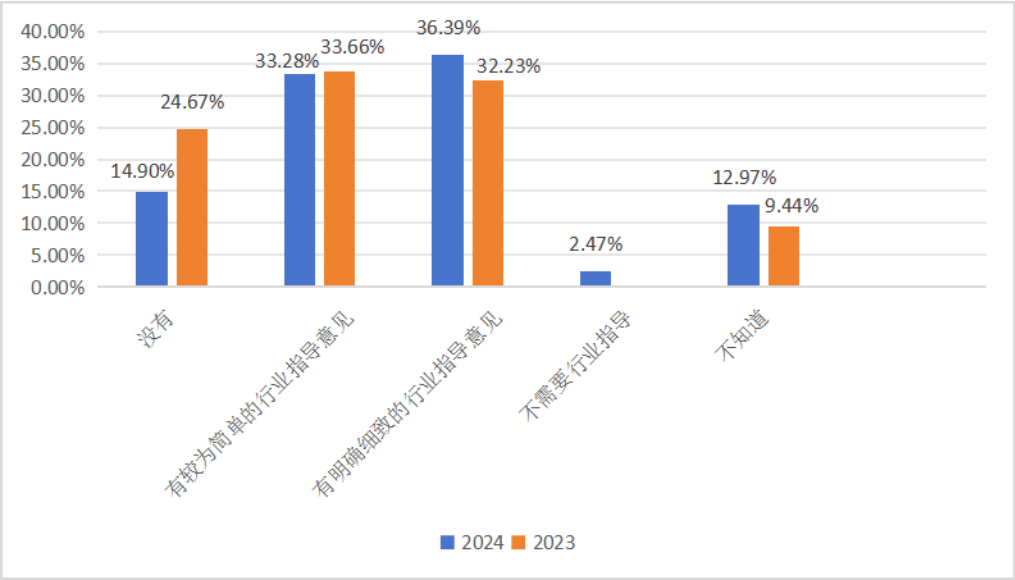

图3-4：主管部门对等级保护指导对比

数据来源：从业人员专题A版问卷行业治理与企业合规专题第3.1题：您单位所在行业是否有明确的推进网络安全方面等级保护、关键信息基础设施保护、密码应用等合规实施的工作指导意见？（等级保护）

3.1.4.2. 主管部门对关键信息基础设施保护指导

根据本次专题调查的结果，参与调查的从业人员中，是关键信息基础设施运营的单位占比达到25.15%。在关键信息基础设施运营的单位的从业人员表示有31.29%的从业人员所在单位所在行业已经出台了关键信息基础设施保护工作的指导意见，但认为这些指导意见较为简单；36.66%的从业人员则表示指导意见明确且细致，并有2.62%的人不需要指导。然而，也有14.60%的从业人员表示其所在单位所在行业尚未出台相关指导意见，而14.83%的从业人员则表示对此情况不了解。

综合以上数据，我们可以看出，大部分（67.95%）从业人员所在单位所在行业已经制定了关键信息基础设施保护工作的指导意见，这反映了当前企事业单位对关键信息基础设施保护工作的重视。然而，仍有32.05%的从业人员表示其单位所在行业未出台相关指导意见或对此情况不了解，这表明在关键信息基础设施保护的工作中还需高度重视。

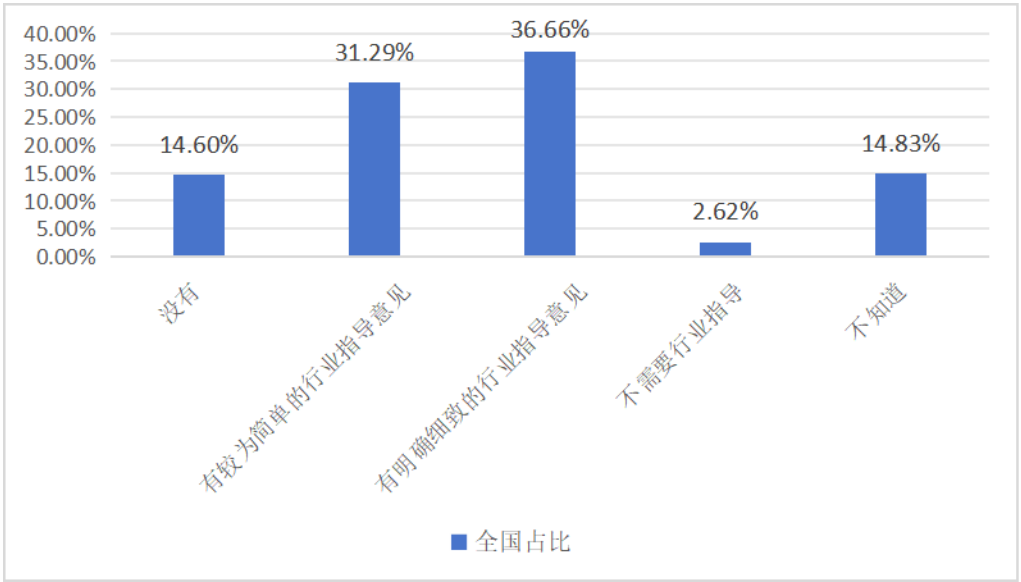

图3-5：主管部门对关键信息基础设施保护指导

数据来源：从业人员专题A版问卷行业治理与企业合规专题第3.2题：您单位所在行业是否有明确的推进网络安全方面等级保护、关键信息基础设施保护、密码应用等合规实施的工作指导意见？（关键信息基础设施保护）

3.1.4.3. 主管部门对密码应用指导

根据本次专题调查的结果，参与调查的从业人员中，有30.27%表示其所在单位所在行业已经出台了密码应用工作的指导意见，但认为这些指导意见较为简单；38.87%的从业人员则表示指导意见明确且细致，并有3.04%的人不需要指导。然而，也有13.53%的从业人员表示其所在单位所在行业尚未出台相关指导意见，而14.29%的从业人员则表示对此情况不了解。

与行业主管部门对等级保护工作指导的调查结果对比，我们可以发现，对密码应用的指导高于对等保的指导，这表明在2024年，密码应用得到了高度重视。在调查中可以看到，大部分（69.14%）从业人员所在单位所在行业已经制定了密码应用工作的指导意见，也有30.86%的从业人员表示其单位所在行业未出台相关指导意见或对此情况不了解，这表明应对密码应用行业的指导还需提升。

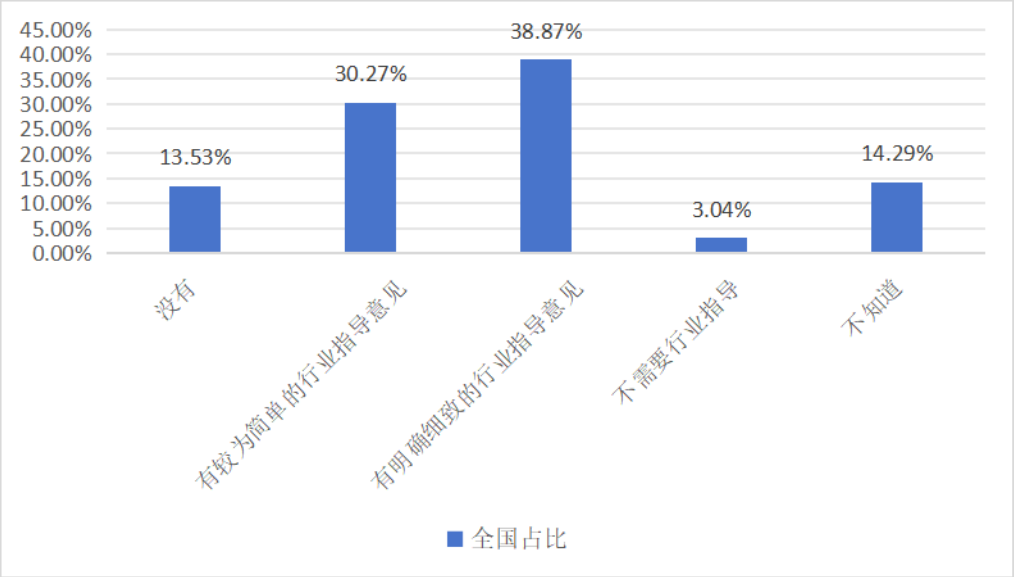

图3-6：主管部门对密码应用指导

数据来源：从业人员专题A版问卷行业治理与企业合规专题第3.3题：您单位所在行业是否有明确的推进网络安全方面等级保护、关键信息基础设施保护、密码应用等合规实施的工作指导意见？（密码应用）

在从业人员版A专题问卷行业治理与企业合规专题第20题：“您对推进等级保护、关键信息基础设施安全保护、商用密码应用以及加强企业合规管理有什么意见和建议？”中，共有28名被调查者提出“加强网络安全监管”类似建议，共有21名被调查者提出“加重对网络安全违法行为的处罚”类似建议，共

有15名被调查者提出“简化监管流程”类似建议，这也说明从业人员对我国网络安全监管和违法行为处罚有更高期望。

3.1.5. 政府部门网络安全服务成效

经过对调查数据的统计分析，我们发现参与调查的从业人员对政府部门提供的网络安全服务的有用性评价前五位依次为：知识普及（占比58.52%）、教育培训（占比45.21%）、信息查询（占比41.09%）、投诉举报（占比27.69%）、监督检查（占比26.86%）。与去年相比，网络安全公共服务的效用评价呈现出升降不一的趋势。具体而言，投诉举报、信息查询、教育培训、知识普及等服务的评价有所下降，而标准制定实施、应急演练、护网行动、技能竞赛、安全通报和风险提示、监督检查、协调处理等服务的评价则呈现出明显的上升趋势。这表明公众对政府网络安全公共服务的需求已经发生了变化，提出了更高的要求。因此，政府部门需要在网络安全公共服务的数量和质量方面做出进一步的改善，以满足公众日益增长的需求。

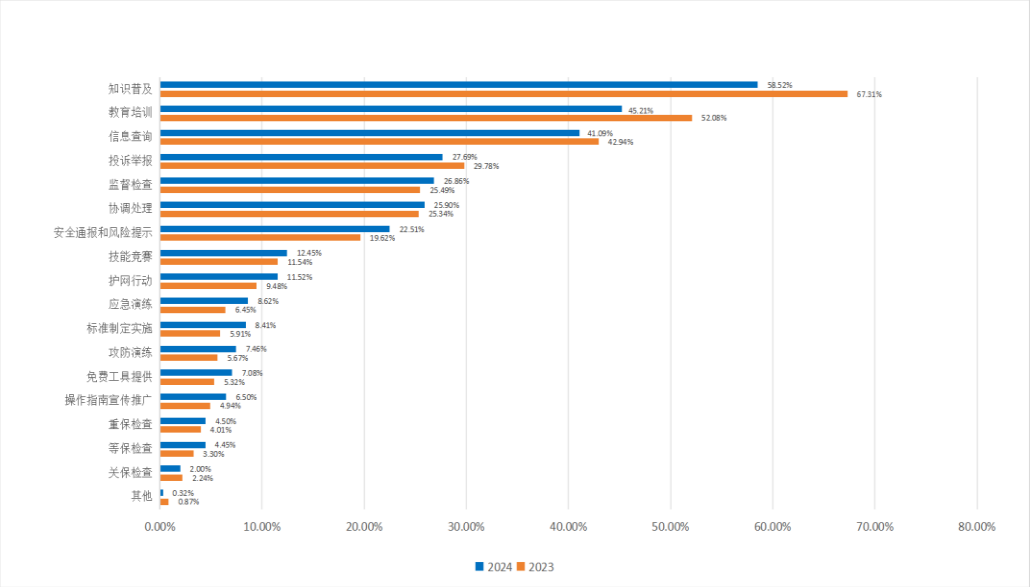

图3-7：政府部门网络安全服务成效对比

数据来源：从业人员版A专题问卷行业治理与企业合规专题第4题：您认为政府部门提供的哪些网络安全服务对行业有较大帮助？

3.2. 企业合规情况

3.2.1. 企业法律法规遵循

对所在单位网络安全法律法规遵循方面，参与调查的从业人员提到前三位分别是《中华人民共和国网络安全法》69.41%，《计算机信息系统安全保护条

例》55.43%，《信息安全等级保护管理办法》52.30%。其中，《密码法》、《关键信息基础设施安全保护条例》、《商用密码管理条例》所占比例较低，分别是20.60%、19.56%、16.98%，但相较于2023年，所占比列却有提升。值得关注的是，相较于2023年，除《中华人民共和国网络安全法》、《反恐怖主义法》提到比列略有下降，其余被提及法律法规所占比列均有提升，其中，对于要遵循的法律法规不够了解的从业人员比例从2023年的6.11%，下降到3.11%。总体遵循情况处于上升态势。

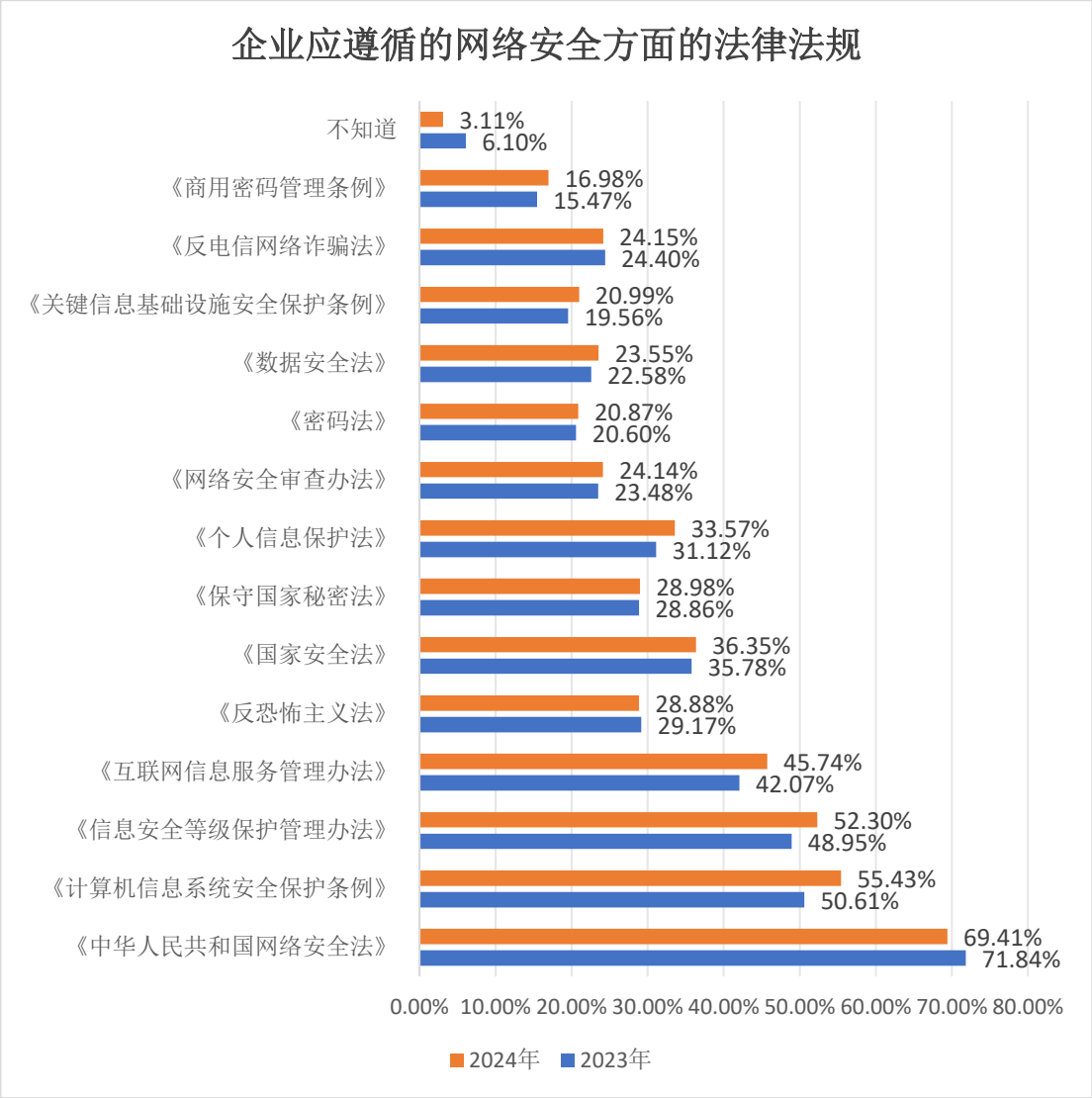

图3-8：企业法律法规遵循对比

数据来源：从业人员版A专题问卷行业治理与企业合规专题第5题：您认为您所在企业在网络安全合规方面应遵循哪些法律法规或者部门规章要求？

在从业人员版A专题问卷行业治理与企业合规专题第20题：“您对推进等级保护、关键信息基础设施安全保护、商用密码应用以及加强企业合规管理有

什么意见和建议？”中，共有35名被调查者提出“建立和完善法律法规”类似建议，共有22名被调查者提出“加强政策宣传和实施”类似建议，这也说明从业人员对我国网络安全法律法规完善程度和宣传实施有更高期望。

3.2.2. 网络安全管理机制完善程度

3.2.2.1. 网络安全保护部门或领导小组设立

关于所在单位是否设立了网络安全保护部门、是否设立了领导小组的问题，调查显示，有66.55%的从业人员表示已经设立保护部门，65.30%表示设立了领导小组，相较于2023年数据，所占比例略有下降。有9.28%表示没有设立安全保护部门，10.91%表示没有设立领导小组，相较于2023年，所占比列大幅下降。有24.16%表示不清楚是否设立安全保护部门，23.80%表示不清楚时候设立领导小组，相较于2023年，所占比列大幅提升。总体设立情况在比列上略有下降。

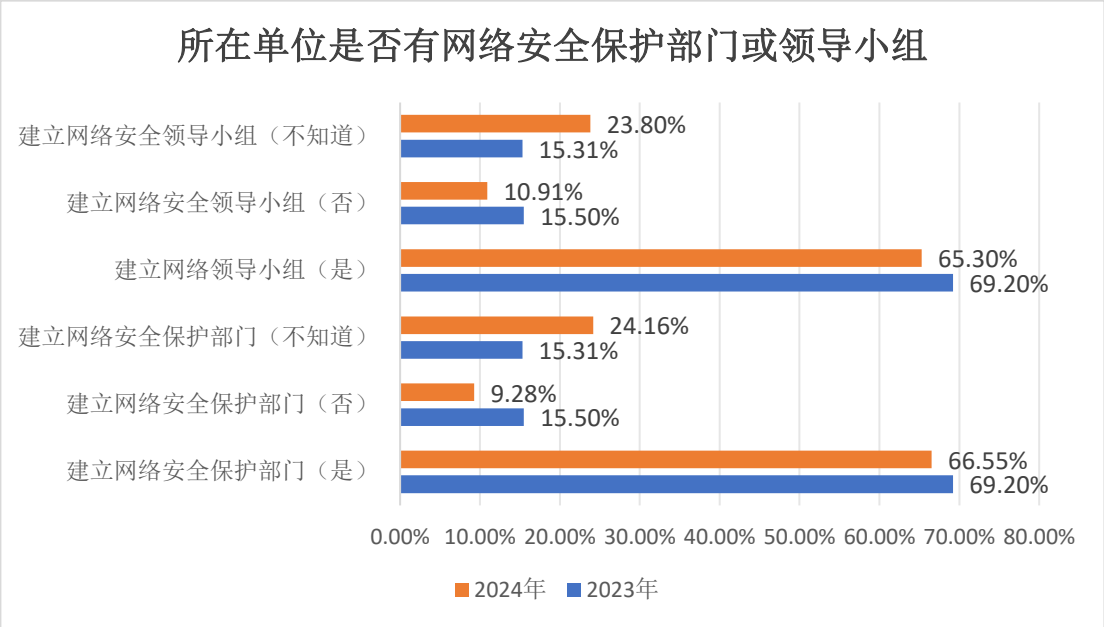

图3-9：网络安全保护部门或领导小组设立对比

数据来源：从业人员版A专题问卷行业治理与企业合规专题第6.1、6.2题：是否设立网络安全保护部门或领导小组？

3.2.2.2. 明确网络安全责任人

对于所在单位是否明确网络安全责任人，调查显示67.64%的从业人员表示所在单位已明确网络安全负责人，与去年相比，数据大概持平。9.23%的人员表示没有明确网络安全负责人，相较于去年，另外有23.14%的人员表示不清楚情况，相较于2023年，表示没有明确网络安全负责人和不清楚情况的两者总体持平。

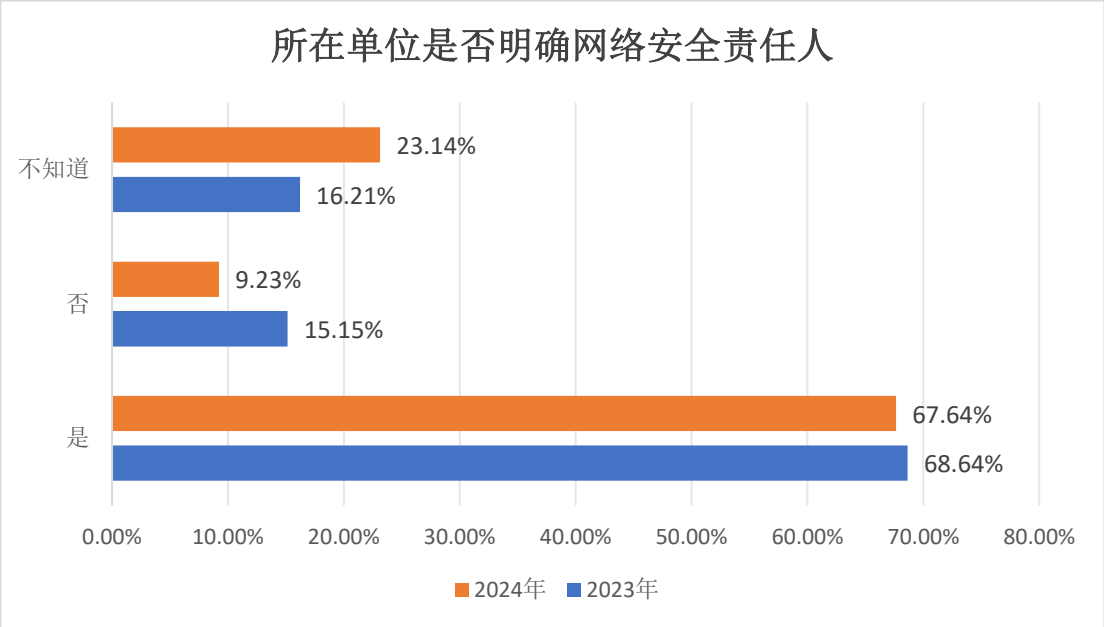

图3-10：网络安全保护部门设置对比

数据来源：从业人员版A专题问卷行业治理与企业合规专题第6.3题：是否明确网络安全责任人？

3.2.2.3. 网络安全责任追究措施

对于所在单位网络安全责任追究措施的建立情况，调查显示66.55%的从业人员表示所在单位已建立网络安全责任追究措施，9.64%的人员表示未建立相关措施，另有23.81%的人员对此表示不清楚。

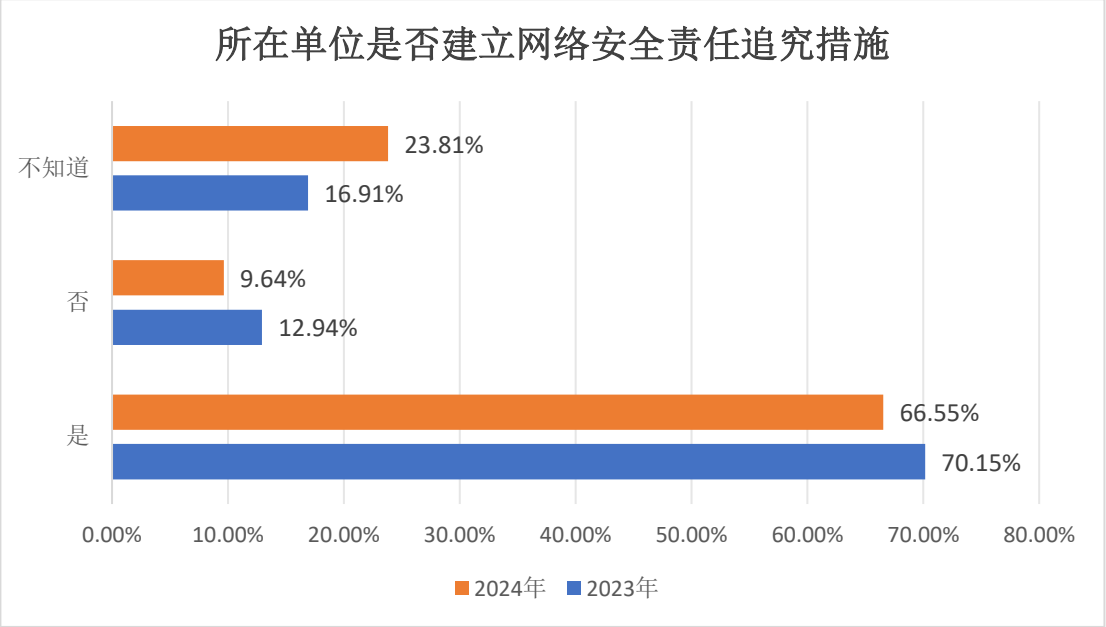

图3-11：网络安全责任追究措施对比

数据来源：从业人员版A专题问卷行业治理与企业合规专题第6.4题：是否建立网络安全责任追究措施？

3.2.2.4. 定期进行安全检查

对于所在单位是否定期进行安全检查情况，调查显示有69.26%的从业人员确认所在单位进行了定期检查，8.30%的人员表示所在单位没有定期检查，22.45%的人员表示对此情况不了解。相较于去年，总体定期检查比列略有下降。

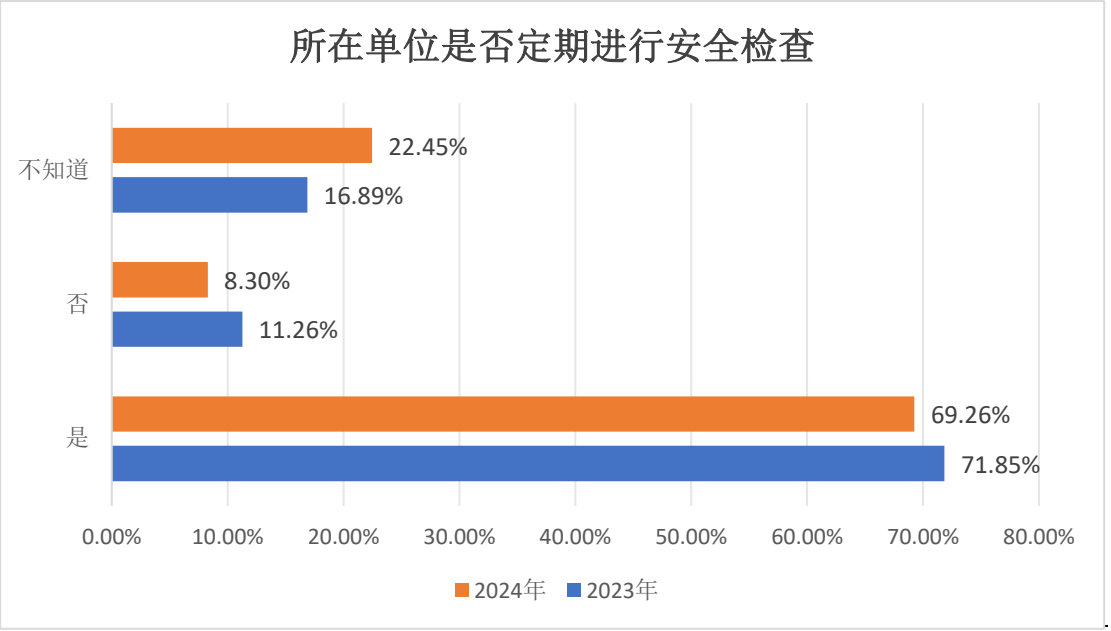

图3-12：定期进行安全检查对比

数据来源：从业人员版A专题问卷行业治理与企业合规专题第6题第5小题：是否定期进行安全检查？

在从业人员版A专题问卷行业治理与企业合规专题第20题：“您对推进等级保护、关键信息基础设施安全保护、商用密码应用以及加强企业合规管理有什么意见和建议？”中，共有21名被调查者提出“严格执行安全制度”类似建议，共有17名被调查者提出“明确责任分配”类似建议，共有15名被调查者提出“简化申报流程”类似建议，这也说明从业人员对企业网络安全制度执行与责任落实有更高期望。

3.2.3. 网络安全经费落实

对于网络安全经费落实情况，调查显示有18.39%的从业人员表示该占比处于1-4%的区间内，18.43%的从业人员认为该占比在5-9%之间，14.27%的从业人员认为该占比在10-15%之间，这三组数据相较于去年，已有显著提升。其中，7.67%的从业人员表示单位在信息化建设过程中没有为网络安全设置预算经费，30.74%人员则表示对此情况并不清楚，这两组数据相较于去年，已大幅下降。总体网络安全相关经费落实情况呈现良好态势。

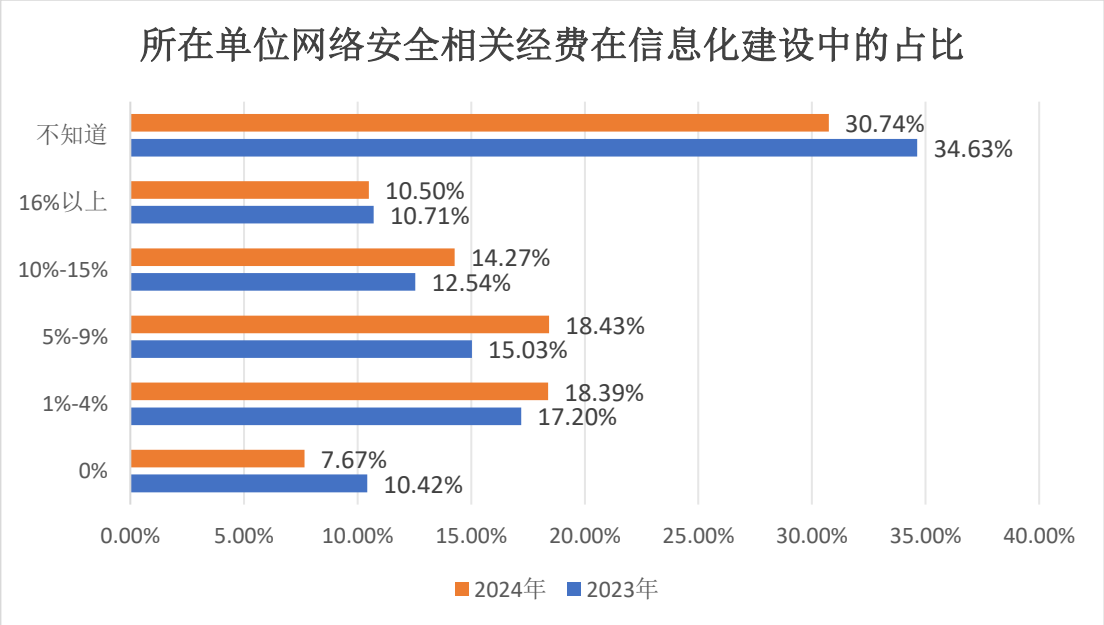

图3-13：网络安全经费落实对比

数据来源：从业人员版A专题问卷行业治理与企业合规专题第7题：您所在单位的网络安全相关的经费预算在信息化建设中的占比是？

3.2.4. 网络安全管理状况

对于所在单位网络安全管理状况的满意度情况，调查显示表示非常满意的比列为29.81%，相较于去年，显著下降。表示满意的人数为34.69%，与去年相比，略有上升。对所在单位网络安全管理状况一般满意、不满意和非常不满意的比列分别为21.47%、3.98%、1.60%，基本与去年数据持平。另外，对网络安全管理状况不太清楚的比列为8.44%，与2023年相比，明显提升。

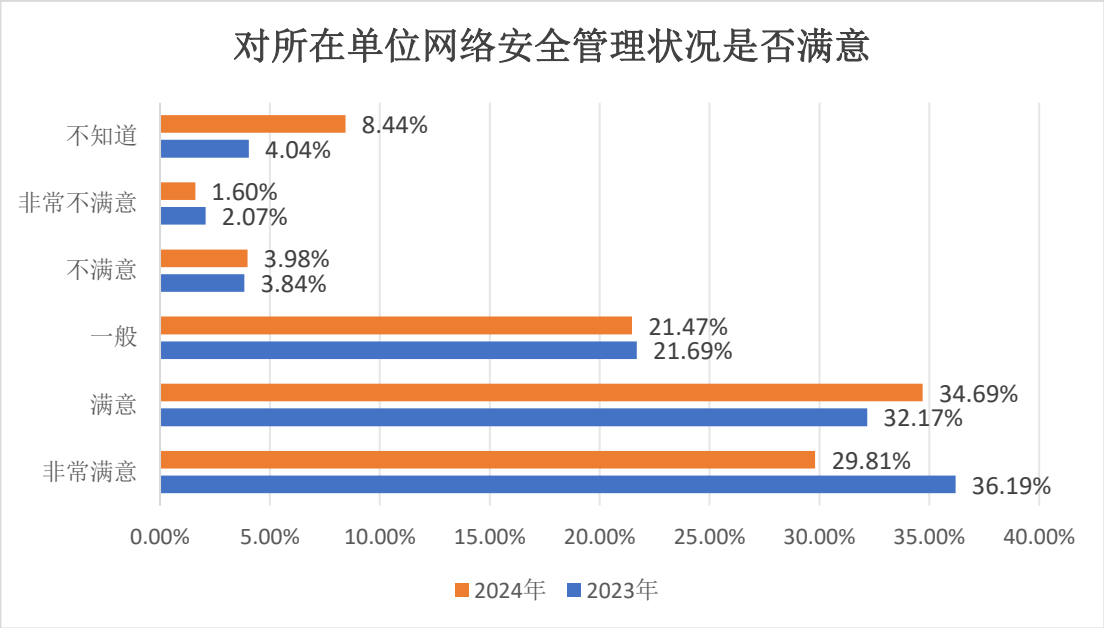

图3-14：网络安全管理状况对比

数据来源：从业人员版A专题问卷行业治理与企业合规专题第8题：您对所在单位的网络安全管理状况是否满意？

3.2.5. 网络安全管理需改善方面

对于所在单位网络安全管理在哪些方面需要改善的问题，调查显示占比最高的前三位分别是：检测预警33.83%、规章制度33.28%、贯彻落实32.67%，与2023年数据相比，前三位数据顺序一致，各占比有所下降。较少提到的三位分别是：全员安全意识15.52%、供应链安全12.55%，攻防演练12.28%。

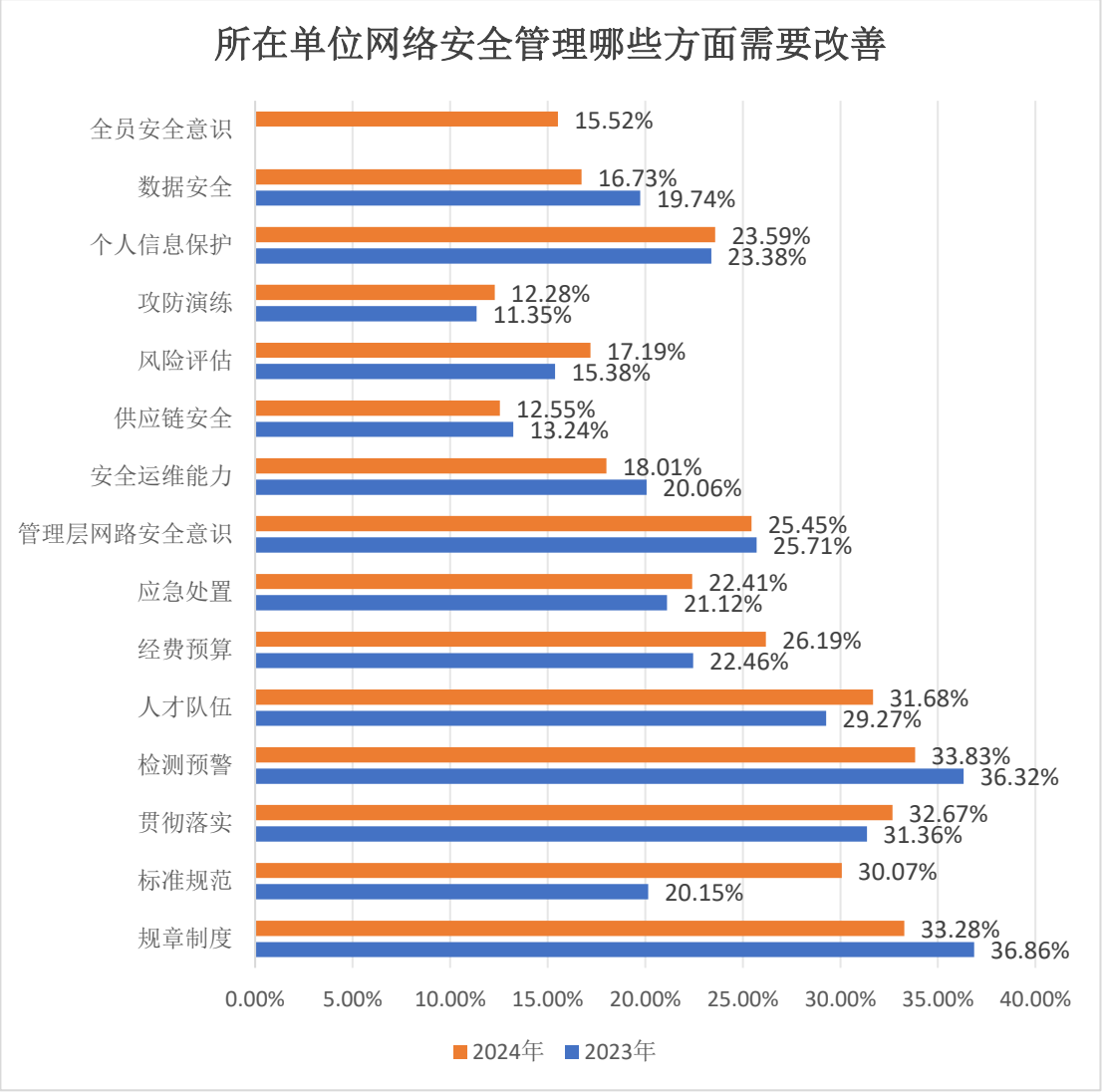

图3-15：网络安全管理需改善方面对比

数据来源：从业人员版A专题问卷行业治理与企业合规专题第8.1题：您认为单位的网络安全管理在哪些方面需要改善？

在从业人员版A专题问卷行业治理与企业合规专题第20题：“您对推进等级保护、关键信息基础设施安全保护、商用密码应用以及加强企业合规管理有什么意见和建议？”中，共有24名被调查者提出“加强企业网络安全合规体系建设”类似建议，共有19名被调查者提出“提高企业网络安全合规管理水平”类似建议，这也说明从业人员对企业网络安全合规管理工作有更高期望。

3.3. 网络安全等级保护落实

3.3.1. 网络安全合规工作

3.3.1.1. 网络安全等级保护工作参与情况

根据本次专题调查的结果，，21.97%的受访者担任主持主管角色，20.49%为主要参与人员，29.74%为一般参与人员，而27.80%的受访者表示没有参与等级保护工作。

主持主管与主要参与人员的总和（42.46%）显示了在等级保护工作中，有超过四成的从业人员处于核心岗位，负责决策、规划和关键任务的执行。

一般参与人员（29.74%）表明在等级保护工作中，有相当一部分从业人员承担着基础性工作，这可能包括日常的安全监控、数据备份、安全策略执行等任务。

未参与者的比例（27.80%）相对较高，这可能意味着在部分单位中，等级保护工作尚未普及到所有相关从业人员，或者部分人员对自身参与等级保护工作的认知不足。

这些数据不仅揭示了等级保护工作在不同层级和角色中的分布情况，而且反映出在网络安全领域，等级保护的实施和参与程度存在一定差异。高比例的一般参与人员显示了基础性工作的重要性，而主持主管与主要参与人员的总和超过四成，突显了核心岗位在等级保护中的关键作用。未参与者的比例相对较高，这可能指向等级保护工作在普及和认知方面存在提升空间。这些发现对于加强网络安全从业人员的培训、明确职责分工，以及加强核心团队建设具有重要的指导意义。

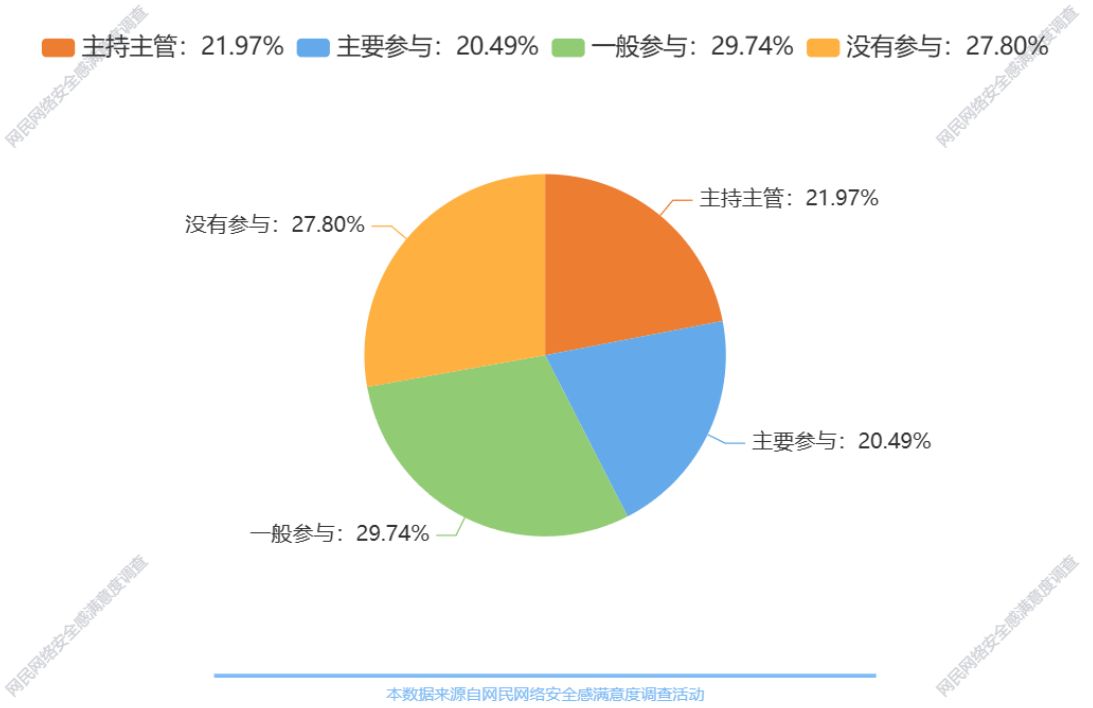

图3-16：等级保护工作参与情况

数据来源：从业人员版A专题问卷行业治理与企业合规专题第9.1题：您是否参与所在单位等级保护、关键信息系统安全保护、商用密码应用等合规工作？（等级保护）

3.3.1.2. 关键信息基础设施安全保护工作参与情况

根据本次专题调查的结果，有20.66%的受访者表示自己在关键信息基础设施安全保护工作中担任主持主管的角色，这一比例反映了管理层在该领域的重要作用；主要参与人员占比为20.78%，这部分从业人员在实施和执行安全措施方面发挥着核心作用；一般参与人员以30.21%的比例成为最大的群体，这表明在日常的安全保护工作中，有相当一部分人员参与其中；未参与人员的比例为28.35%，这一数据提示我们，在关键信息基础设施的安全保护方面，仍有相当一部分从业人员未能参与其中。

这些数据揭示了关键信息基础设施安全保护工作的参与度分布情况。高比例的一般参与人员显示了基础性工作的重要性，而主持主管与主要参与人员的总和超过四成，突显了核心岗位在安全保护中的关键作用。未参与者的比例相对较高，这可能指向安全保护工作在普及和认知方面存在提升空间。

为了提高关键信息基础设施的安全保护水平，建议各单位加强对从业人员的培训和宣传，以提升全体从业人员的安全意识和参与度。同时，建议进一步

明确各角色的职责和任务，确保安全保护工作的有效执行。对于主持主管和主要参与人员，建议加强核心团队建设，提升其专业能力和应急响应能力，以强化关键信息基础设施的安全防护。这些措施将有助于构建更加完善的安全保护体系，确保关键信息基础设施的安全性和稳定性。

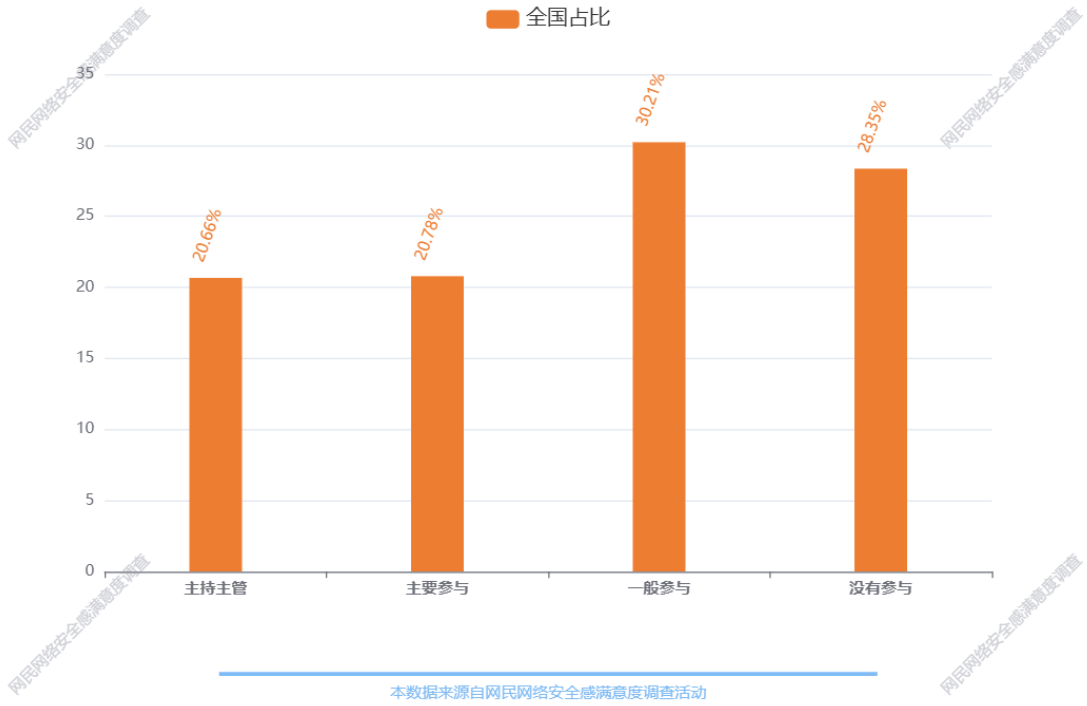

图3-17：关键信息基础设施安全保护工作参与情况

数据来源：从业人员版A专题问卷行业治理与企业合规专题第9.2题：您是否参与所在单位等级保护、关键信息系统安全保护、商用密码应用等合规工作？（关键信息基础设施安全保护）

3.3.1.3. 商用密码应用工作参与情况

根据本次专题调查的结果，20.64%的受访者担任主持主管角色，负责相关工作的领导与管理；19.65%的受访者作为主要参与人员，直接参与核心任务的执行；29.27%的受访者处于一般参与层级，执行日常的操作与执行工作；而30.45%的受访者表示并未参与商用密码应用合规工作，这一比例显示了在商用密码应用合规领域仍有较大的提升和动员空间。

调查结果显示，商用密码应用合规工作的参与度分布呈现出一定的层级性。一般参与人员的比例最高，这可能反映了在商用密码应用合规工作中，日常操作和执行层面的工作量较大。同时，主持主管和主要参与人员的总和接近四成，

这表明在商用密码应用合规工作中，有一定比例的从业人员处于关键岗位，负责重要的规划和执行工作。

未参与者的比例较高，这可能意味着在部分单位中，商用密码应用合规工作尚未得到足够的重视，或者部分从业人员对自身在该领域的职责认识不足。为了提高商用密码应用的合规性，建议各单位加强对从业人员的培训，提升他们对商用密码应用合规重要性的认识。同时，建议明确各角色的职责和任务，确保商用密码应用合规工作的有效执行。对于主持主管和主要参与人员，建议加强专业能力建设，提升其在商用密码应用合规工作中的领导力和执行力。通过这些措施，可以进一步提升商用密码应用的合规水平，保障网络与信息安全。

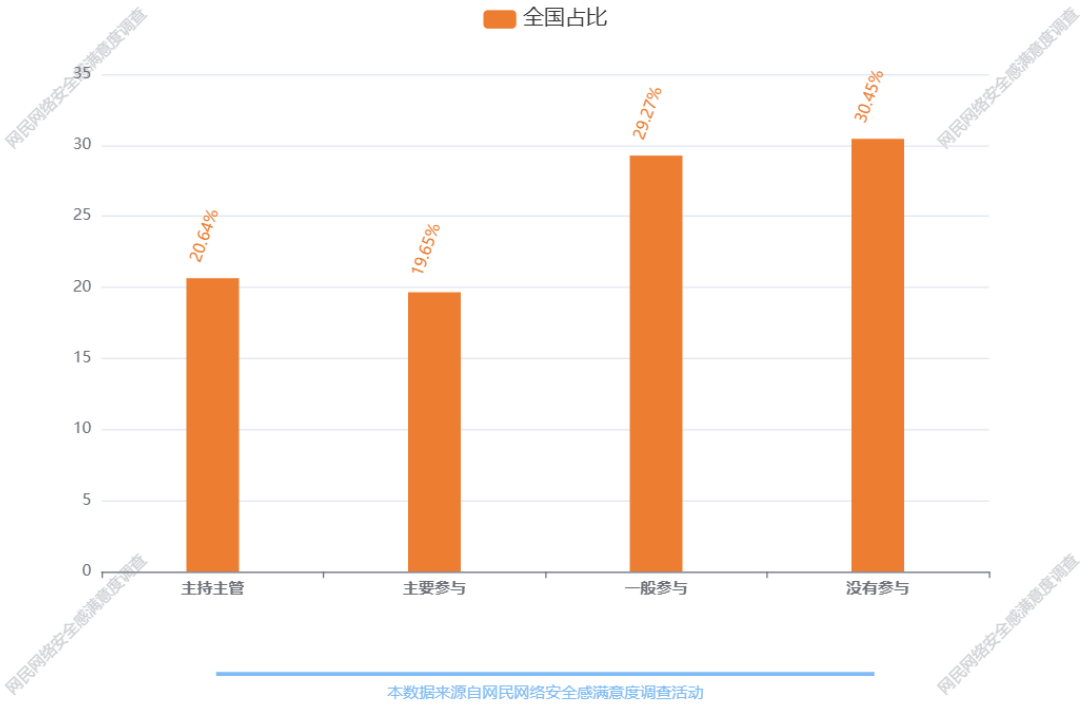

图3-18：商用密码应用工作参与情况

数据来源：从业人员版A专题问卷行业治理与企业合规专题第9.3题：您是否参与所在单位等级保护、关键信息系统安全保护、商用密码应用等合规工作？（商用密码应用）

3.3.2. 网络安全等级保护满意度

根据本次专题调查的结果，34.51%的受访者表示“非常满意”，而35.67%的受访者选择“比较满意”，两者合计占比超过70%，显示出对网络安全等级保护工作的普遍认可。同时，有25.63%的受访者认为实施情况“一般”，表明

对现状有一定的保留意见。在不满意度方面，仅有2.67%的受访者表示“比较不满意”，而“非常不满意”的比例为1.52%。

综合来看，超过70%的受访者对网络安全等级保护的总体实施情况表示满意（“非常满意”和“比较满意”的总和），这表明网络安全等级保护工作得到了行业内部的广泛认可。然而，也有一小部分受访者表达了不满（“比较不满意”和“非常不满意”的总和），这提示我们网络安全等级保护工作仍有改进空间。对于这些不满的声音，相关部门应予以关注，并作为进一步提升工作质量的参考。总体而言，调查结果显示网络安全等级保护工作取得了积极成效，但仍需持续优化以满足所有从业人员的期望。

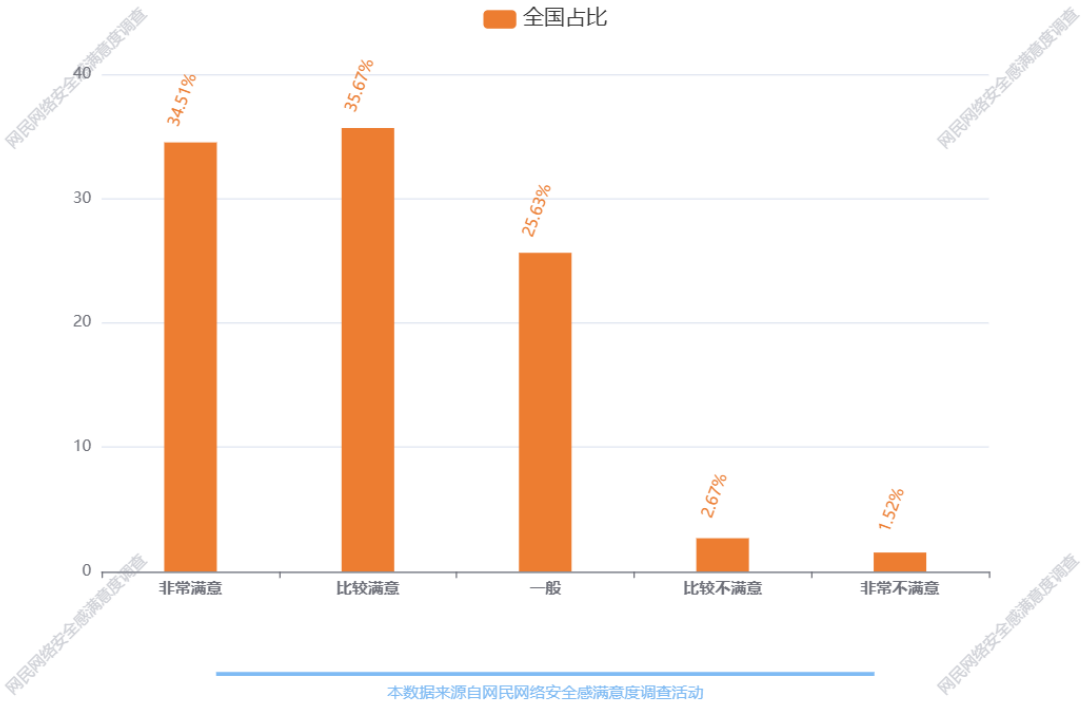

图3-19：网络安全等级保护满意度

数据来源：从业人员版A专题问卷行业治理与企业合规专题第10题：您对目前网络安全等级保护总体实施情况满意吗？

在从业人员版A专题问卷行业治理与企业合规专题第20题：“您对推进等级保护、关键信息基础设施安全保护、商用密码应用以及加强企业合规管理有什么意见和建议？”中，共有19名被调查者提出“明确等级保护流程和标准”类似建议，共有16名被调查者提出“强化等级保护的实施和监督”类似建议，共有26名被调查者提出“加强基础设施保护”类似建议，共有33名被调查者提

出“提高网络安全防护措施”类似建议，这也说明从业人员对网络安全等级保护有更高期望。

3.3.3. 网络安全等级保护工作开展情况

根据本次专题调查的结果，其所在单位是否进行过特定网络安全等级保护工作情况：

定级备案：有32,201名受访者表示其所在单位已经进行了定级备案工作，占比达到43.29%。这显示了相当一部分单位对网络安全等级保护的初步步骤给予了足够的重视，并已按照规定完成了相关的备案流程。

安全建设整改：安全建设整改方面的数据略低于定级备案，有31,935名受访者确认单位进行了此项工作，占比42.93%。这一比例表明，大多数单位在网络安全建设方面采取了积极的整改措施，以提升安全防护能力。

安全测评：在安全测评方面，有30,442名受访者表示其所在单位已经进行了安全测评，占比为40.93%。这表明有很大一部分单位重视通过专业的安全测评来识别和解决潜在的安全问题。

网络安全自查：网络安全自查的执行情况相对较低，有29,099名受访者表示单位进行了自查，占比39.12%。这可能意味着在网络安全自查方面，还有提升的空间，需要进一步强化单位的自我监督和检查机制。

不了解与未进行：有12,310名受访者表示对所在单位是否进行过网络安全等级保护工作“不了解”，占比16.55%；而有4,465名受访者明确表示单位“没有进行过”任何网络安全等级保护工作，占比6.00%。这两个比例的存在提示我们，在网络安全等级保护的普及和执行方面，仍存在一定的盲区和不足。

调查结果显示，大部分单位已经开展了网络安全等级保护的相关工作，尤其是在定级备案和安全建设整改方面。然而，也有一部分单位在网络安全自查和整体等级保护措施的执行上存在不足，还有少数单位未进行过任何相关工作。这些发现为网络安全等级保护工作的进一步优化和加强提供了重要的数据支持和改进方向。

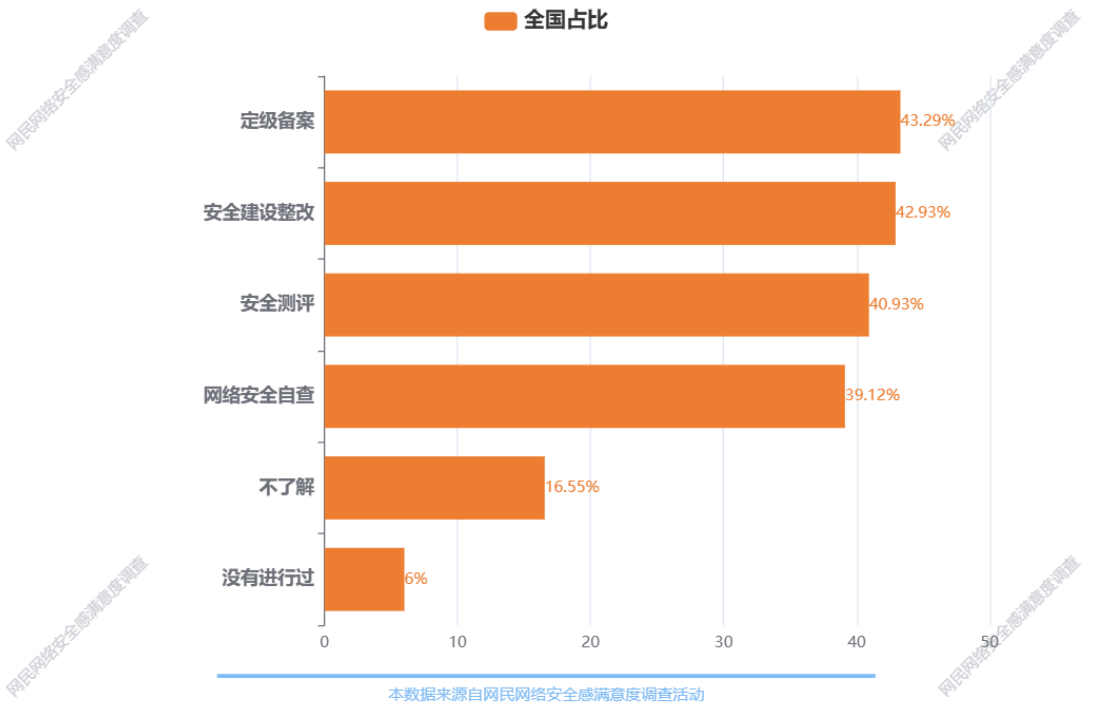

图3-20：网络安全等级保护工作开展情况

数据来源：从业人员版A专题问卷行业治理与企业合规专题第11题：您所在单位是否进行过以下网络安全等级保护工作？

3.3.4. 网络安全等级测评满意度

根据本次专题调查的结果，绝大多数受访者对测评机构的工作表示满意。具体来说，35.76%的受访者表示“非常满意”，而42.87%的受访者表示“满意”，两者合计占比接近80%，这一数据强有力地表明了测评机构在执行网络安全等级保护测评工作中获得了广泛的积极反馈。

然而，也有部分受访者对测评工作持有中立或负面的看法。其中，19.07%的受访者认为测评工作表现“一般”，这可能意味着这些受访者对测评机构的工作有一定的保留，或认为存在改进的空间。此外，1.86%的受访者表示“不满意”，而0.44%的受访者表示“非常不满意”，这些比例相对较低，但仍然值得关注，因为它们可能指向测评服务中的特定问题或不足之处。

总体而言，调查结果揭示了测评机构在网络安全等级保护测评工作中的总体满意度较高，但也指出了进一步提升服务质量和客户满意度的潜在机会。对于测评机构而言，这些反馈是宝贵的资源，可以帮助它们识别服务中的优势和弱点，从而不断改进和优化工作流程，以满足行业日益增长的安全需求。

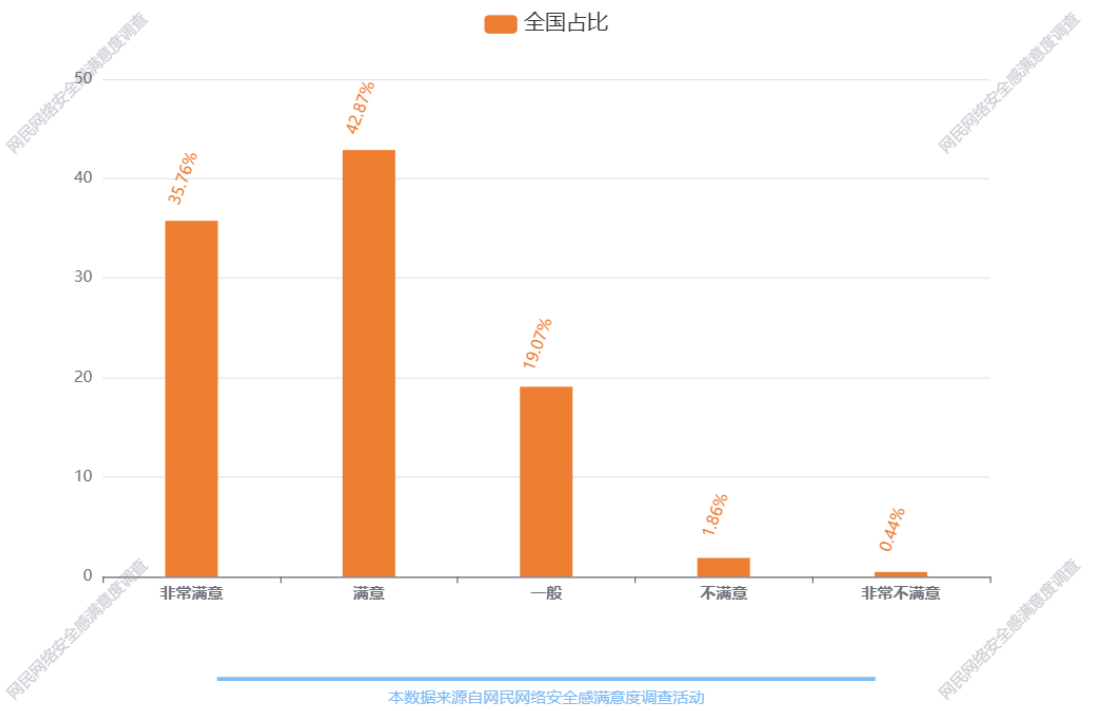

图3-21：网络安全等级测评满意度

数据来源：从业人员版A专题问卷行业治理与企业合规专题第11.1题：您对测评机构进行测评工作的满意度评价如何？

在对等级保护工作的满意度调研中，我们深入探究了受访者不满意的具体原因，以期为测评机构提供改进的方向。

调研结果显示：受访者普遍关注的首要问题为测评机构的专业能力欠缺，占比高达50.22%。这表明，超过半数的受访者认为测评机构在专业知识和技能方面存在不足，这可能直接影响了测评结果的准确性和可靠性，从而削弱了受访者对测评工作的信任。

其次，过程复杂和效率低下是受访者不满的另一个重要原因，占比46.93%。这一反馈揭示了当前测评流程可能存在的冗长和低效问题，受访者期望测评工作能够更加高效，减少不必要的复杂性，以适应快速变化的网络安全环境。

整改措施的不切实际也是受访者普遍关注的问题，占比43.40%。这表明，测评后提出的整改建议可能与受访者的实际业务环境和能力不匹配，导致整改难以落地执行。这一问题的存在，不仅影响了测评工作的实际效果，也可能导致受访者对测评结果的实用性产生怀疑。

时间周期长、服务态度差和收费不合理也是受访者不满意的原因之一，分别占比29.65%、25.61%和18.14%。这些反馈指出了测评机构在服务周期管理、

客户服务态度和费用透明度方面的不足，这些因素都可能影响受访者的总体满意度。

最后，有极少数受访者选择了“其他”选项，这0.47%的比例代表了一些未被充分关注或理解的具体问题。

综上所述，这些调研结果为测评机构提供了深刻的洞察，指出了在提升专业能力、优化流程效率、确保整改措施的实用性、缩短服务周期、改善服务态度和提高收费透明度等方面需要改进的关键领域。测评机构应认真对待这些反馈，采取切实措施进行改进，以提升服务质量，增强客户信任，从而提高网络安全等级保护工作的整体效能。

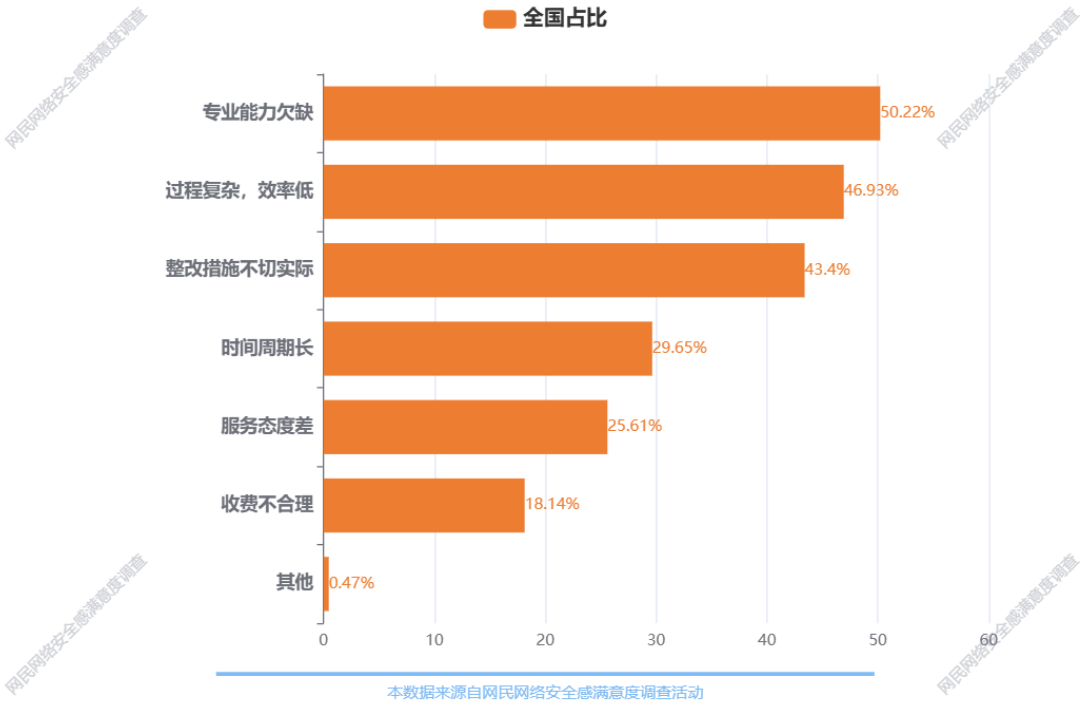

图3-22：对网络安全等级测评不满意原因

数据来源：从业人员版A专题问卷行业治理与企业合规专题第11.2题：您不满意的原因是？

在从业人员版A专题问卷行业治理与企业合规专题第20题：“您对推进等级保护、关键信息基础设施安全保护、商用密码应用以及加强企业合规管理有什么意见和建议？”中，共有14名被调查者提出“提高测评机构的专业能力”类似建议，共有13名被调查者提出“加强定期的安全评估和审计”类似建议，这也说明从业人员对网络安全等级测评工作有更高期望。

3.3.5. 发生网络安全事件情况

根据本次专题调查的结果，有13,975名受访者表示其所在单位“发生过”网络安全事件，占比18.79%。这一比例虽然相对较低，但仍然揭示了一定数量的单位曾遭受过网络安全威胁。另一方面，有36,492名受访者表示“没发生过”网络安全事件，占比高达49.06%，这可能表明这些单位在网络安全防护方面做得相对到位，或者网络安全事件并未被及时发现和报告。最后，有23,913名受访者表示“不清楚”单位是否发生过网络安全事件，占比32.15%，这一较高比例可能反映了部分单位在网络安全意识和事件监控方面的不足。

综合上述统计数据，我们可以得出一些初步结论。首先，接近一半的受访者表示没有发生过网络安全事件，这可能意味着这些单位在网络安全防护措施上投入了较多的资源和努力，或者他们的安全防护措施相对有效。然而，也有近五分之一的单位报告称发生过网络安全事件，这一比例虽然不高，但也不容忽视，它提醒我们网络安全威胁是现实存在的，需要持续关注和应对。

更值得关注的是，超过三分之一的受访者对单位是否发生过网络安全事件表示“不清楚”。这一结果可能暗示了在网络安全意识、事件报告机制和监控系统方面存在的不足。这不仅可能导致安全事件的漏报和延误响应，还可能掩盖实际的安全风险，从而对单位的信息安全构成潜在威胁。

总体而言，这些调研结果强调了加强网络安全防护、提高网络安全意识和建立有效的网络安全事件监测和响应机制的重要性。对于发生过网络安全事件的单位，需要进一步分析事件原因，加强安全防护措施；对于表示不清楚的单位，则需要提高网络安全意识，建立和完善网络安全事件的监测和报告机制，以确保能够及时发现和应对网络安全威胁。

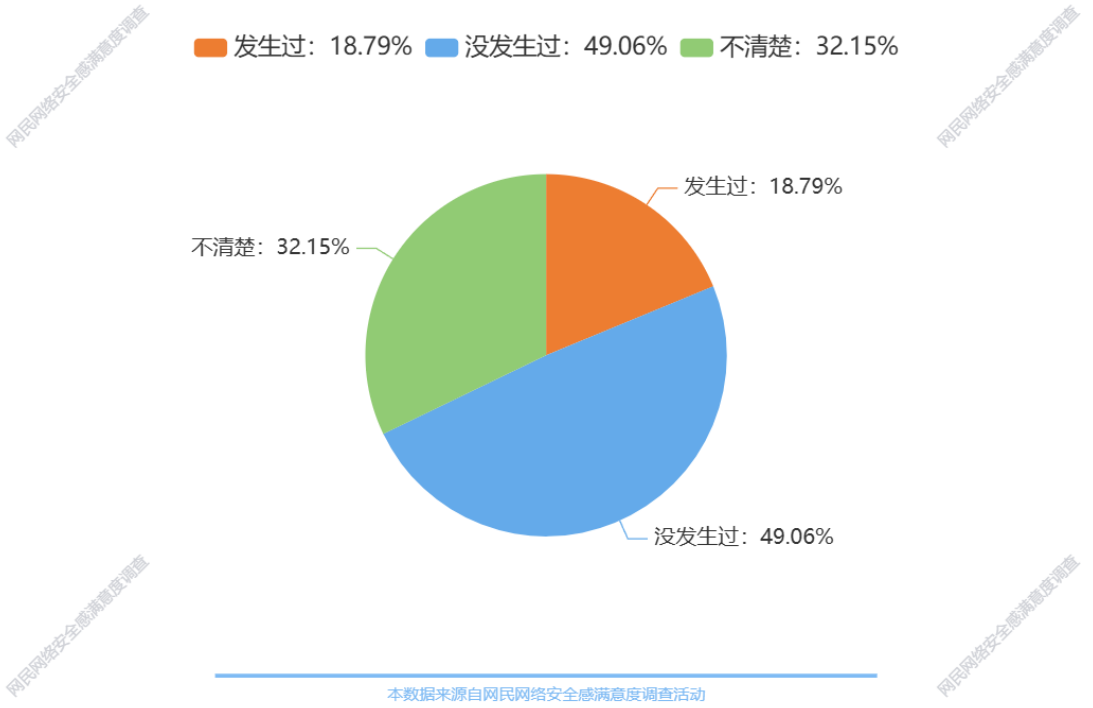

图3-23：网络安全等级测评满意度

数据来源：从业人员版A专题问卷行业治理与企业合规专题第12题：您所在单位发生过网络安全事件吗？

3.3.5.1. 发生网络安全事件类型

根据本次专题调查的结果，数据安全事件是最常见的网络安全问题，占比高达43.02%，涉及数据篡改、假冒、泄露等情况，共有6,200名受访者报告了此类事件。紧随其后的是恶意程序事件，包括病毒、蠕虫、木马等，占比42.55%，共有6,132名受访者选择。网络攻击事件也较为普遍，占比36.01%，共有5,190名受访者报告。信息内容安全事件，包括反动、暴恐、色情、虚假信息、网络欺诈等，占比29.58%，共有4,263名受访者选择。设备设施故障事件和违规操作事件分别占比17.40%和16.50%，显示出技术故障和人为失误也是网络安全事件的重要组成部分。安全隐患事件和异常行为事件分别占比15.20%和12.57%，而不可抗力事件占比7.35%，其他事件占比0.20%。

综合上述统计数据，我们可以发现网络安全事件的类型多样，且发生频率不一。数据安全事件和恶意程序事件是最主要的网络安全问题，这可能与当前网络攻击者日益增长的技术能力和多样化的攻击手段有关。网络攻击事件的高发率也提醒我们，外部攻击仍然是网络安全的重要威胁。

信息内容安全事件的占比相对较高，这可能与互联网信息的快速传播和监管难度有关。设备设施故障事件和违规操作事件的占比表明，内部管理和技术问题也是网络安全事件的重要来源。安全隐患事件和异常行为事件的占比虽然较低，但它们的存在提示我们网络安全需要持续的关注和预防。

不可抗力事件的占比最低，这可能是因为这类事件的发生与网络安全措施的直接关联性较小。然而，它们的存在也提醒我们，在网络安全管理中需要考虑到各种不可预测的因素。其他事件的占比最低，这可能包括一些罕见或特殊的网络安全问题。

总体而言，这些调研结果强调了网络安全管理的复杂性和多维性。为了有效应对网络安全事件，需要采取全面的安全措施，包括技术防护、人员培训、事件监测和应急响应等多个方面。同时，这些数据也为网络安全政策制定者和实践者提供了宝贵的参考，有助于他们更好地理解和应对网络安全威胁。

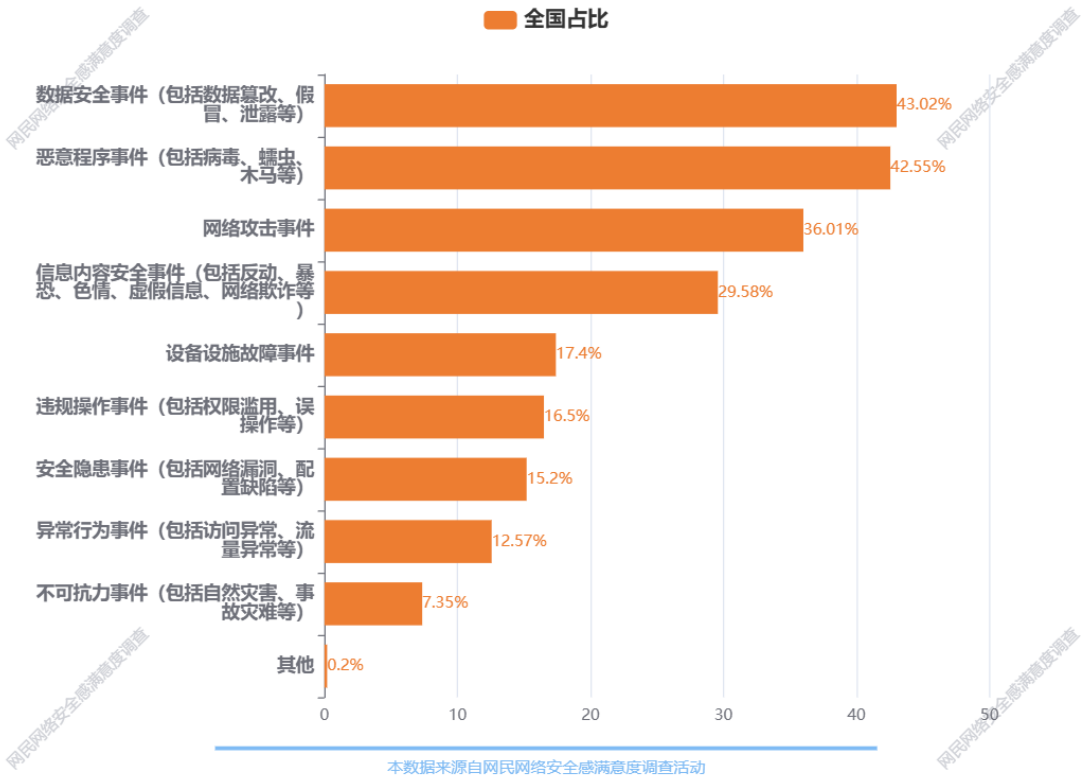

图3-24：发生网络安全事件类型

数据来源：从业人员版A专题问卷行业治理与企业合规专题第12.1题：发生了什么事件？

3.3.5.2. 网络安全应急预案完善程度

根据本次专题调查的结果，有7,173名受访者认为所在单位的应急预案“很完善”，占比高达51.33%，这表明超过一半的受访单位在应急预案建设方面做得相对不错。2,949名受访者认为应急预案“较完善”，占比21.10%，这一比例显示了一定数量的单位在应急预案方面也有一定的准备，但可能还有改进的空间。有2,774名受访者认为应急预案“一般”，占比19.85%，这可能意味着这些单位的应急预案处于中等水平，既不是特别完善，也不是特别不完善。相对较低比例的受访者认为应急预案“较不完善”（5.11%）和“很不完善”（1.78%），分别有714名和249名受访者选择。最后，有116名受访者表示单位“没有预案”，占比仅为0.83%。

综合上述统计数据，我们可以得出以下结论：绝大多数受访者认为所在单位的网络安全事件应急预案相对完善，其中超过一半的受访者认为应急预案“很完善”，而认为“较完善”和“一般”的受访者比例也相对较高。这表明大多数单位对网络安全事件的应急响应给予了一定的重视，并建立了相应的预案。然而，也有一小部分受访者认为应急预案存在不足，无论是“较不完善”还是“很不完善”，都需要单位进一步关注和改进。特别是对于那些表示“没有预案”的单位，建立和完善应急预案显得尤为迫切。

这些调研结果强调了应急预案在网络安全管理中的重要性。一个完善的应急预案可以帮助单位在面对网络安全事件时迅速响应，减少损失。对于那些应急预案不够完善的单位，建议加强预案的制定和演练，确保在真正的网络安全事件发生时能够有效应对。同时，这些数据也为网络安全管理部门提供了宝贵的参考，有助于他们了解当前的应急准备状况，并采取相应的措施来提高整体的网络安全应急响应能力。

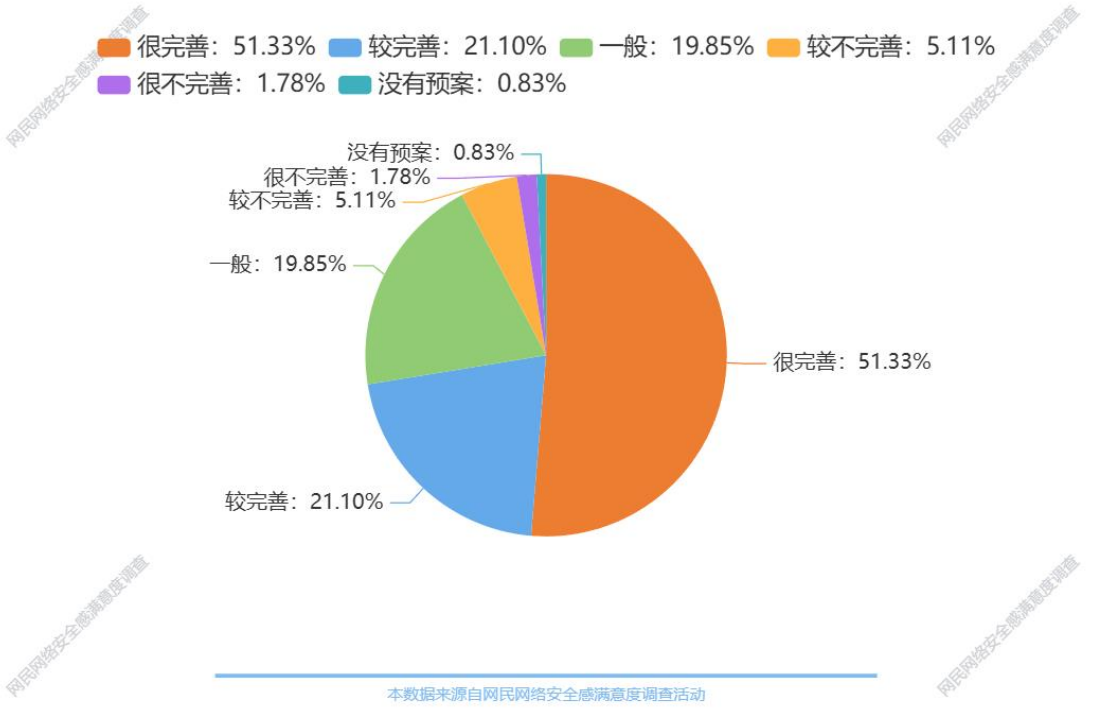

图3-25：网络安全应急预案完善程度

数据来源：从业人员版A专题问卷行业治理与企业合规专题第12.2题：您认为所在单位目前针对网络安全事件的应急预案是否完善？

3.3.5.3. 网络安全事件报案情况

根据本次专题调查的结果，有8,728名受访者表示所在单位在发生网络安全事件后“报案了”，占比高达62.45%，这一比例表明大多数单位在遇到网络安全事件时选择了向公安机关报告，显示出较强的法律意识和对网络安全事件处理的规范性；也有2,341名受访者表示“没有报案”，占比16.75%，这一比例虽不高，但也不容忽视，可能反映了一些单位在网络安全事件应对上的不足或犹豫。另外，有2,054名受访者选择“担心被处罚不敢报案”，占比14.70%，这揭示了一些单位可能对网络安全法律法规的理解和执行存在顾虑。852名受访者表示“不知道如何报案”，占比6.10%，这一比例指向了在网络安全事件报告流程上的知识和信息普及不足。

综合上述统计数据，我们可以得出以下结论：大多数受访单位在面对网络安全事件时能够积极履行法律责任，主动向公安机关报案，这不仅体现了单位对网络安全事件的重视，也反映了单位对法律规范的遵守。然而，也有相当一

部分单位在报案问题上存在犹豫或不知如何行动，这可能与对网络安全法律法规的不了解、担心报案后可能面临的处罚或其他实际困难有关。

这些调研结果强调了加强网络安全法律法规教育的重要性，特别是对于那些担心报案后被处罚的单位，需要通过法律宣传和教育来消除他们的顾虑，明确网络安全事件报案的法律责任和程序。对于那些不知道如何报案的单位，需要提供明确的指导和流程，确保他们在遇到网络安全事件时能够迅速、正确地采取行动。

总体而言，这些调研结果为网络安全管理部门提供了宝贵的参考，有助于他们了解当前单位在网络安全事件报案方面的现状，并采取相应的措施来提高单位的法律意识和应对能力。同时，也提示了在网络安全事件处理中，需要进一步加强法律支持和服务体系的建设，以确保网络安全事件能够得到及时、有效的处理。

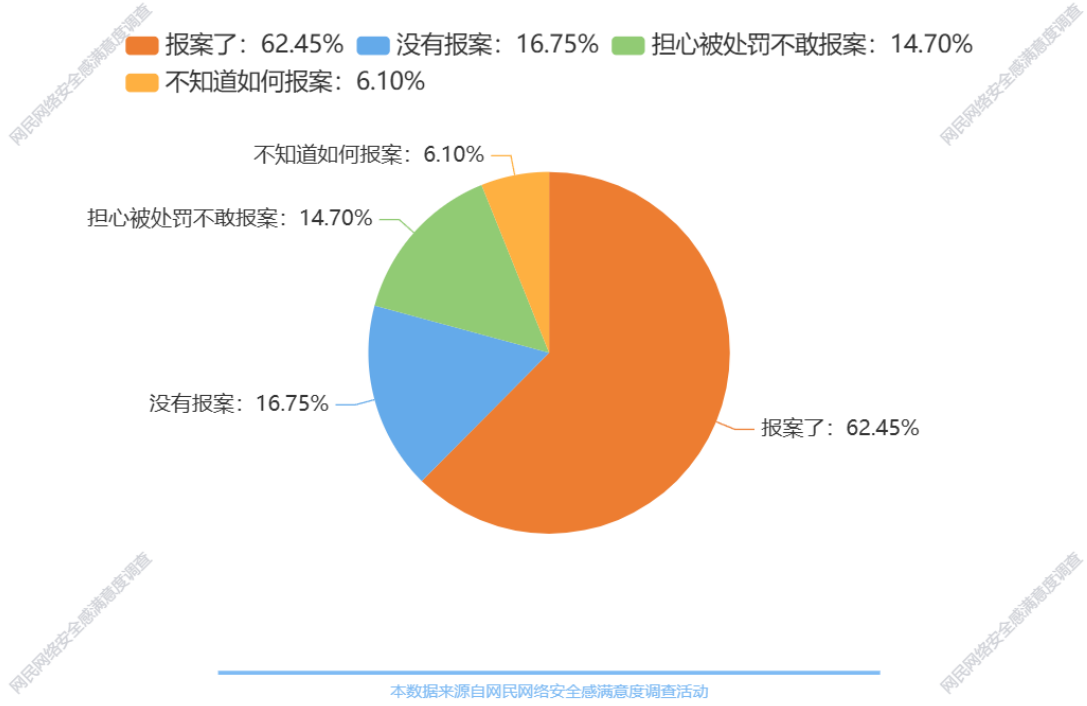

图3-26：网络安全事件报案情况

数据来源：从业人员版A专题问卷行业治理与企业合规专题第12.3题：您所在单位针对发生的网络安全事件向公安机关报案了吗？

3.3.5.4. 网络安全事件报案满意度

根据本次专题调查的结果，有5,732名受访者表示对公安机关案件受理“非常满意”，占比高达65.67%，这一比例显著，表明绝大多数报案单位对公安机关的案件受理工作给予了高度评价。此外，1,607名受访者表示“满意”，占比18.41%，进一步强化了公安机关案件受理工作的积极反馈。相对较少的受访者表示“一般”（1,123人，12.87%），“不满意”（123人，1.41%）和“非常不满意”（144人，1.65%），这些比例较低，但仍然值得关注，因为它们指出了公安机关在案件受理方面可能存在的问题或改进空间。

综合上述统计数据，我们可以得出以下结论：绝大多数受访单位对公安机关在网络安全事件案件受理方面的工作表示满意，其中超过三分之二的受访者表示“非常满意”，而“满意”的受访者比例也相对较高。这表明公安机关在处理网络安全事件的报案方面得到了广泛的肯定，其专业性和效率得到了报案单位的认可。

然而，也有一小部分受访者对案件受理表示“不满意”或“非常不满意”，虽然这些比例不高，但它们的存在提示公安机关在服务过程中可能存在一些不足之处，如响应速度、沟通效率或案件处理结果等方面可能需要进一步改进。这些反馈对于公安机关来说是宝贵的，可以帮助其识别服务中的弱点，并采取措施进行优化。

总体而言，调研结果显示了公安机关在网络安全事件案件受理方面的积极形象，同时也指出了改进的方向。对于公安机关而言，持续提升服务质量、增强与报案单位的沟通和反馈机制，以及提高案件处理的透明度和效率，是提升满意度的关键。对于调研报告的编写者来说，这些数据提供了有力的证据，支持了公安机关在网络安全领域的作用和影响力，同时也为进一步的政策制定和法律实施提供了依据。

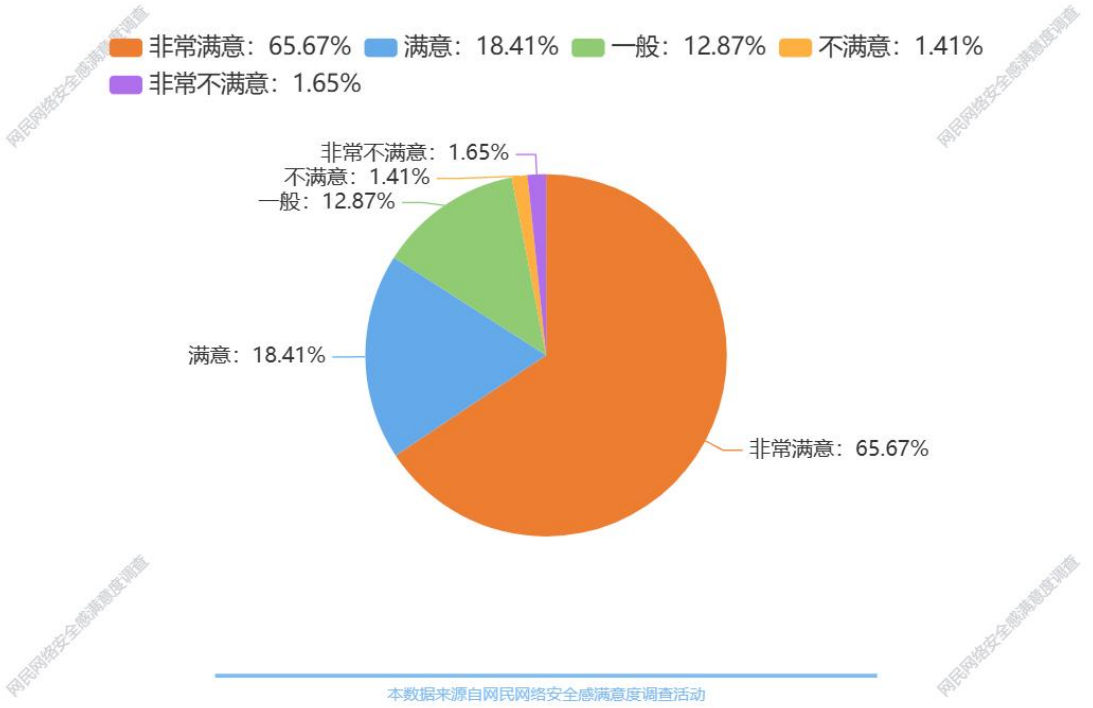

图3-27：网络安全事件报案满意度

数据来源：从业人员版A专题问卷行业治理与企业合规专题第12.4题：您所在单位对公安机关案件受理是否满意？

3.3.5.5. 网络安全事件报案不满意原因

根据本次专题调查的结果，最主要的不满原因是“没有结果”，占比达到30.99%，共有587名受访者选择此项，这表明受访单位在报案后未能获得明确的案件处理结果，这对他们的满意度造成了显著影响。其次是“专业能力欠缺”，占比25.34%，有480名受访者认为公安机关在处理网络安全事件时的专业能力不足。第三位的是“执法范围小，立案门槛高”，占比20.27%，共有384名受访者选择，这可能反映了受访单位对现行法律框架和立案标准的不满。“报警太麻烦”和“打击力度不够，效果不明显”也是受访者不满的原因，分别占比19.38%和18.00%。“处理不及时，效率低”的占比为11.56%，共有219名受访者选择。最后，“其他”原因的占比仅为0.21%，共有4名受访者选择。

综合上述统计数据，我们可以得出以下综述：受访单位对公安机关案件受理不满意的原因主要集中在案件处理结果的不明确、公安机关的专业能力不足、执法范围和立案门槛的问题、报警流程的复杂性以及案件处理的效率和效果。这些反馈指出了公安机关在网络安全案件受理方面存在的挑战和改进空间。

“没有结果”成为最主要的不满原因，这可能意味着案件处理流程缺乏透明度或者反馈机制不健全，导致报案单位对案件进展和结果缺乏了解。专业能力的欠缺可能指向公安机关在网络安全领域的专业培训和资源配置不足。执法范围和立案门槛的问题可能需要通过法律改革和政策调整来解决。报警流程的复杂性和案件处理效率的低下则指向了公安机关在案件受理流程优化和资源配置方面需要进一步改进。

这些调研结果对于公安机关而言是宝贵的反馈，它们不仅揭示了公安机关在案件受理方面存在的问题，也为公安机关提供了改进服务质量、提升公众满意度的具体方向。对于调研报告的编写者来说，这些数据提供了有力的证据，支持了公安机关在网络安全领域的作用和影响力，同时也为进一步的政策制定和法律实施提供了依据。公安机关可以利用这些反馈来优化案件受理流程，提高服务标准，以进一步提升公众的满意度和信任度。同时，对于表示不满意的少数受访者，公安机关应当给予特别关注，通过深入了解他们的具体不满点，采取针对性的措施进行改进，以确保所有单位都能获得高效、公正的案件受理服务。

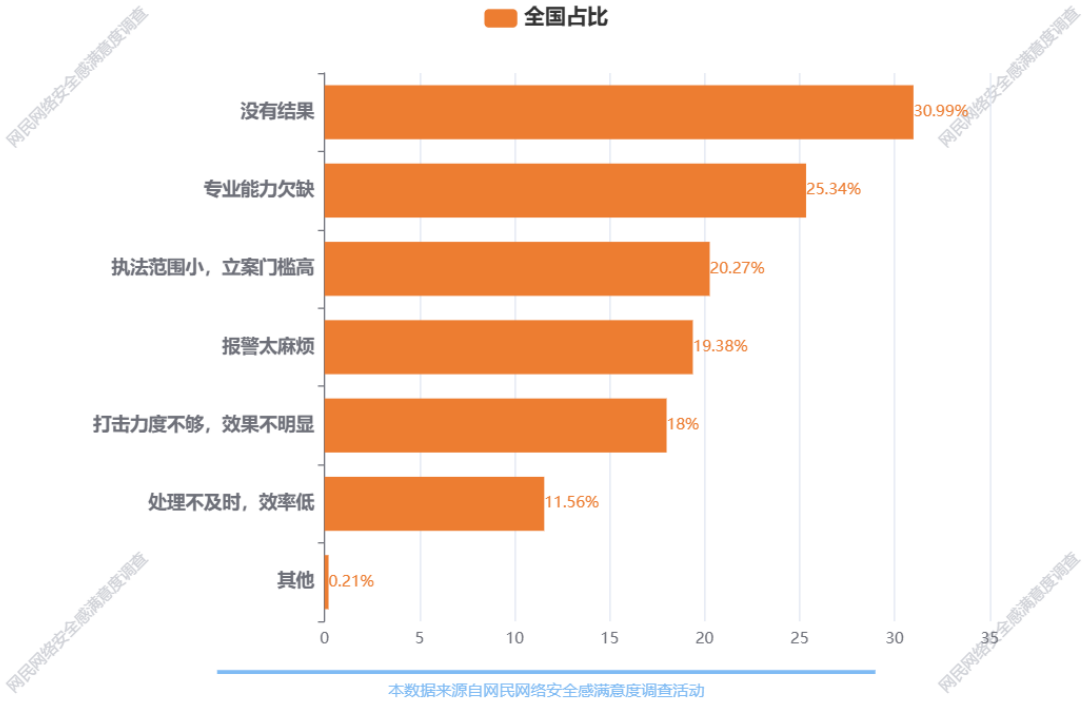

图3-28：网络安全事件报案不满意原因

数据来源：从业人员版A专题问卷行业治理与企业合规专题第12.5题：您认为不满意的原因是？

3.4. 关键信息基础设施安全保护落实

3.4.1. 对关键信息基础设施安全保护要求的认识

对于关键信息基础设施保护要求的认知情况，经过调查，我们发现41.09%的从业人员表示他们不仅了解这些要求，而且他们的单位已经积极实施。另一方面，14.50%的从业人员表示他们了解这些要求，但尚未在单位中实施。同时，有14.77%的从业人员表示他们知道这些要求，但对具体细节不够清晰。最后，29.64%的从业人员表示他们对这些要求并不了解。

通过对比23年的数据，我们可以看到，那些了解并已在单位实施关键信息基础设施保护要求的、了解，还没有实施的与知道，不清楚具体要求的从业人员比例都有所下降，而不了解的从业人员比例却上升了7.26%。这些数据表明了与去年相比，对于关键信息基础设施安全保护要求的整体认知情况不及去年。

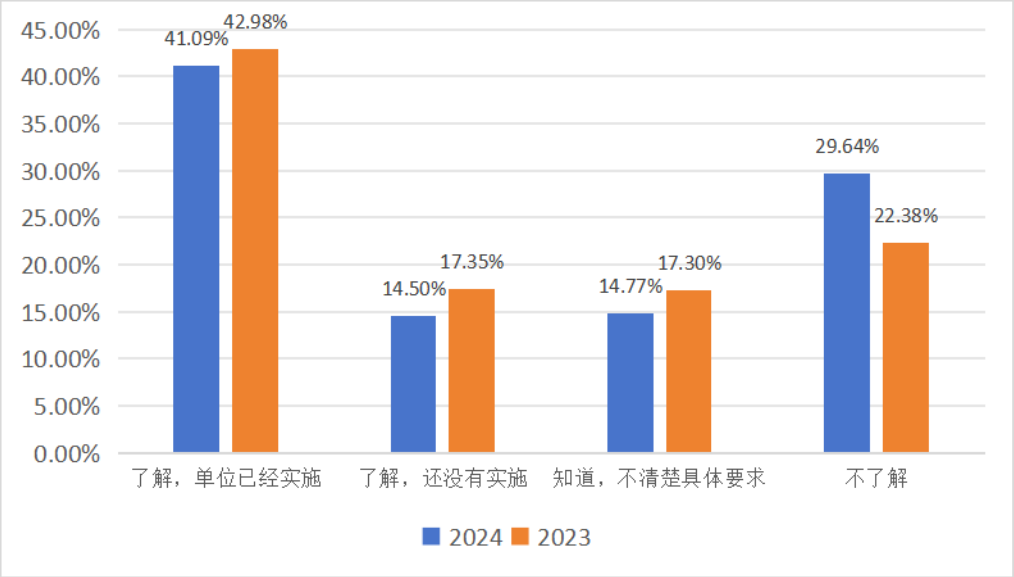

图3-29：对关键信息基础设施安全保护要求认识对比

数据来源：从业人员专题A版问卷行业治理与企业合规专题第13题：您对 GB/T 39204-2022《关键信息基础设施安全保护要求》标准了解吗？

在从业人员版A专题问卷行业治理与企业合规专题第20题：“您对推进等级保护、关键信息基础设施安全保护、商用密码应用以及加强企业合规管理有什么意见和建议？”中，共有22名被调查者提出“加强关键基础设施的识别和保护”类似建议，共有18名被调查者提出“提升关键基础设施的防御能力”类似建议，这也说明从业人员对关键信息基础设施安全保护有更高期望。

3.4.2. 对关保核心岗位人员管理要求的认识

关于关键信息基础设施保护关键岗位人员管理要求的认识，经过调查，结果显示：有57.07%的从业人员表示对其有所了解，且所在单位已经实施了相关管理措施；21.56%的从业人员表示虽然了解，但所在单位尚未实施；18.31%的从业人员表示知道这一要求，但对具体要求不够清晰；仅有3.06%的从业人员表示对此不了解。与去年相比，了解并已经实施的从业人员比例有所上升，对于了解，还没有实施的从业人员比例也有所上升，而对于知道，不清楚具体要求的从业人员占比下降了1.2%，对于不了解的从业人员占比下降的了1.41%。这表明从业人员对关键信息基础设施保护关键岗位人员管理要求的认识正在不断提高。

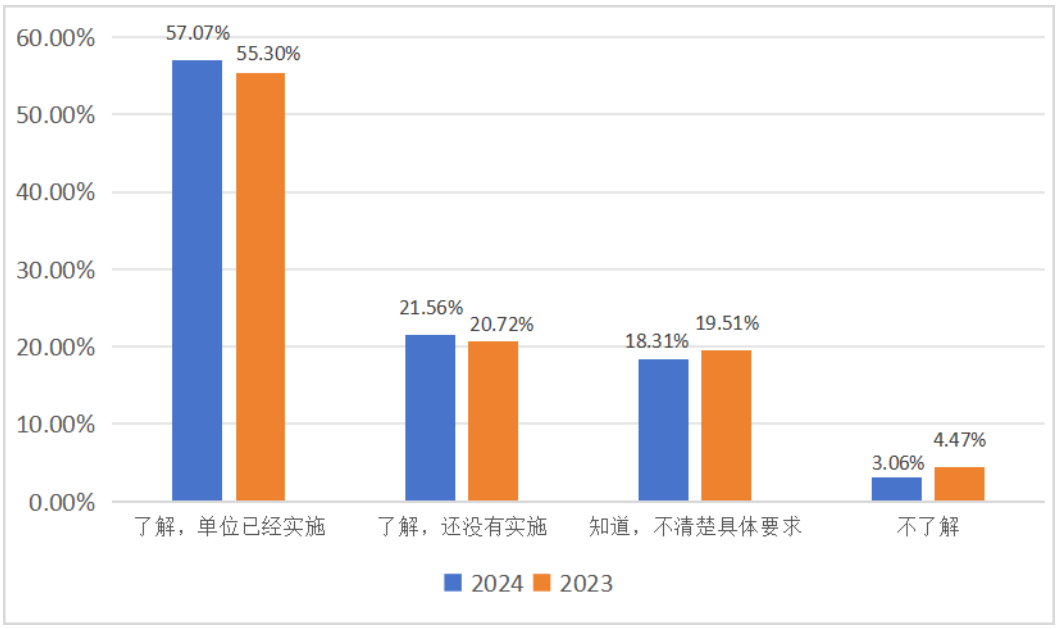

图3-30：对关保核心岗位人员管理要求认识对比

数据来源：从业人员专题A版问卷行业治理与企业合规专题第13.1题：您对关键信息基础设施安全保护关键岗位人员管理要求了解吗？

3.4.3. 对关保供应链安全管理要求的认识

对于关键信息基础设施保护供应链安全管理要求的认知情况，经过调查，结果显示有56.94%的从业人员表示已经了解并已在所在单位实施相关措施。另外，有21.19%的从业人员表示虽然了解但尚未在单位实施，18.43%的从业人员表示对此有所了解但不明确具体要求，而3.45%的从业人员则表示对此不了解。与去年相比，了解并已在单位实施相关措施的从业人员比例有所上升，对了解但尚未实施、了解但不明确具体要求以及不了解的从业人员比例也均有所

上升。这表明从业人员对关键信息基础设施保护供应链安全管理要求的认知程度正在逐步提高。

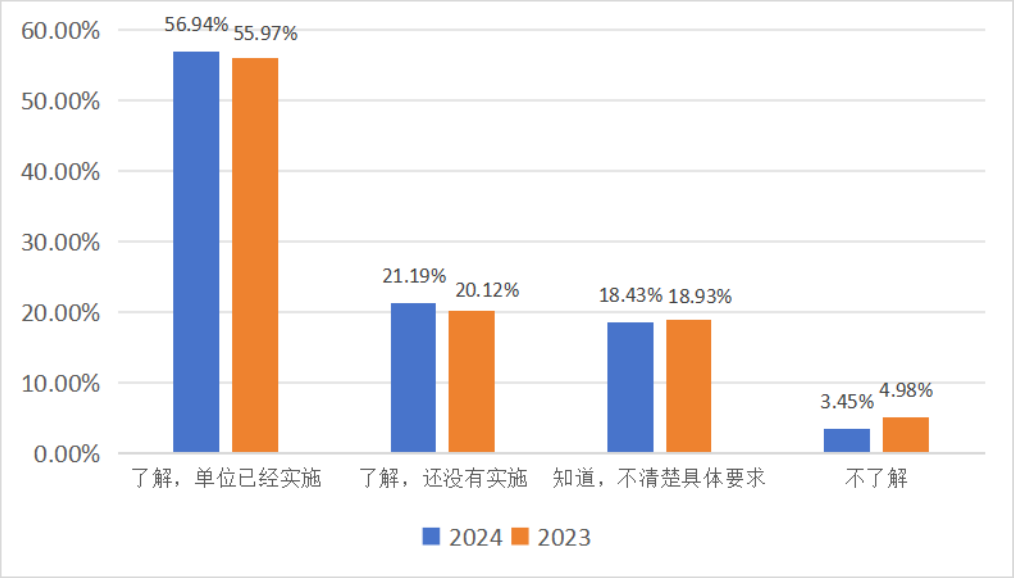

图3-31：对关保供应链安全管理要求的认识对比

数据来源：从业人员专题A版问卷行业治理与企业合规专题第13题：您对关键信息基础设施安全保护供应链安全管理要求了解吗？

3.4.4. 对关保总体实施情况满意度

经过对参与调查的从业人员对目前关键信息基础设施保护总体实施情况满意度分析调查，结果显示，有37.34%的从业人员对目前实施情况非常满意，33.04%的从业人员表示目前实施情况比较满意，有29.154.86%的从业人员表示对此一般。而4.75%的从业人员表示较不满意。在调查中发现，这次参与调查的从业人员对关键信息基础设施保护总体的实施情况还是比较满意。

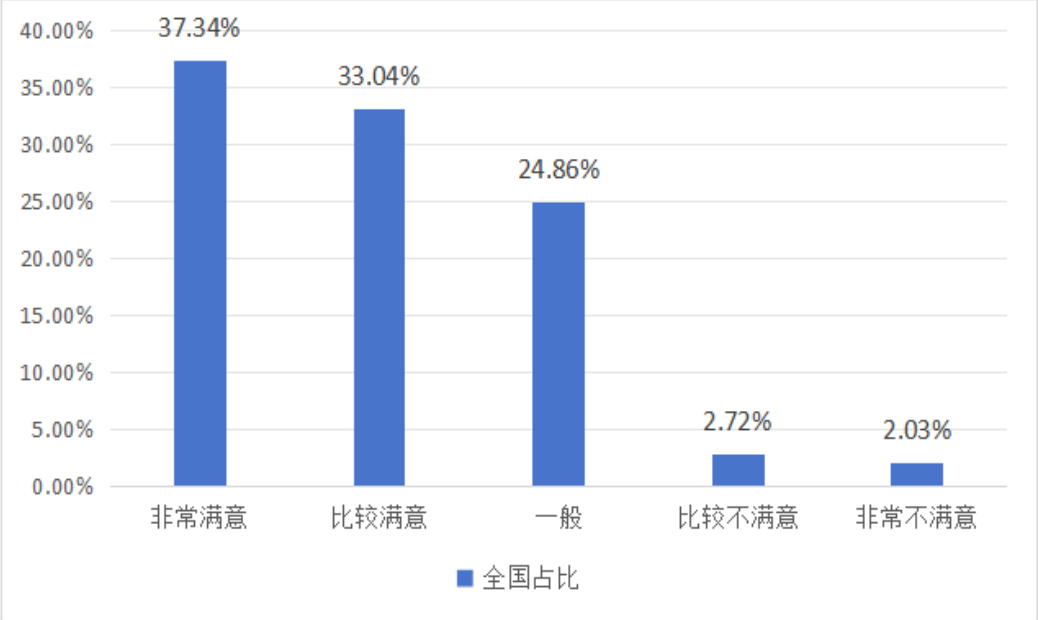

图3-32：对关保总体实施情况满意度

数据来源：从业人员专题A版问卷行业治理与企业合规专题第14题：您对目前关键信息基础设施保护总体实施情况满意吗？

3.4.5. 对关保主要问题分析

经调查研究比对，有近 32%的从业人员在单位所在行业没有制定关键信息基础设施保护工作的措施或不了解此事。在这近 32%的从业人员中，我们发现参与调查的从业人员认为行业指导不足的占 41.55%，对企业领导层不够重视的占 37.14%，对标准规范指南不足的占 35.62%，对相关产品和服务不能满足需求的占 28.50%，对企业资金压力太大的占 21.05%，对政府检查督促不足的占 19.54%，对认为企业技术队伍能力不足的占 15.71%，其他则占 1.35%。所以在此调查中表明需加强对其指导，提升能力。

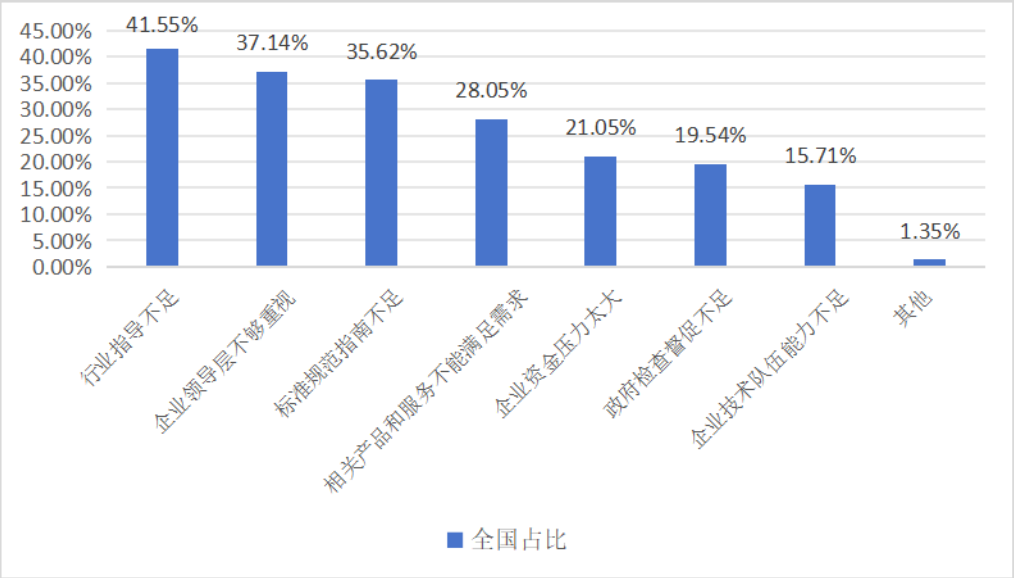

图3-33：对关保主要问题分析

数据来源：从业人员专题A版问卷行业治理与企业合规专题第14.1题： 你认为关键信息基础设施保护的主要问题？

3.5. 密码应用落实

3.5.1. 密码应用满足安全需求

在针对从业人员所在行业密码应用是否满足安全需求的调研中，有37.57%的受访者认为密码应用“完全满足”安全需求，是所有选项中占比最高的，显示出相当一部分从业人员对当前密码应用的安全性持有较高的信心。紧随其后的是“较满足”的受访者，占比32.11%，这进一步表明了对密码应用的普遍认可。然而，也有2.56%的受访者表示“较不满足”，而1.26%的受访者认为“完全不满足”，这些比例虽小，但暗示了在某些领域中密码应用的安全性还有待提升。

总体而言，调查结果显示大多数从业人员对所在行业的密码应用安全性持积极态度，但仍有一小部分受访者认为密码应用未能满足安全需求。对此，建议行业主管部门能够进一步调查分析那些不太满意或不满意情况，以识别潜在的安全漏洞和改进空间。同时，对于表示“不清楚”的7.87%的受访者，需要加强密码安全知识的普及教育，确保从业人员对密码应用的安全性有清晰的认

识。通过这些措施，可以进一步提升密码应用的安全性，确保行业整体的网络安全。

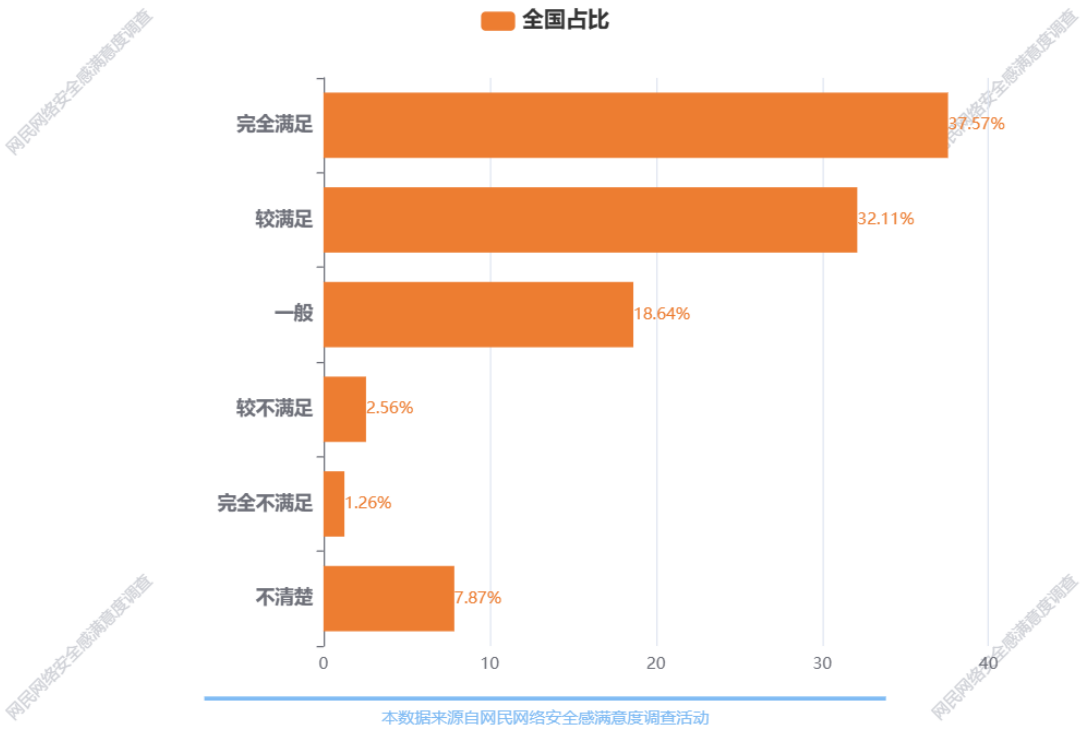

图3-34：密码应用满足安全需求情况

数据来源：从业人员版A专题问卷行业治理与企业合规专题第15题：您认为您所在行业密码应用是否满足安全需求？

在从业人员版A专题问卷行业治理与企业合规专题第20题：“您对推进等级保护、关键信息基础设施安全保护、商用密码应用以及加强企业合规管理有什么意见和建议？”中，共有20名被调查者提出“推广商用密码技术”类似建议，共有15名被调查者提出“加强密码管理”类似建议，这也说明从业人员对商用密码应用工作有更高期望。

3.5.2. 密码应用需求迫切程度

在商用密码技术应用场景的调研中，对哪个领域的密码应用需求最为迫切进行调查，结果按选择比例从高到低依次为：

1.企业内部的数据加密与防泄漏：占比最高，为44.15%，突显了企业对于内部数据安全的高度关注，尤其是在数据泄露事件频发的当下，企业对于保护其商业秘密和用户数据的需求十分迫切。

2.金融行业支付过程中的数据保护：占比41.38%，金融行业因其涉及资金往来，对数据安全的要求极高，任何支付过程中的数据泄露都可能导致严重的经济损失和信任危机。

3.政府机构的敏感信息保护：占比38.28%，政府机构持有大量公民个人数据和重要敏感信息，其对于密码应用的需求在于确保信息的安全性和可靠性，防止数据被非法访问或篡改。

4.数字化学习中的身份认证问题：占比36.44%，随着在线教育的兴起，确保学习平台上的用户身份真实性和防止身份盗用成为了一个重要议题。

5.智能网联汽车的车路数据协同：占比24.36%，随着车联网技术的发展，车辆与基础设施之间的数据交换安全变得尤为重要，密码技术在确保数据传输和处理安全方面发挥着关键作用。

6.生成式AI的数据泄露：占比22.17%，人工智能技术的发展带来了新的安全挑战，尤其是在数据保护方面，如何防止敏感数据的泄露成为了一个新问题。

7.VR应用中的个人信息保护：占比15.89%，虚拟现实(VR)技术在提供沉浸式体验的同时，也涉及到大量个人信息的处理，因此其对密码技术的需求同样不容忽视。

8.其他：占比0.49%，可能包括一些特定的行业或应用场景。

从调查结果来看，企业内部数据安全、金融支付数据保护和政府机构信息保护是商用密码应用中最为迫切的三个领域。这可能与这些领域数据的高价值性、对安全敏感性以及一旦发生安全事件可能带来的严重影响有关。同时，随着技术的发展，新兴领域如智能网联汽车、AI等对密码技术的需求也在逐渐增

加。对于这些领域，需要进一步强化密码技术的应用，提高安全防护能力，以应对不断增长的安全挑战。

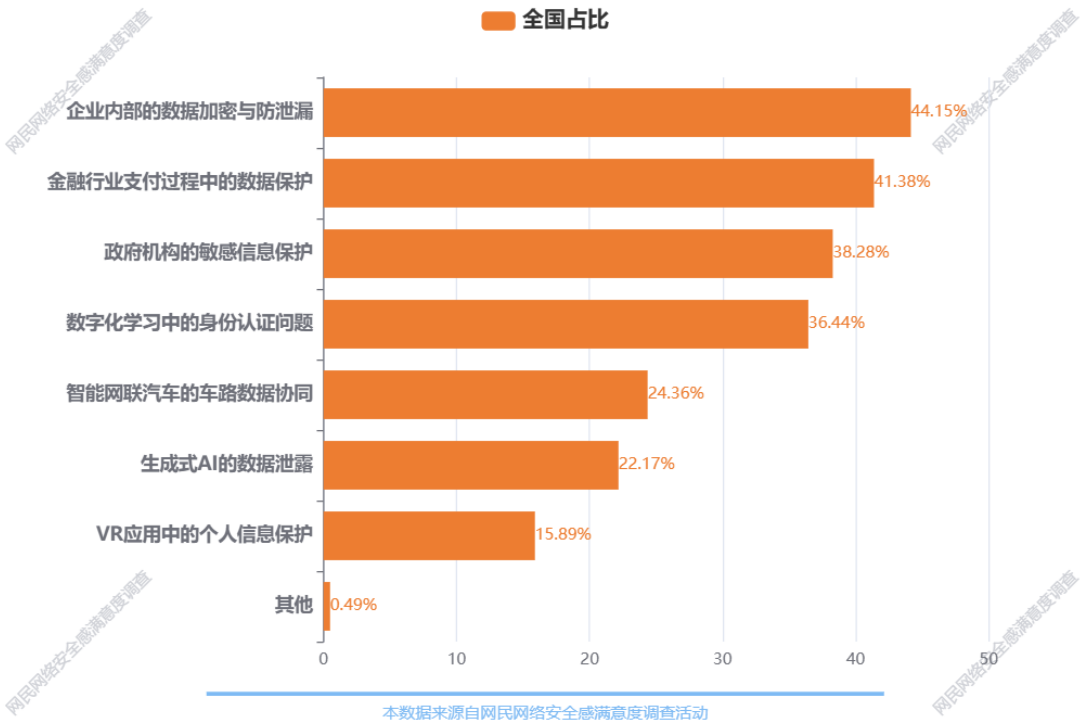

图3-35：密码应用需求迫切程度

数据来源：从业人员版A专题问卷行业治理与企业合规专题第15.1题：在商用密码技术的应用场景中，您认为哪个领域的需求最为迫切？

3.5.3. 商用密码安全性评估满意度

对于商用密码应用安全性评估工作整体状况的满意度，结果显示有35.38%的受访者表示“非常满意”，而33.25%的受访者表示“比较满意”。这表明绝大多数受访者对当前商用密码安全性评估工作持有积极的态度，这可能与商用密码在保障网络与信息安全中的重要作用有关。

然而，也有2.77%的受访者表示“较不满意”，1.24%的受访者“非常不满意”，还有8.40%的受访者表示“不清楚”。这表明尽管商用密码安全性评估工作得到了一定程度的认可，但仍有改进的空间，特别是对于那些不太了解或不满意当前评估工作的人。可能需要进一步的培训和教育，以提高从业人员对商用密码安全性评估工作的认识和满意度。

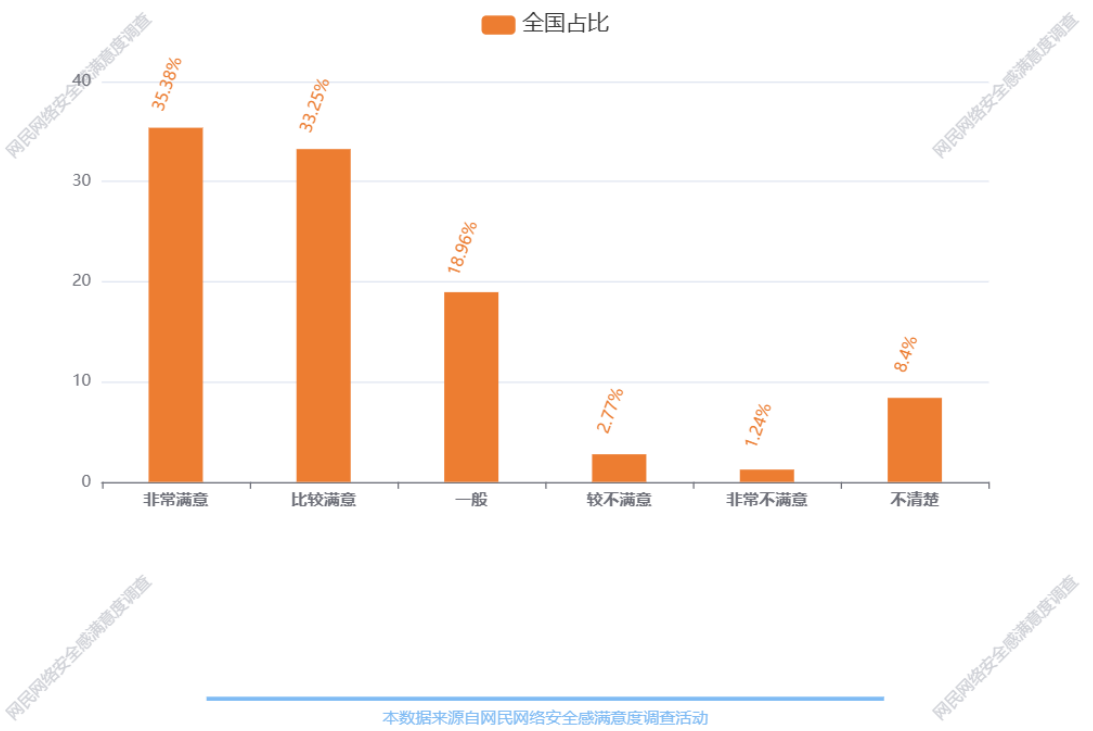

图3-36：商用密码安全性评估满意度

数据来源：从业人员版A专题问卷行业治理与企业合规专题第16题：您对商用密码安全性评估工作整体状况是否满意？

3.5.4. 商用密码安全性评估存在问题

对于商用密码安全性评估工作中存在一系列问题，按问题被提及的比例从高到低，结果如下：

1.评估工作时间过长（28.62%）：这一问题表明受访者认为商用密码安全性评估的周期过长，可能影响被评估单位项目的进度和效率。

2.评估人员技术能力不足（28.18%）：紧随其后的是评估人员的技术能力问题，这可能影响评估的准确性和可靠性，从而影响整个安全性评估工作的有效性。

3.过程监督和管理有待加强（26.80%）：这一问题的存在暗示了被调研的从业人员认为商用密码安全性评估过程中可能缺乏有效的监督和管理机制，需要进一步加强以确保评估工作的质量和效率。

4.申报流程有待优化（20.60%）：申报流程的复杂性或不明确性给从业人员带来了不便，这表明流程优化是提高评估工作满意度的关键环节。

5.评估机构数量不足（14.21%）：评估机构的数量不足可能导致资源分配不均，影响评估服务的及时性。

6.现场测评人员工作不够细致（8.45%）：现场测评工作如果不够细致，可能会遗漏关键的安全问题，影响评估结果的全面性和准确性。

7.现场测评人员太教条化，过于死板（5.70%）：这一问题表明，一些现场测评人员可能过于依赖规定流程，缺乏灵活性。

8.不清楚（15.27%）：有相当一部分受访者表示不清楚存在的问题，这可能反映出对商用密码安全性评估工作的了解不足，或者对评估工作的细节不够关注。

9.其他（0.16%）：最后，有极小部分受访者提出了其他方面的问题。

调查结果揭示了商用密码安全性评估工作中仍然存在一些重要问题，这些问题的存在可能影响评估工作的质量和效率。为了提高商用密码安全性评估工作的满意度，建议采取以下措施：

- 简化流程：优化申报流程，减少不必要的步骤，提高流程的透明度和易操作性。
- 提升人员能力：加强对评估人员的培训，提升他们的专业技能和评估能力。
- 加强监督管理：建立和完善评估工作的监督和管理机制，确保评估工作的质量。
- 扩充评估机构：增加评估机构的数量，提高服务的覆盖面和及时性。

- 细致化现场测评：鼓励现场测评人员更加细致和灵活地进行评估，确保评估结果的全面性和准确性。
- 提高认知度：通过教育和培训，提高从业人员对商用密码安全性评估工作的认识和了解。
- 通过这些措施，希望可以有效解决当前商用密码安全性评估工作中存在的问题，提升评估工作的质量和效率。

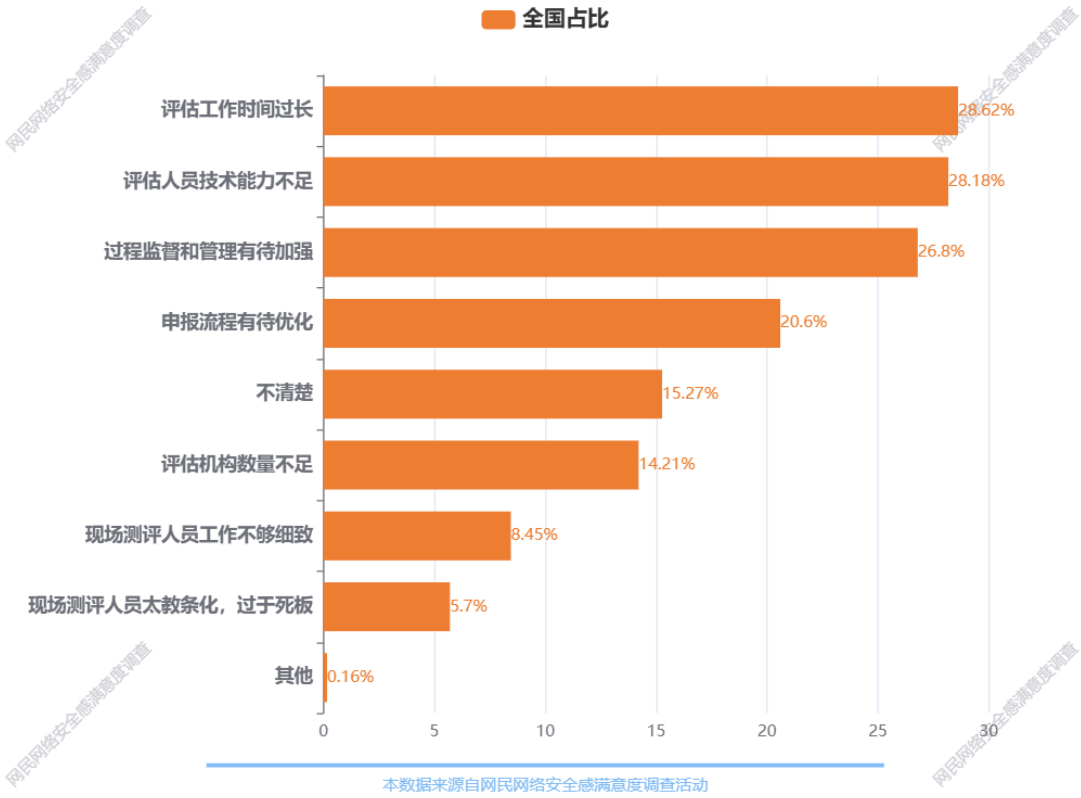

图3-37：商用密码安全性评估存在问题

数据来源：从业人员版A专题问卷行业治理与企业合规专题第16.1题：您认为商用密码安全性评估工作中那些方面存在问题？

3.5.5. 密码技术升级改造中遇到问题

在针对密码技术升级或改造的调研中，我们发现从业人员普遍面临一些挑战。其中最为显著的是资金管理不到位，占比高达33.00%，这反映出在技术升级过程中资金的合理分配和使用是一大难题。紧随其后的是政策支撑不足，占

比32.29%，这可能意味着在升级或改造过程中缺乏足够的政策指导和支持，导致从业人员感到方向不明确。此外，技术人员能力不足也是一个重要问题，占比27.47%，这表明在密码技术领域，专业技术人才的培养和引进亟需加强。

另一方面，密码产品技术缺乏的问题也不容忽视，占比16.36%，这可能限制了技术升级或改造的选项和质量。同时，有5.88%的受访者表示缺乏有效的领导小组，而6.22%的受访者指出缺乏密码应用管理制度。这些问题都可能影响到密码技术升级或改造的顺利进行。还有18.39%的受访者表示对过程中遇到的问题并不清楚，这可能反映出对整个升级或改造流程的了解不够深入。最后，有0.20%的受访者提出了其他方面的问题。

这些调研结果指出了在密码技术升级或改造过程中需要重点关注和解决的问题。为了确保技术升级或改造的成功，我们需要从加强资金管理、提供明确的政策支持、提升技术人员能力、丰富密码产品技术等方面入手。同时，建立有效的领导和管理制度，提高从业人员对流程的认识，也是推动密码技术升级或改造的关键步骤。

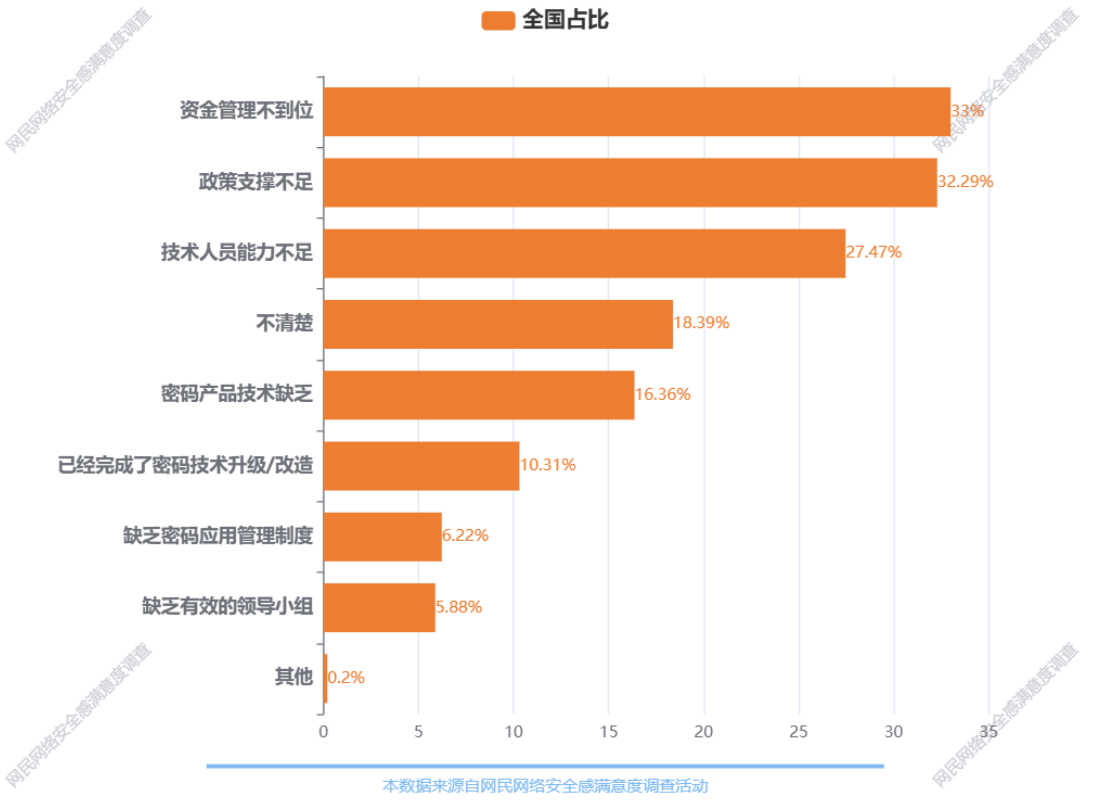

图3-38：密码技术升级改造中遇到问题

数据来源：从业人员版A专题问卷行业治理与企业合规专题第17题：您认为在进行密码技术升级或者改造过程中遇到哪些问题？

3.5.6. 密码设备监测计划

对于密码设备进行长期监测的计划，结果显示有44.47%的单位已经建立了统一的监管平台，并制定了对密码设备进行长期监测的计划，这显示出这些单位在密码设备安全性监管方面的前瞻性和主动性。

同时，有26.06%的单位虽然拥有统一的监管平台，但尚未制定长期监测计划，这可能意味着这些单位在密码设备监管方面存在一定的滞后性。此外，7.65%的单位还没有设立对密码设备进行长期监测的计划，这可能表明这些单位对密码设备的安全监管重视不够，或者缺乏相应的资源和能力。

还有21.83%的受访者表示不清楚本单位是否有相关计划，这可能反映出这些单位在内部沟通和管理上存在一定的不足。只有极少数单位表示已经完成了密码技术升级/改造，这可能说明大多数单位仍在进行或尚未开始这一过程。

综上所述，虽然有近半数的单位已经实施了密码设备的长期监测计划，但仍有相当一部分单位在这方面存在欠缺。这提示我们，加强密码设备监管的意识、提升监管能力、优化内部沟通机制是提高密码设备安全性的关键步骤。

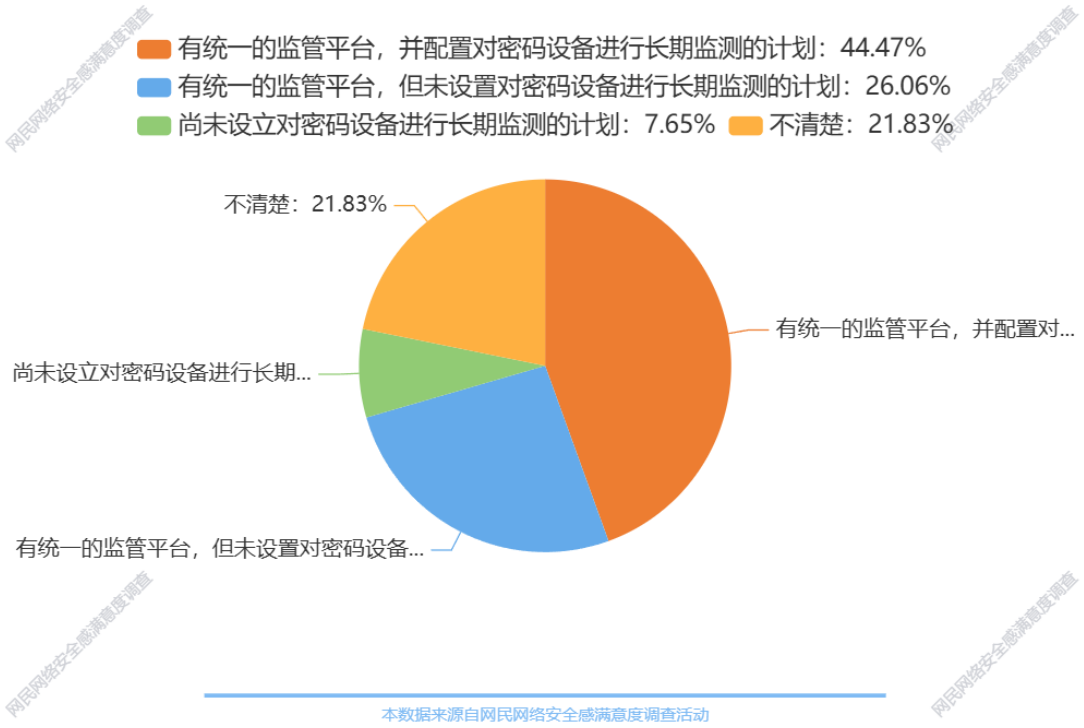

图3-39：密码设备监测计划

数据来源：从业人员版A专题问卷行业治理与企业合规专题第18题：您所在单位是否有对密码设备进行长期监测的计划？

3.5.7. CA证书申请使用问题

对于从业人员在CA证书申请和使用过程中遇到的问题，结果显示最突出的问题是“CA证书申请流程比较繁琐”，占比达到了44.58%。这表明许多从业人员认为CA证书的申请过程复杂，可能涉及多个步骤和要求，这不仅增加了工作量，也可能成为技术升级和实施的障碍。其次，有40.08%的受访者关注“个人隐私信息泄露风险”，这反映了在CA证书申请和使用过程中，个人信息保护是受访者非常关心的问题。任何涉及个人信息的处理都需要谨慎，以防止数据泄露和其他安全风险。此外，还有37.82%的受访者认为“CA证书审核过程较长”，这可能意味着在申请CA证书后，需要等待较长时间才能获得审批和证书发放，这可能影响业务流程和项目进度。而“CA证书更新不及时”和“CA证书管理缺乏制度”分别占比27.74%和22.20%，这些问题指出了证书管理过程中的不足，包括证书更新的及时性和管理制度的完善性。最后，16.89%的受访者提到“不同CA发放的数字证书的通用性不强”，这表明不同CA机构颁发的

证书在互认和兼容性方面存在问题，这可能给需要跨平台或跨系统操作的用户提供不便。

通过对于以上调查结果的分析，我们可以看到，在CA证书申请和管理过程中，有很多需要关注和改进的领域。为了提高效率和用户满意度，建议简化申请流程、加强隐私保护措施、缩短审核时间、及时更新证书以及建立更加完善的管理制度。同时，也建议主管单位能够出台一些政策，以提高不同CA证书间的互操作性。

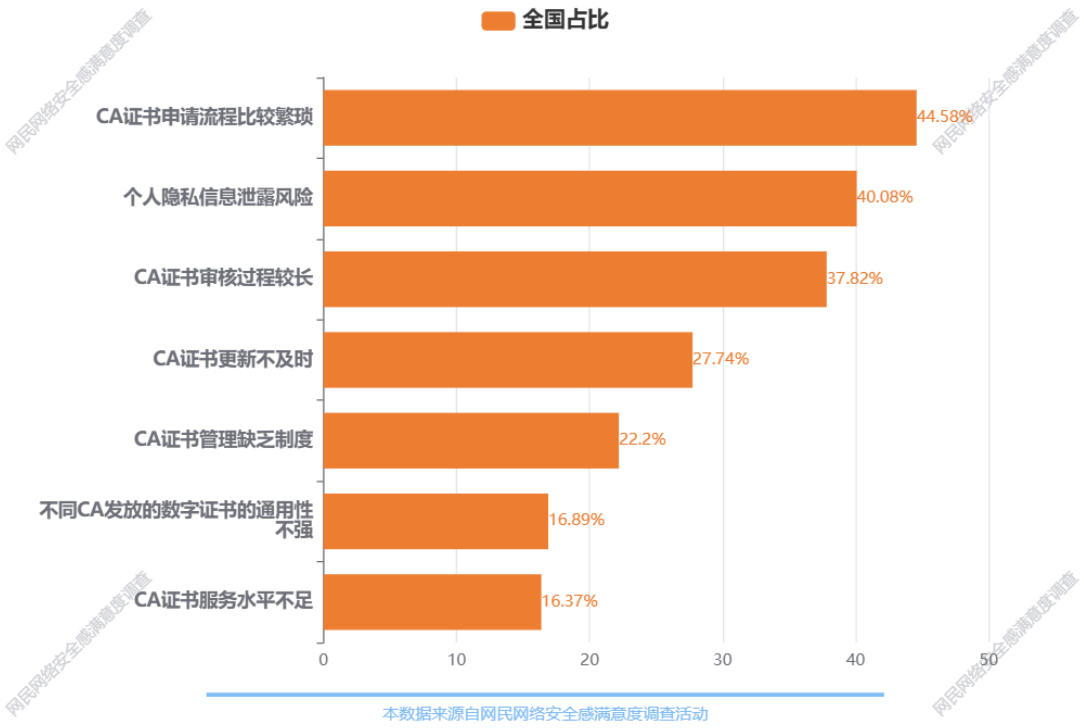

图3-40：CA证书申请使用问题

数据来源：从业人员版A专题问卷行业治理与企业合规专题第19题：您在 CA 证书在申请、使用过程中遇到的以下那些问题？

四、“行业治理与企业合规”专题调查建议

经过对2024年调查数据进行详尽的统计与研究分析，我们发现参与本次调查的网络安全从业人员对我国整体的网络安全状况以及网络安全行业治理水平表达了较高的满意度。他们普遍认为，网络安全等级保护、关键信息基础设施安全保护和商用密码应用的实施为我国网络空间安全行业的治理以及企业的合规发展提供了有力的支撑。同时，随着等级保护制度、关键信息基础设施安全保护制度和商用密码管理制度的逐步落地之中，各类企业也正逐步加强对网络安全合规工作的认识和自觉性。

面对当前国内外复杂多变的网络空间安全新形势和人工智能大模型等新技术发展带来的新挑战，我们需要在网络安全等级保护制度为我国网络空间安全奠定坚实基石的基础上，进一步推动关键信息基础设施安全保护和商用密码应用工作的落地实施，进一步完善企业网络安全合规体系的建设。这将为我们早日实现“网络强国”和“数字中国”的战略目标提供坚实的保障。

4.1. 加强网络安全等级保护专业能力有效支撑数字中国建设

经过五年的实施，网络安全等级保护2.0对我国网络安全工作的推动作用已得到显著体现。通过本次调研数据显示，网络安全等级保护在定级、备案、建设整改以及等级测评等方面的普及率已相当高。同时，各单位及网络安全从业人员对等级保护测评的满意度也在持续上升。展望未来，网络安全等级保护工作制度作为《网络安全法》明确规定的我国网络安全基础制度，有力地支撑了数字中国建设，保障我国数字经济发展。同时，随着我国公共数据要素的开发利用、以及各行业数字化转型的加速推进，网络安全等级保护制度将在更多领域发挥基础保护作用。我国公安机关也在网络安全等级保护2.0中提出的对各种新技术和新应用场景的安全保护要求的基础上，也正在完善人工智能大模型系统安全相关标准，防范人工智能大模型技术应用时带来的新风险。

值得注意的是对于网络安全等级测评不满意的主要原因已经连续两年为对“专业能力欠缺”，且均超过了50%，且攻击有14名被调查者提出“提高测评机构的专业能力”的明确建议。因此，建议网络安全等级测评主管部门应通过开

展定期测评专项能力验证、加强飞行技术检查、推动测评技术科研成果推广等措施提高测评机构专业能力。

4.2. 推动关键信息基础设施安全保护标准体系尽快完善

通过本次调查发现相比去年数据，今年关键信息基础设施安全保护工作的普及率有所提升，特别是在核心岗位人员管理和供应链管理这两大核心工作上，取得了从2022年开展关保调查以来的首次上升，但相比网络安全等级保护工作水平而言仍有很大的上升空间。

自《关键信息基础设施安全保护条例》发布以来已满两年，同时GB/T 39204-2022《关键信息基础设施安全保护要求》也已实施近一年。鉴于关键信息基础设施安全关乎国家安全和国计民生稳定，其配套实施落地工作亟须加快步伐，尽快驶入快车道。特别是在GB/T 39204-2022《关键信息基础设施安全保护要求》中，已明确规定关于关键信息基础设施的分析识别、安全防护、检测评估、监测预警、主动防御和事件处置等具体安全保护要求。但是，与之配套的具体政策和标准还迟迟未立项或颁布实施。

因此，根据本次调查结果建议我国关键信息基础设施行业主管部门尽快依据《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》（公网安〔2020〕1960号）的核心精神，出台相关政策文件和技术标准指导关基安全保护要求的落地实施，并借鉴以往网络安全等级保护制度中定级、备案、建设整改和等级测评等工作宣贯落地的经验，迅速组织具备咨询规划、检测评估、监测预警等能力的第三方机构，共同推进关键信息基础设施安全保护工作的宣贯落地。

4.3. 提升商用密码应用安全性评估水平

随着《商用密码管理条例》的实施和以GB/T 39786-2021《信息系统密码应用基本要求》为核心的密码应用系列标准的应用，我国商用密码应用正逐步走上既定轨道。今年商用密码应用作为首次加入行业治理与企业合规专题的新调查领域，展现出远超2022年关键信息基础设施安全保护新加入时的满意度水平。商用密码安全性评估的满意度也紧随网络安全等级测评满意度78.63%达到了68.63%。但是，本次调查也发现了商用密码应用安全性评估工作过程中存在

的一系列不足问题，包括评估时间过长、评估人员技术能力不足、过程监督和管理有待加强等问题。

因此，有必要参照网络安全等级测评发展的历程，通过简化流程、加强对评估人员技术能力提升、加强第三方监督管理、对评估机构进行优胜劣汰、细化现场评估标准要求等措施来进一步完善。

4.4. 谋划企业网络安全合规新举措

随着我国《中央企业合规管理办法》和GB/T 35770-2022《合规管理体系要求及使用指南》的发布和实施，企业合规管理体系在我国已初步构建。然而，根据本次调研结果，众多企业在网络安全合规体系的建设方面尚处于起步阶段，对网络安全合规体系的仍然一知半解。

结合我国当前企业网络安全合规工作的实际情况，建议应优先建立健全网络安全合规管理机制。依据“四法三条例”，重点落实网络安全合规专门责任机构和合规负责人的设立，并进一步完善违规责任追究制度和定期合规安全检查机制。通过实施上述措施，提升网络安全合规在企业合规管理体系中的重要程度，保障企业网络安全合规运营。特别是应首先推动企业网络安全经费占信息化开支的比例平均不低于10%的基础目标，充足资源保障企业网络安全合规体系建设。

附件一：调查方法与数据样本情况

一、背景

为贯彻习近平总书记有关“网络安全为人民，网络安全靠人民”等网络强国的重要思想，进一步落实《网络安全法》及相关法律法规，增强网民的网络安全意识和防范能力，促进互联网企业履行社会责任意识和能力的提高，提升网民网络安全感和满意度，最大限度调动网民参与网络生态社会治理的自觉性和主动性，助力政府相关部门积极探索网络治理规律，提高网络治理成效，由全国135家网络安全行业协会及相关社会组织联合发起了2024网民网络安全感满意度调查活动。

二、目的

网民网络安全感满意度调查的宗旨就是以人为本。调查活动直接面向网民大众，目的是让大家有话可以说，让政府主管部门可以直接倾听网络安全在网民中的感受、了解网民的诉求和存在的问题，同时也向广大网民宣传网络安全的相关政策、法规和知识。

开展网民安全感满意度调查活动的具体目的有以下几点：

（1）通过广泛收集广大网民上网用网过程中对网络公共秩序、安全环境的真实感受和评价，多角度反映我国网络空间安全治理成效和网络安全现状，为政府部门决策提供数据支持。为各级政府主管部门加强互联网安全监管和打击网络违法犯罪提供指引。

（2）通过发挥社会组织的桥梁作用，调动社会各方力量，广泛发动广大网民积极参与网络安全治理，齐心协力，贡献智慧，共建良好网络生态，共筑网络安全屏障。

（3）通过不断收集和积累网民网络安全感满意度数据，形成庞大的数据库，为满意度研究和各种数据分析挖掘研究提供数据基础，建立和优化网民网络安全感满意度评价模型，推动网民网络安全感满意的量化研究向前发展。

三、调查方式

（1）调查时间

2024年7月，2024网民网络安全感满意度调查活动正式启动。调查活动于2024年7月16日开始正式对外采集数据，至7月25日24时结束。采集的时间段为10天。

（2）调查对象

本次调查对象分为两类：一类是普通网民，另外一类是网络行业从业人员。普通网民主要面向在中国境内有上网经验，熟悉中国互联网情况的互联网使用者。他们的意见主要体现互联网普通用户的感受。网络行业从业人员主要面向在网络行业工作人员，其工作单位或工作岗位和互联网有关，包括互联网企业、网络安全产品与服务的提供者、网络安全协会、政府主管部门、企事业单位、网络安全的学校和科研机构、一般的互联网用户等。网络行业从业人员对互联网的状态比较了解，是网络安全治理中主要的参与者、服务提供者和服务利用者。他们的意见体现了网络安全治理中关系密切的各方面利益群体和专业人士的观点。

两类调查对象的意见的综合和对比可以较为全面地反映各类网民的真实感受，为课题研究提供较全面的数据基础。

（3）调查内容

本次网民网络安全感满意度调查内容丰富，内容涵盖个2个主问卷、12个专题领域，问卷题目总数量达432道。调查问卷按访问对象不同分两类问卷：面向普通网民的公众版和面向网络行业人员的从业人员版问卷

公众版的调查问卷除了以共性问题为主的主问卷外，还根据内容主题的不同分了9个专题问卷，具体名称如下：

专题1：网络安全法治社会建设

专题2：网络诚信建设

专题3：遏制惩处网络违法犯罪行为

专题4：个人信息保护和数据安全

专题5：网络购物权益保护

专题6：特殊人群（未成年人和老人等）网络权益保护

专题7：互联网平台监管与企业自律

专题8：数字政府服务与治理能力提升

专题9：网络社会发展的变化与冲击

从业人员版的调查问卷除了以共性问题为主的主问卷外，还根据内容主题的不同分为A到C共3个专题问卷，具体名称如下：

A专题：行业治理与企业合规

B专题：行业发展与科技创业

C专题：新技术挑战与网络安全

本次调查问卷的设计以网络安全感满意指标体系为框架，以网民对网络安全的认知、需求、感受与评价为主线，针对相关政府主管部门、互联网企业、安全产品服务供应商、协会、科研机构、一般联网使用单位及网民等不同网络角色在网络空间活动的问题、感受及其期望设计调查问题。

除了一般的选择题外，问卷还设立了9道征求意见的填空题，以开放题的形式让网民畅所欲言，以求充分收集网民的意见。

（4）调查形式

本次调查形式主要为线上问卷调查方式。组委会牵头统一部署，各省发动单位分别组织落实，企业机构参与，网民自愿参加。

线上方式主要是依托在基于云平台问卷调查云服务，通过建立网民网络安全感满意调查服务门户和相应的网上问卷调查应用，同时支持两份公众版和从业人员版调查问卷的数据采集，提供手机和PC两个渠道，支持二维码扫描分享。组委会利用微信公众号和各合作单位以及支持单位的信息服务门户进行推广，取得良好的效果。

（5）调查组织

各级公安、网信等政府主管部门对调查活动给予了大力支持。有关组织单位领导高度重视，明确目标，指导把关，积极推动，狠抓落实，成效显著。

在政府主管部门领导的关心和指导下，为加强对调查活动的组织，活动发起单位组建了强有力的组织机构，机构分为领导小组、活动组委会（秘书处）和专家组等。

领导小组由各级有关主管部门、发起单位网安联主要领导组成，负责调查活动重大事项的决策。

活动组委会由各发起单位和承办单位的主要领导组成，负责活动的组织工作，有关活动事项的组织实施。下设秘书处，负责日常办公事务处理和对外联系和活动的宣传、组织、协调。承办单位广东新兴国家网络安全和信息化发展

研究院负责调查问卷设计、技术实施、数据处理、数据分析、报告编写等。活动组委会和承办单位在总结历届网民网络安全感满意度调查活动经验基础上，今年的调查活动在活动组织、品牌建设、推广发动、研究规划、问卷设计等方面进行了多方面的创新和改进，取得显著的效果。

专家组由国家及地方相关领域的专家、学者组成，负责审查及评价调查设计、调查过程的科学性、客观性和真实性。

活动的组织分为前期策划、问卷设计、组织发动、调查实施、数据分析与报告编制、成果发布与总结表彰等几个阶段。

各地发起单位按照组委会的统一部署和要求开展工作，一是协调所在地互联网企业组织员工参与调查活动。最大限度地协调所在地互联网企业组织员工参与调查活动，确保调查活动有针对性、合理性、科学性地开展；二是组织协调所在地商业门户网站、新媒体网络平台、中央（地方）重点新闻门户网站等参与调查活动。充分发挥这些网络平台在本地影响力大、覆盖面广、粉丝量多的特点，通过一定的推广合作和激励机制，最大限度地吸引网民在线上参与调查，确保调查活动的广泛性、代表性；三是拓宽推广渠道，利用志愿者组织和网络，组织志愿者下沉社区进行推广，拓宽推广面；四是抓好落实，跟进本地样本量的完成情况，确保按量保质完成数据采集工作。

在领导小组、组委会、承办单位、课题小组和各地参与发动单位的共同努力下，本次调查活动按计划有序推进，采集了大量的问卷数据，引起社会较大的反响，活动取得圆满成功。

四、调查样本数据的评估

经分析和评估，本次调查活动收集的数据具有以下特点：

1）调查样本数据量大，总样本数超百万级

本次调查活动收回的问卷总数为323.9805万份（主问卷+专题问卷），其中，公众网民版问卷272.9930万份，网络从业人员版问卷50.9875万份。经过数据清洗后，有效问卷总数为206.4726万份，其中，公众网民版有效问卷173.6912万份，网络从业人员版有效问卷32.7814万份。问卷总有效率为63.73%。另外，调查活动还收到网民对我国网络安全建设提出的意见和建议49.9756万条。本次调查活动受到网民的热烈响应，参与问卷调查的人数众多，采集的数

据样本规模可观，单从公众网民版主问卷的采集数量来看，总数超过108万，其中样本数据量有1个省超过25万，3个省超9万，25个省的样本数据量过万，31个省（不包括港、澳、台）的采集的问卷数量全部超过千。样本规模巨大显示网民参与度较高。

2）调查样本数据覆盖面广，基本实现区县级全面覆盖

从调查数据样本来源地来看，地区分布广泛。全国34个省、直辖市、自治区（包括港澳台），大陆地区的333个地市（区）均有数据样本分布，地市级采集覆盖率和有效覆盖率均为100%，2843个县区中除了个别县区以外其他县区均有数据样本分布，县区级地区的样本有效覆盖率达99.79%（样本覆盖县区数占计划采集县区数的比例）。另外还有小部分样本数据来自海外。样本分布的广泛度体现了调查活动有较强的影响力和辐射力。

3）调查样本数据地区分布差异仍然存在

从调查数据来源来看，虽然样本数据的分布广泛，但数据的地区分布仍有较大差异。广东、河南、陕西、黑龙江、江苏、山东、北京、河北、浙江、安徽、新疆、湖南、山西等地的组织发动工作较好，网民参与积极性较高，采集的问卷样本数据较多。总体上看样本的分布仍存在一定程度上地区差异，数据分布的均衡度略有提升，数据样本分布基本实现了县级区域全面覆盖。

为了保持各地区之间数据份量和人口基数的基本平衡，公众网民版主问卷数据在进行全国和省级数据汇总时按照统计局有关各下属区域人口占本区域人口的比例作为权重因子进行了适当的加权处理，经过加权以后，省级和全国的统计数降低了样本分布地区差异带来的影响。另外为了平衡不同人群在样本中的分布比例，对每个地市级的数据按人口构成比例进行了均衡处理。

4）调查样本数据反馈的信息内容丰富数据质量略有下降

从数据清洗的结果来看，总体样本数据有效率在63.73%左右，比去年有效率有所下降，今年有新渠道加入，有不少新人参与，占比较高，但也出现了答卷数据质量有所下降的现象。从答卷内容来看，大多数参与者都参与答题的积极性较高，采集的专题问卷数量明显提升，开放性作答的填空题方面网民提交了近50万多条意见和建议。这些意见和建议包含了丰富的内容，反映了网民的意见和诉求，也是调查数据集重要的组成部分。

综上所述，本次问卷调查数据的样本基本符合网民分布的主要特性，可以多维度、多层次地反映网民的意见，具有较高的代表性和参考价值。

附件二：调查报告致谢词

致谢词

2024年网民网络安全感满意度调查活动已顺利完成，在全国各级网信、公安、工信、市场监管等政府部门的精心指导和大力支持下，在参与调查的各机构和团队的共同努力下，调查活动取得圆满成功。调查活动结果经统计分析形成了本调查报告。调查报告的编制得到有关各方的指导和支持，课题组对有关参与各方的机构和人员表示衷心感谢。

感谢各发起单位、组委会的组织指导！（名单参看附件三、四）

感谢各牵头实施单位、承办单位、技术支撑单位的付出和贡献！（名单参看附件四）

感谢各新闻媒体、支持企业和机构的大力支持和配合！（名单参看附件四）

感谢参与调查活动的各位专家、研究人员、技术人员和工作人员的辛勤劳动！

感谢参与调查活动的公众网民和从业人员的积极参与！

2024年网民网络安全感满意度调查课题组

2024年10月

网安联微信公众号

网安联微信小程序

“网络安全共建网”官网

网安联秘书处

官网：www.iscn.org.cn

电话：020-8380 3843 / 139 1134 5288

邮箱：cinsabj@163.com