2026年7月1日

电动汽车电池新国标将施行

新华社北京4月15日电（记者**周圆、张辛欣**）记者15日获悉，工业和信息化部组织制定的强制性国家标准《电动汽车用动力蓄电池安全要求》（GB38031-2025）日前发布，将于2026年7月1日起开始实施。

本次修订内容主要有修订热扩散测试，进一步明确待测电池温度要求、上下电状态、观察时间、整车测试条件，技术要求从此前的着火、爆炸前5分钟提供热事件报警信号等，调整为不起火、不爆炸(仍需报警)，烟气不对乘员造成伤害等；新增底部撞击测试，考查电池底部受到撞击后的防护能力；新增快充循环后安全测试，300次快充循环后进行外部短路测试，要求不起火、不爆炸等。

此外，修订版本明确本标准适用于电动汽车用动力电池，即非驱动类电池不适用；完善绝缘电阻要求，增加包含交流电路电池系统绝缘电阻要求；提升挤压测试要求，增加绝缘电阻相关判定条件。

国家安全机关表彰奖励90余名群众

新华社北京4月15日电（记者**冯家顺**）记者15日从国家安全部了解到，在第十个全民国家安全教育日来临之际，国家安全机关对2024—2025年度为维护国家安全作出重要贡献的90余名群众进行了集中表彰奖励。这是自2019年以来，国家安全机关连续第7年在全国范围内组织评选、奖励举报有功人员。

这次表彰奖励中，全国共有90余名群众分别获得特别重大贡献、重大贡献或重要贡献奖励。各地国家安全机关依据反间谍法、公民举报危害国家安全行为奖励办法，对获奖人员给予了精神和物质奖励。

其中，来自边境地区的出租车司机老康，不顾个人安危，与境外间谍嫌疑人员英勇斗争，协助破获重大间谍案件，获得特别重大贡献奖励；来自山东的影视从业者小王，及时发现重大失泄密隐患并举报，获得重大贡献奖励；来自沿海地区的渔民小鲁，在海中打捞到一件境外窃密装置，获得重大贡献奖励；来自北京的大学生小徐，举报有人售卖国家秘密，协助及时消除安全风险，获得重大贡献奖励；来自辽宁的公司职员小刘，举报可疑人员窃拍军事设施，获得重要贡献奖励；来自浙江的学者老石，发现境外机构非法窃取我敏感信息数据，获得重要贡献奖励。

这90余名人民群众，来自全国各地、各行各业、各年龄段，有军人、教师、医生、工程师、公务员、学生、农民、渔民等。从16岁的中学生到70岁的退休教师，各条战线各个领域的人民群众，在总体国家安全观的指引下，心怀“国之大者”、心存国家大义、心系国家安全，自觉同危害国家安全行为作斗争，在各自平凡的岗位上，为国家安全作出了不平凡的特殊贡献。

哈尔滨市公安局公开通缉3名美国国家安全局（NSA）特工

新华社哈尔滨4月15日电（记者**熊丰**）记者15日从黑龙江省哈尔滨市公安局获悉，为依法严厉打击境外势力对我网络攻击窃密犯罪，切实维护国家网络空间安全和人民生命财产安全，哈尔滨市公安局决定对3名隶属于美国国家安全局（NSA）的犯罪嫌疑人凯瑟琳·威尔逊（Katheryn A. Wilson）、罗伯特·思内尔（Robert J. Snelling）、斯蒂芬·约翰逊（Stephen W. Johnson）进行通缉。

前期，“2025年哈尔滨第九届亚冬会”遭受境外网络攻击事件经媒体报道后，引发广泛关注。国家计算机病毒应急处理中心和亚冬会赛事网络安全保障团队，及时向哈尔滨市公安局提交了亚冬会遭受网络攻击的全部数据。哈尔滨市公安局立即组织技术专家组成技术团队开展网络攻击溯源调查。在相关国家支持下，经技术团队持续攻坚，成功追查到美国国家安全局（NSA）的3名特工和两所美国高校，参与实施了针对亚冬会的网络攻击活动。

经技术团队层层溯源，此次针对亚冬会开展网络攻击是由美国国家安全局（NSA）精心组织实施的一次网络攻击行动，实施此次网络攻击行动的组织是美国国家安全局信息情报部（代号S）数据侦察局（代号S3）下属特定入侵行动办公室（Office of Tailored Access Operation，简称“TAO”，代号S32）。美国国家安全局特定入侵行动办公室为了掩护其攻击来源和保护网络武器安全，依托所属多家掩护机构购买了一批不同国家的IP地址，并匿名租用了一大批位于欧洲、亚洲等国家和地区的网络服务器。

调查发现，美国国家安全局（NSA）赛前攻击行为主要集中在亚冬会注册系统、抵离管理系统、竞赛报名系统等重要信息系统，这些系统用于赛前开展相关工作，保存有大量赛事相关人员身份敏感信息，美国国家安全局（NSA）意图利用网络攻击窃取参赛运动员的个人隐私数据。从2月3日第一场冰球比赛开始，美国国家安全局（NSA）网络攻击达到高峰，此时攻击重点方向为赛事信息发布系统（包括API接口）、抵离管理系统等，此类系统为赛事过程保障的重要信息系统，美国国家安全局（NSA）妄图破坏系统，扰乱影响亚冬会赛事的正常运行。同时，美国国家安全局（NSA）针对黑龙江省内能源、交通、水利、通信、国防科研院校等重要行业开展网络攻击，意图破坏我关键信息基础设施引发社会秩序混乱和窃取我相关领域重要机密信息。

美国国家安全局（NSA）主要围绕特定应用系统、特定关键信息基础设施、特定要害部门开展网络渗透攻击，涵盖数百类已知和未知攻击手法，攻击方式超前，包括未知漏洞盲打、文件读取漏洞、短时高频定向检测攻击、备份文件和敏感文件及路径探测攻击、密码穷举攻击等，攻击目标、攻击意图明显。技术团队还发现，亚冬会期间美国国家安全局（NSA）向黑龙江省内多个基于微软Windows操作系统的特定设备发送未知加密字节，疑为唤醒、激活微软Windows操作系统提前预留的特定后门。

经持续攻坚溯源，哈尔滨市公安局成功锁定了参与网络攻击亚冬会的美国国家安全局（NSA）3名特工。进一步调查发现，该3名特工曾多次对我国关键信息基础设施实施网络攻击，并参与对华为公司等企业的网络攻击活动。技术团队同时发现，具有美国国家安全局（NSA）背景的美国加利福尼亚大学、弗吉尼亚理工大学也参与了本次网络攻击。公开信息显示：加利福尼亚大学自2015年起就被美国国家安全局（NSA）和国土安全部指定为网络防御教育领域的学术卓越中心。弗吉尼亚理工大学是美国6所高级军事院校之一，曾在2021年接受美国国家安全局（NSA）资助，用于加强网络攻防的队伍建设。该学校是美国国家安全局（NSA）认证的“网络安全防御研究中心”和“网络安全作战研究中心”，长期参与美国国家安全局（NSA）资助的联邦奖学金项目。此外，该校还承建了弗吉尼亚州政府的网络攻防靶场建设。

哈尔滨市公安局表示，请广大群众积极提供线索，凡向公安机关提供有效线索的举报人，以及配合公安机关抓获有关犯罪嫌疑人的有功人员，公安机关将给予一定金额的奖励。

4月14日，医务人员展示儿童用磁悬浮双心室辅助装置。 新华社 发

我国儿童用磁悬浮“人工心”植入成功

新华社武汉4月15日电（记者**闫睿、乐文婉**）华中科技大学同济医学院附属协和医院15日对外宣布，该院心脏大血管外科主任董念国团队，近期将历时3年自主研发的儿童用磁悬浮双心室辅助装置，成功植入一名7岁终末期心衰患儿体内。患儿在“人工心”辅助下，心肺功能平稳恢复。

这一单泵只有45克重的磁悬浮技术装置的成功应用，意味着在低龄、低体重患儿体内构建起稳定的血液循环系统，突破了第一代、第二代儿童机械循环辅助的“禁区”，也为心衰儿童的治疗提供了中国“心辅助”方案。

儿童心脏衰竭是医学界长期面临的难题。终末期心衰患儿亟需心脏移植。患儿等不到合适供心，则需要通过人工辅助装置暂时承担心脏泵血功能，为心肌修复争取时间。“现有设备多针对成人设计。低于30斤的患儿因体重低、胸腔狭小等限制，长期处于无第三代泵可用的困境。”董念国说。

团队历经多轮理论推演与实验验证，将装置迭代至第三代磁悬浮技术，重量压缩至45克，泵体直径缩至2.9厘米。据介绍，该装置在性能上有三重突破：能耗降低，电池续航长；稳定性更强，能满足患者紧急转运等需求；转速更精准，为1500-3600转/分钟。还可根据患儿实时循环支持需求进行调节，避免过度泵血导致功能损伤。

2021年，武汉协和医院心脏大血管外科团队联合深圳核心医疗科技股份有限公司，启动了针对低龄低体重患儿的磁悬浮心室辅助装置研发项目，致力于填补儿童机械循环辅助领域的空白。该项目由武汉协和医院牵头，获国家重点研发计划专项支持，同时联动国内外19家医疗机构开展多中心临床研究。