

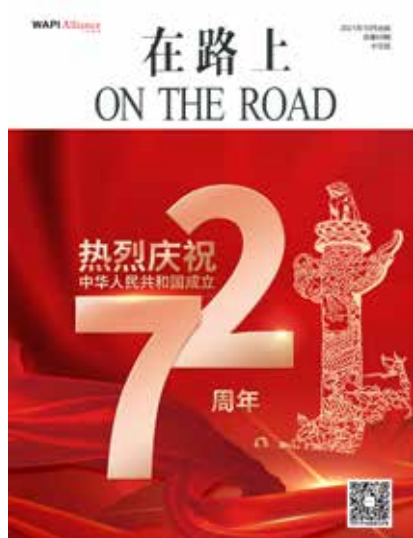
在路上 ON THE ROAD

热烈庆祝
中华人民共和国成立

72

周年





WAPI产业联盟

理 事 长： 曹 军

秘 书 长： 张璐璐

《在路上 On The Road》编辑部

主 编： 张璐璐

编 辑： 周 园 刘 婷 简 练
王立华 肖 非 刘剑昕

美术编辑： 周 园

WAPI产业联盟秘书处

会员服务部 标 准 化 部 市场与产业部
测试实验室 综合管理部

联络单位

ISO/IEC JTC1/SC6中国对口委员会
工业和信息化部宽带无线IP标准工作组

联系方式

地 址： 北京海淀区知春路27号量子芯座1608室

邮 编： 100191

电 话： 010-82351181

传 真： 010-82351181 ext.1901

邮 箱： wapi@wapia.org zhouy@wapia.org

网 站： <http://www.wapia.org.cn>

公众号：



WAPI产业联盟公众号

理事成员：

中国移动通信集团公司

中国电信集团有限公司

中国联合网络通信集团有限公司

国家密码管理局商用密码检测中心

国家无线电监测中心检测中心

北大方正集团有限公司

北京中电华大电子设计有限责任公司

北京六合万通微电子科技股份有限公司

广州杰赛科技股份有限公司

西电捷通无线网络通信股份有限公司

深圳市明华澳汉科技股份有限公司

媒体聚焦 Media Focus

- 05 通信世界等：发挥创新联合体作用 WAPI产业联盟组织开发WLAN快速切换CPE
- 07 飞象网等：服务命脉行业关基建设 WAPI产业联盟推出便携式网络运维检查工具
- 09 中国电子报/电子信息产业网等：ISO/IEC JTC1/SC6第43次全会及工作组会议闭幕
中国代表团多项提案取得进展

特别报道 Special Report

- 12 国家密码管理局牛路宏：守正创新 高起点建设高质量商用密码检测认证体系
- 16 详解：《铁路无线电管理办法》
- 20 规范管理 满意服务：WAPI产业联盟连续第十一年通过质量管理体系认证

联盟关注 Alliance Concerns

- 21 《关键信息基础设施安全保护条例》与WAPI行业发展研究
- 28 联盟人谈标准创新系列（四）周 园：浅谈如何以平台推动团体标准创新和应用

政经要闻 Policy News

- 34 习近平：中国支持中关村开展新一轮先行先试改革
- 34 习近平：让数字文明造福各国人民
- 35 国务院：对关键信息基础设施实行重点保护
- 35 国务院：扩大科研项目经费管理自主权 加大科研人员激励力度
- 36 《关键信息基础设施安全保护条例》：关基运营者8大必须做
- 36 国家市场监管总局：深化改革，促进检验检测行业做优做强
- 37 肖亚庆：繁荣开源生态，打造开放、公平、公正、非歧视的数字经济发展环境
- 37 田玉龙：推进工业和信息化领域密码应用向纵深发展
- 37 张工：标准化是推动可持续发展的有效途径
- 38 中共北京市委：强化联盟的标准规范和引领作用 建设全球数字经济标杆城市
- 38 北京市科委：北京市高新技术企业认定实行“报备即批准”
- 38 北京市经信局：推动新基建标准化建设，支持核心技术攻关
- 39 范一飞：切实加强数据治理和信息保护
- 39 刘家义：以标准引领提升助力新时代现代化强省建设
- 39 方滨兴：人工智能赋能网络攻击安全威胁的应对策略

联盟工作 Alliance Work

- 40 WAPI产业联盟等5家联盟获批成立流动党员联合支部
- 41 联盟积极响应中关村联合护航行动 新增开放2个共性技术平台1项产业研究
- 42 跨界合作：WAPI产业联盟与中国智慧能源产业联盟协同创新基础网络安全
- 43 WAPI产业联盟支持香河智慧家居产业安全创新发展， 参加 “科技促进香河智慧家居产业引领与提升对接交流会”
- 44 WAPI产业联盟召开2021年第三次标准工作及项目组会议（总第119次）
- 46 WAPI产业联盟团体标准《GB/T 39786 实施指南：无线局域网密码应用基本要求》正式立项
- 47 西电捷通公司便携式WAPI无线接入鉴别综合网关 通过联盟测试
- 48 广西线材厂WAPI系列产品通过联盟测试

新成员 New Member

- 49 恩智浦（中国）管理有限公司加入WAPI产业联盟

成员与市场 Member & Marketing

- 50 中国电科院：提升工作效率 完成变电站巡检机器人检测
- 50 中兴通讯上半年营收情况可喜
- 51 华大电子首次发布数字人民币钱包芯片
- 51 新华三：致力做政府数字化变革 “背后的力量”
- 52 工信部：2023年网络安全产业规模将超过2500亿元
- 53 全国医疗机构网络信息安全管理办法将出台
- 55 美国NSA警告公共网络是黑客攻击的温床

WAPI 产业应用论坛 WAPI Forum

- 56 浅谈2021版无线局域网设备测试规范

通信世界等：

发挥创新联合体作用 WAPI产业联盟组织开发WLAN快速切换CPE

【编者按】日前，结合物联网市场应用需求，WAPI产业联盟组织成员开发了WLAN快速切换CPE，该产品可有效解决此前传统的客户端前置设备（CPE）无法满足无线局域网相邻无线接入点（AP）间毫秒级切换的难题，实现了移动高清视频等业务无间断、不卡顿、实时传输。2021年9月7日，通信世界网、中国电子报/电子信息产业网、飞象网等媒体，对此进行了规模报道。

以下是通信世界的报道。



日前，结合物联网市场应用需求，WAPI产业联盟组织成员开发了WLAN快速切换CPE，该产品可有效解决此前传统的客户端前置设备（CPE）无法满足无线局域网相邻无线接入点（AP）间毫秒级切换的难题，实现了移动高清视频等业务无间断、不卡顿、实时传输。



图：WAPI快速切换CPE，正在各命脉行业广泛使用

当前WAPI安全无线局域网在各行业广泛应用，类似巡检机器人、移动视频监控等应用场景对无线传输提出了低延时、高速率、高可靠的需求。这些业务终端移动过程中要在不同AP间进行切换，由于涉及物理层无线信道秒级切换，会不可避免地造成数据包丢失，从而导致传输的视频出现延时增加、卡顿、长时间停滞等情况。

针对这一问题，联盟组织西电捷通公司、深圳市瑞科慧联科技有限公司、深圳市智开科技有限公司、广西电力线路器材厂有限责任公司等成员单位进行了WLAN快速切换CPE的开发工作。通过深入研究WLAN快速切换协议技术和工程化实现技术，改进了CPE底层的无线发现及信号强度识别过程，能根据实时监测到的关联AP和相邻AP的无线信号强度变化，优化调整切换阈值及算法。通过上述，突破性地实现了CPE在AP间毫秒级切换，保障了视频传输的实时性、连续性、可靠性。

目前，联盟多家厂商已率先推出WAPI快速切换CPE产品，联盟测试实验室也同步增加了配套测试项目，为市场用户产品选型提供可靠依据。

部分媒体新闻链接：

通信世界：<http://www.cww.net.cn/article?id=490912>

中国电子报/电子信息产业网：<http://www.cena.com.cn/infocom/20210907/113043.html>

飞象网：<http://www.cctime.com/html/2021-9-7/1589062.htm>

飞象网等：

服务命脉行业关基建设 WAPI产业联盟推出便携式网络运维检查工具

【编者按】日前，结合关键信息基础设施运营者对WAPI网络运行状态和质量检查的需求，WAPI产业联盟快速开发了便携式WAPI网络运维检查工具，可满足场站等应用环境下的WAPI网络现场检查，为WAPI网络更大规模部署提供支撑。该产品具有“便携性强、可单人操作、功能全面、检查时不影响正常业务”等特点。2021年9月8日，飞象网、中国电子报/电子信息产业网、通信世界等媒体，对此进行了规模报道。

以下是飞象网的报道。



日前，结合关键信息基础设施运营者对WAPI网络运行状态和质量检查的需求，WAPI产业联盟快速开发了便携式WAPI网络运维检查工具，可满足场站等应用环境下的WAPI网络现场检查，为WAPI网络更大规模部署提供支撑。

近年来WAPI因产业成熟度高、不增加采购成本、建设配套条件丰富、对行业的信息通道安全 and 数据资产安全能形成有效保护，越来越受到用户的青睐，已广泛服务政务、国防、公安、海关、能源、交通等命脉行



图：便携式WAPI网络运维检查工具示意图

业，支持这些行业建成了安全自主可控、向网络化智能化数字化发展的关键信息基础设施。最近有用户单位向WAPI产业联盟提出：在行业WAPI网络系统的日常运维和定期检查中，需要更加专业的小型化现场检查工具。结合用户需求，联盟迅速组织成员单位开发出便携式WAPI网络运维检查工具，具有“便携性强、可单人操作、功能全面、检查时不影响正常业务”等特点，及时消除了用户网络运维检查中的“梗阻”，发挥了联盟创新联合体的作用和优势。

目前该产品已成为网络运营者开展WAPI无线局域网现场巡检和日常运维检查的“利器”。帮助用户在检查中实时判定WAPI网络的工作状态、安全隐患和管理配置要求的偏离度等等。尤其在应急故障排查的时候，十分有利于快速确认网络运行状态、定位问题并快速修复。

该产品采用可背负式设计，方便检查人员轻松携行；采用硬质EVA箱体，兼顾了现场作业的安全性；自主供电模块，可提供10小时的不间断工作能力；采用领先的自动化测试技术，可通过非介入式手段对无线局域网运行状况进行检查，有效规避了检查作业时对网络及其业务运行造成不必要的影响或导入可能存在的风险。目前产品检查能力包括：网络部署合规性检查、安全配置差异度检查、安全接入可用性检查等。

作为产业公共支撑和服务平台，WAPI产业联盟紧密贴合市场需求，不断创新测试工具，支持用户WAPI测试能力建设，目前已形成完备的WAPI关基行业应用测试解决方案，相关产品包括：测试项目全面准确、测试颗粒度高的WAPI安全协议检测系统、适用于工程现场的WAPI网络验收测试工具箱、便携式WAPI网络运维检查工具等等。

部分媒体新闻链接：

飞象网：<http://www.cctime.com/html/2021-9-7/1589020.htm>

中国电子报/电子信息产业网：<http://www.cena.com.cn/infocom/20210907/113038.html>

通信世界：<http://www.cww.net.cn/article?id=490894>

中国电子报/电子信息产业网等：

ISO/IEC JTC1/SC6第43次全会及工作组会议闭幕

中国代表团多项提案取得进展

【编者按】2021年8月20日至9月10日，国际标准化组织（ISO）和国际电工委员会（IEC）第一联合技术委员会（JTC1）第六分技术委员会（SC6）第43次全会及工作组会议以网络会议方式召开，来自奥地利、加拿大、中国、日本、韩国、西班牙、瑞典、瑞士、英国、美国等10个国家成员体以及ITU-T、IEEE、ECMA、NFC论坛等联络组织的40余位专家参加了会议。中国代表团方面，来自无线网络安全技术国家工程实验室、WAPI产业联盟和无线网络安全标准化委员会的多位专家参会，会议成果显著。中国电子报/电子信息产业网、通信世界、飞象网等媒体，对此进行了报道。

以下是中国电子报/电子信息产业网的报道。



2021年8月20日至9月10日，国际标准化组织（ISO）和国际电工委员会（IEC）第一联合技术委员会（JTC1）第六分技术委员会（SC6）第43次全会及工作组会议以网络会议方式召开，来自奥地利、加拿大、中国、日本、韩国、西班牙、瑞典、瑞士、英国、美国等10个国家成员体以及ITU-T、IEEE、ECMA、NFC论坛等联络组织的40余位专家参加了会议。中国代表团方面，来自无线网络安全技术国家工程实验室、WAPI产业联盟和无线网络安全标准化委员会的黄振海、张璐璐、简练、李琴、李玉娇、高波、郑骊等专家参会。

本次会议历时3周，包括SC6团长/召集人会议、三个常设工作组（WG1、WG7、WG10）及三个临时工作组会议、决议起草委员会会议和SC6第43次全会，讨论了包括近场通信接口协议（NFCIP）、低空无人机区域



网络（LADAN）、射频定向信号传输控制协议（RF-DST）、确定性无线工业网络（DWIN）、可穿戴机器人域网络（WRAN）、未来网络（架构、协议和机制）、递归网络互连架构和协议、无线局域网接入控制、区块链网络互连技术、抽象语法标记（ASN.1）、对象标识符（OID）解析系统等在内的30余项标准项目及其他议题，会议成果显著。

在国际标准技术提案推进方面，由中国电信、WAPI产业联盟、西电捷通和新华三于2020年5月立项的“无线局域网接入控制”（ISO/IEC 5021-1和ISO/IEC 5021-2）两项提案进入委员会草案（CD）投票阶段；由重庆邮电大学牵头制定的“未来网络服务质量”（ISO/IEC 21558-2和ISO/IEC 21559-2）即将开始国际标准草案（DIS）投票，会议预授权根据WG7中期会议讨论情况启动最终国际标准草案（FDIS）投票；其他由中国代表团主导/参与的多项提案也均有不同程度的进展。

在国际标准生态环境建设方面，由中国提出并获批成立的概念和术语咨询组（AG2）及可信赖特设组（AHG2）在上一研究周期成果显著，SC6批准AG2和AHG2继续按照职责范围开展工作，李琴和李玉娇继续担任AG2及AHG2召集人；黄振海在全会做SC27标准化联络报告，并继续被任命为SC6到SC27联络员；黄振海、李玉娇参加决议起草委员会会议，获全会决议致谢。

在持续推动SC6管理提升方面，中国代表团根据ISO/IEC导则条款新变化，在会前向团长/召集人会议提交了“周期复审实践行动建议”提案，该提案旨在促进SC6将已发布国际标准复审工作纳入日常工作序列，并促进针对已发布的国际标准复审投票给出具体指导和建议。SC6管理层一致认为该提案具有重要意义，SC6全会批准成立“周期复审流程”咨询组来讨论和输出委员会建议及指导，黄振海、李琴、李玉娇成为该咨询组的创

始成员。

ISO/IEC JTC1/SC6是信息技术领域国际标准化组织重要的分技术委员会，其技术方向为系统间远程通信和信息交换，专注于开放系统之间信息交换领域的技术研究和标准化，涵盖国际标准化组织提出的开放系统互连（OSI）七层模型，是全球网络空间系统信息通信的基础。我国在SC6已开展了多项国际标准制修订和技术研究工作：在WG1开展了无线局域网、近场通信、局域网安全、访问控制、传感器网络安全架构等多项国际标准的研究制定工作；在WG7正牵头制定无线局域网接入控制相关国际标准，以及未来网络架构、协议和机制体系中服务质量相关国际标准；在WG10正积极推进实体证书管理和对象标识符（OID）相关国际标准新提案。

部分媒体新闻链接：

中国电子报/电子信息产业网：<http://www.cena.com.cn/infocom/20210914/113122.html>

通信世界：<http://www.cww.net.cn/article?id=491154>

飞象网：<http://www.cctime.com/html/2021-9-14/1589952.htm>

国家密码管理局牛路宏：

守正创新 高起点建设高质量商用密码检测认证体系

中国信息安全

2020年1月1日,《中华人民共和国密码法》正式施行,明确提出国家推进商用密码检测认证体系建设,为商用密码检测认证工作指明了方向,提供了根本遵循。商用密码检测中心作为经市场监管总局和国家密码管理局批准的全国唯一一家商用密码认证机构,深入贯彻落实习近平总书记重要指示批示精神和《密码法》相关要求,立足发展实际,借鉴相关领域成熟做法和先进经验,为商用密码检测认证体系建设贡献积极力量。

一、商用密码检测认证体系的重要意义

进入全面建设社会主义现代化强国的新历史时期,商用密码在维护国家安全、促进经济社会发展、保障人民群众利益等方面发挥着越来越重要的作用,商用密码治理体系和治理能力面临新形势与新挑战,建设商用密码检测认证体系对贯彻落实新发展理念,推动商用密码进入高质量发展快车道具有重要意义。

建设商用密码检测认证体系是落实国务院“放管服”改革要求,服务商用密码管理重塑的重要举措。贯彻落实《密码法》,重塑商用密码管理,检测认证体系建设是重要组成和关键环节。从行政许可管理向检测认证体系转变,有效加强事中事后监管,实现商用密码管理“放”与“管”的有机衔接,也是“放管服”改革的要求。作为国家质量管理体系的一项基本制度,检测认证利用技术手段对商用密码产品和服务进行技术把关、质量控制,为行政执法提供公正数据和技术支持,政府从“前台”转入“后台”,进一步放宽市场准入,促进行政职能转变,推进供给侧结构性改革,激发市场活力和社会创造力,创新商用密码发展,规范商用密码管理。

建设商用密码检测认证体系是引导商用密码从业单位提质升级,增加商用密码高质量供给的发展需要。通过检测认证手段,保障商用密码产品、服务符合相关技术标准规范,引导商用密码从业单位加强技术升级迭代,不断提升产品、服务质量,全面提升供给能力,实质高质量发展。商用密码检测认证采用强制性认证和国推自愿性认证相结合的方式,充分发挥强制性认证的“保底线”作用,对涉及国家安全、国计民生、社会公共利益的商用密码产品及使用相关设备的服务进行强制性认证,把安全风险降到最低;以国推自愿性认证“拉高线”,引导消费和采购,形成有效的市场选择机制,促进商用密码企业提升产品和服务质量,推动“产品”向“精品”转变,增加优质供给。

建设商用密码检测认证体系是优化商用密码营商环境,推动商用密码产业繁荣发展的有效手段。检测认证提供独立公正、专业可信的评价信息,向市场和社会传递质量与信用信号,引导市场优胜劣汰,从源头把关,规范市场秩序。在商用密码产业发展中,针对现有产品和服务,检测认证评价信息引导市场调节和政府调控;

围绕新兴技术和产业发展需求，检测认证积极促进新兴产品标准研究，努力打造高水准、一站式的检测认证服务平台，促进新产品研发、生产和应用，为商用密码产业结构升级和有序发展提供有力支撑。

二、商用密码检测认证体系的总体部署

商用密码检测认证体系按照高质量发展的要求，以制度机制建设为统领，以标准建设、机构建设、力量建设为重点，全面推进产品认证、服务认证和管理体系认证能力建设，大力服务并促进商用密码产业发展和改革创新。

（一）规划检测认证体系建设目标

建立科学完备、公正权威、先进高效的商用密码检测认证体系，覆盖商用密码产品、服务和管理体系。检测认证法律法规和标准体系健全，形成市场机制为主导、政府加强事中事后监管的运行机制，推动检测认证与产业发展深度融合；密码检测分析基础理论研究取得原创性成果，突破一批密码检测认证核心关键技术，研制一批适应新技术新应用发展以及检测认证工作需求的检测认证工具，以科研创新驱动检测认证发展；培育一批操作规范、技术能力强、服务水平高、规模效益好的检测认证机构，建成多层次、高水平的检测认证专业队伍，构建完备的检测认证基础设施，推动检测认证服务做强做优做大。

（二）构建检测认证制度体系

自 2019 年 10 月 26 日《密码法》颁布至今，在市场监管总局、国家密码管理局领导下，初步建立商用密码检测认证制度体系，为检测认证实施提供根本遵循。

开展顶层设计。2019 年 12 月至 2020 年 5 月，市场监管总局会同国家密码管理局陆续发布《关于调整商用密码产品管理方式的公告》（第 39 号）、《关于开展商用密码检测认证工作的实施意见》（国市监认证〔2020〕50 号）、《商用密码产品认证目录（第一批）》和《商用密码产品认证规则》，取消“商用密码产品品种和型号审批”制度，建立国家统一推行的商用密码认证制度，坚持“统一管理、共同实施、规范有序、保障安全”的基本原则，明确市场监管总局、国家密码管理局以及检测认证机构等各方职责分工，为商用密码检测认证体系奠定制度基础。

修订规章制度。落实党和国家要求、贯彻《密码法》精神、适应新时代商用密码事业发展，国家密码管理局组织对《商用密码管理条例》进行修订，并面向社会征求意见。条例征求意见稿落实《密码法》规定的推进商用密码检测认证体系建设，鼓励商用密码从业单位自愿接受商用密码检测认证，明确检测、认证机构资质审批条件、程序及其从业规范，细化检测认证体系的管理要求和运作机制。

完善标准规范。标准是检测认证科学性、权威性、规范性和有效性的根本依据和技术基础。按照共性先立、急用先行的原则，稳步推进密码标准制修订工作，形成了具有自主知识产权的 SM 系列国产算法及相关密

码技术标准和规范。目前国家密码管理局已发布密码行业标准 115 项，推进发布密码国家标准 39 项，覆盖密码算法、密码芯片、密码设备、密码应用中间件、密码系统、密码检测等的密码标准体系基本建立，为商用密码检测认证实施提供了有力的标准支撑。

（三）布局检测认证力量

建设国家密码管理局一手抓机构布局，一手抓能力建设，双管齐下，稳步推进商用密码检测认证体系建设工作。

建设商用密码检测认证机构。立足商用密码发展实际，我国积极构建“1+M+N”的商用密码检测认证体系，即设立 1 家商用密码认证机构、M 家商用密码产品检测机构和 N 家商用密码应用安全性评估机构。围绕产业需求，综合考虑地理因素，目前我国设立认证机构 1 家（商用密码检测中心）；产品检测机构 4 家，分布在北京、深圳、上海和成都等地；密评机构 48 家，分布在北京、天津、上海、杭州、广州、乌鲁木齐、郑州等地，商用密码检测认证队伍日益壮大。

强化商用密码检测认证能力。经过二十余年的深耕细作，我国密码检测基础理论、关键技术、工具平台、运行机制等方面都取得新突破，多项成果达到国际先进水平，商用密码检测能力大幅提升。以安全芯片检测能力建设为关键突破口，逐步建成覆盖芯片、板卡、整机、系统等 22 类密码产品的检测能力；在探索和实践建立完善的电子认证服务系统安全性测评和信息系统密码应用安全性评估工作机制，积极推进相关测评工作，很好地满足了商用密码管理和产业发展的检测评估需要。

三、商用密码检测认证工作的实施成效

自《密码法》实施以来，商用密码检测认证工作立足发展实际，积极开展工作，在商用密码产品检测认证方面取得了阶段性成果。初步建成国推商用密码产品认证实施体系。根据市场监管总局和国家密码管理局联合公告要求，依据《商用密码产品认证规则》，立足认证工作实际，商用密码检测中心制定发布 22 类商用密码产品的认证实施细则，明确认证模式和认证实施流程，作为认证规则的配套文件，共同指导国推产品认证工作的开展。完成型号审批机制向检测认证体系的平稳过渡。《密码法》实施后，原“商用密码产品品种和型号审批”行政许可调整为检测认证制度。为确保商用密码产品管理工作平稳有序衔接和过渡，2020 年 7 月 1 日前圆满完成有效期内的《商用密码产品型号证书》换发《商用密码认证证书》工作，共换发证书 1876 张；此前尚未完成的型号审批，申请单位可自愿转为认证申请；审批期间已经开展的审查及检测，认证机构不再重复审查、检测。有序开展检测认证工作。依据《商用密码产品认证规则》，有序开展产品认证工作；按照密码应用安全性评估要求，不断探索推进密评试点。截至 2021 年 6 月 30 日，累计完成产品检测 3000 余款（含型号审批制度阶段），累计发放认证证书 2528 张（含换发证书）；对 1000 多个高安全等级的重要信息系统进行了密

码应用安全性评估，有效引导了商用密码企业提质升级，丰富产品供给，保障了商用密码在重要信息系统和关键信息基础设施中的安全合规应用。

四、商用密码检测认证发展的未来展望

新时代商用密码发展面临新形势、新挑战和新问题，商用密码检测认证体系建设将重点围绕以下目标继续推进。一是制度体系更加完善。依据《密码法》和《商用密码管理条例》，加快构建科学规范、系统完备、运行高效的法规体系，完善检测认证规则，加强检测认证机构和人员管理，规范检测认证活动。按照共性先立、急用先行的原则，跟踪密码技术和密码应用发展，大力推进密码检测认证标准的制修订，不断适应商用密码产业和应用发展新需求。二是检测认证机构能力全面提升。持续提升检测认证技术能力，突破检测认证关键核心技术，丰富密码检测认证工具，优化完善检测认证手段，提高检测认证技术水平和服务质量。加强检测认证人才培养，聚焦高层次领军人才和紧缺急需人才，坚持引进和培养并重，打造一支结构合理、素质优良、业务精湛的创新人才队伍。三是商用密码产品、服务和管理体系认证全面开展。建立完善的商用密码检测认证体系，促进商用密码市场健康有序发展。强化国推商用密码产品认证体系建设。推动建立商用密码服务国推自愿认证制度，稳妥开展服务认证。研究探索并适时推动商用密码管理体系认证。针对商用密码新产品、新应用、新业态、新模式，探索开展自愿性检测认证活动。四是服务产业发展、应用促进、密码管理的作用更加突出。以服务为宗旨，以需求为导向，推动检测认证在商用密码优质供给，推动密码与新兴技术的融合应用，保障密码应用的合规、正确、有效。增强检测认证服务的全面性、针对性、专业性和有效性，为行政执法监管提供公正数据和技术支持，提升政府监管的可靠性和公信力。推进商用密码检测认证体系高质量建设和发展，责任重大，使命光荣。商用密码检测中心将深入学习贯彻习近平新时代中国特色社会主义思想，深入贯彻落实《密码法》相关要求，在国家密码管理局的领导下，携手商用密码产业和应用各方，守正创新，积极奋进，为建设科学完备、公正权威、先进高效的商用密码检测认证体系，服务国家安全和经济社会发展作出新的更大贡献。

作者牛路宏，系国家密码管理局商用密码检测中心主任。

详解：《铁路无线电管理办法》

中国无线电杂志

近年来，随着铁路事业的发展，尤其是高铁技术的快速发展，无线电频谱资源作为铁路行业的生产要素，在铁路通信、自动化、安全等领域发挥着越来越重要的作用。早期一些铁路无线电管理规定和工作机制随着铁路事业的发展变化与铁路管理机构的改革，已不适应当前的管理需要。为此，工业和信息化部、交通运输部联合颁布了《铁路无线电管理办法》（工业和信息化部 交通运输部第56号令）（以下简称《办法》），将于2021年10月1日起施行。为更好地宣传和实施《办法》，现对《办法》进行详细解读。

一、制定《办法》的必要性

（一）制定《办法》是贯彻落实《中华人民共和国无线电管理条例》的需要

2016年颁布实施的《中华人民共和国无线电管理条例》（以下简称《条例》），明确了国家无线电管理机构和国务院有关部门的无线电管理机构之间的业务指导关系。国务院有关部门的无线电管理机构在国家无线电管理机构的业务指导下开展工作，其在无线电管理方面的具体工作要遵守《条例》的规定。国务院有关部门的无线电管理机构主要是指公安、民航、广播、铁路、渔业等部门为开展本系统（行业）无线电管理工作而设立的机构。国务院有关部门的无线电管理机构具体职责包括：贯彻执行国家无线电管理的方针、政策和法律、行政法规、规章；依照《条例》规定和国务院规定的部门职权，管理国家无线电管理机构分配给本系统（行业）使用的航空、水上无线电专用频率，规划本系统（行业）无线电台（站）的建设布局和台址，核发制式无线电台执照及电台识别码。

在无线电台（站）管理方面，《条例》明确由国务院有关部门的无线电管理机构核发船舶、航空器、铁路机车设置、使用的制式无线电台执照及电台识别码，并要求国家无线电管理机构会同国务院有关部门制定船舶、航空器、铁路机车设置、使用非制式无线电台的管理办法。为贯彻落实有关规定，进一步规范铁路无线电管理，保障铁路系统无线电业务安全，国家无线电管理机构会同交通运输部制定关于铁路无线电管理的部门规章，对铁路无线电频率使用和制式、非制式无线电台（站）设置、使用管理加以规范。

（二）制定《办法》是适应铁路无线电管理情况变化的需要

1994年，国家无线电管理委员会发布《加强国务院各部门无线电管理的若干规定》（国无管〔1994〕18号），明确了授权或委托国务院各部门无线电管理机构行使部分无线电管理职权等问题。随后，铁道部成立了无线电管理机构，负责铁路系统无线电管理工作。1996年，国家无线电管理委员会、铁道部联合发布《铁路无线电管理规则》，进一步明确了铁路各级无线电管理机构的职责等。后续，工业和信息化部、铁道部通过建立铁路无线电专用频率保护工作长效机制，大力支持铁路高速化、信息化建设，并加强对相关频率的保护性监测，切实保障铁路GSM-R、800MHz频段列车安全预警等频率的使用安全。

2013年3月，铁路系统实行政企分开改革，原铁道部拟定铁路发展规划和政策的行政职责划入交通运输部，新组建的国家铁路局由交通运输部管理，承担原铁道部的其他行政职责，部分铁路无线电管理和技术人员

划入铁路运输企业。铁路系统改革后，铁路无线电频率管理者与使用者也从合一变为分开，铁路无线电应用点多线长，跨行政区域多，台站属地管理也存在一定问题。早期铁路无线电管理相关规章已不适应当前需求，需要通过制定《办法》，对铁路无线电频率和无线电台（站）相关许可的审查程序、职责分工、无线电监测和干扰查处机制等予以明确，进而提升铁路无线电管理的依法行政水平。

二、立法过程

2016年《条例》修订公布后，工业和信息化部就启动了《办法》的起草制定，主要开展了以下工作：

一是在组织相关机构开展铁路无线电管理机制课题研究并深入总结实践经验的基础上，组织国家无线电监测中心及湖南、辽宁、上海无线电管理机构，赴国家铁路局、中国铁路集团公司、中国铁道科学研究院、上海铁路监督管理局、中国铁路集团公司上海铁路局等单位开展铁路无线电管理工作情况调研，了解铁路当前建设运营及未来发展规划，在此基础上研究起草了《办法（初稿）》。

二是多次组织国家铁路局、中国铁路集团公司等单位就铁路无线电管理思路和机制进行座谈研讨，结合无线电频率使用，无线电台（站）设置、使用以及铁路无线电监测、干扰查处等实际业务需求，听取相关立法建议，修改完善《办法》。

三是根据《规章制定程序条例》相关要求，向社会公开征求意见，并多次征求国家铁路局、中国铁路集团公司、各省（区、市）无线电管理机构和国家无线电监测中心的意见，在综合各方面意见基础上，就《办法》内容于2020年9月和12月两次书面征求交通运输部意见，经协调达成一致意见。

2021年3月23日，工业和信息化部第4次部务会审议通过了《办法》，并经交通运输部联签同意，6月30日，两部门联合颁布出台了《办法》。

三、主要内容

《办法》进一步贯彻落实《条例》要求，依法依规加强铁路无线电频率使用和无线电台（站）设置、使用相关行政许可的审查、无线电监测和干扰查处等工作，明确了铁路相关无线电频率使用许可委托制度，无线电台（站）设置、使用审批分工制度以及建立完善无线电干扰查处机制等，有利于相关部门厘清权责、理顺关系，强化铁路无线电管理，保障铁路运行安全。主要规定了以下内容：

（一）明确铁路无线电管理职责分工

落实《条例》关于国务院有关部门的无线电管理机构职责的相关规定，《办法》明确由国家无线电管理机构委托国家铁路局实施相关无线电频率、无线电台（站）许可。

关于铁路无线电相关行政许可的实施，一是依授权实施许可。《条例》修订后，授权国务院有关部门的无线电管理机构履行相关职责，以自己的名义行使相关职权，并承担相应的法律责任。其中，在铁路机车上设置、使用制式无线电台，由国务院有关部门的无线电管理机构负责核发无线电台执照及电台识别码；关于非制式无线电台具体的管理要求，《条例》授权国家无线电管理机构、国务院有关部门共同制定相关的管理办法。二是依委托实施许可。《中华人民共和国行政许可法》第二十四条规定，行政机关在其法定职权范围内，依照法律、法规、规章的规定，可以委托其他行政机关实施行政许可。《办法》按照相关要求规定，部分无线电频

率以及在铁路机车上设置、使用非制式无线电台的许可由国家无线电管理机构委托国家铁路局实施。根据《中华人民共和国行政许可法》的相关要求，国家无线电管理机构将另行发布委托国家铁路局实施行政许可的公告，详细列明委托行政许可的具体事项及相关内容。

（二）细化铁路无线电频率使用和管理规范

《办法》明确了国家无线电管理机构、国家铁路局和省级无线电管理机构的无线电频率使用许可审批管理权限。考虑到铁路无线电业务的特殊性，《办法》规定国家无线电管理机构委托国家铁路局对专门用于铁路运营指挥调度、列车运行控制等涉及铁路运营安全的无线电频率进行许可管理，这也符合当前国家深化行政审批制度改革、加强“放管服”等有关要求。《办法》对铁路无线电频率使用许可证载明事项、频率使用许可期限及续办、频率收回制度等内容进行了规定，要求铁路运输企业依法使用无线电频率，减少对铁路枢纽和相邻线路等区域的无线电干扰。

《办法》规定，国家铁路局根据委托实施许可的无线电频率的频率占用费，由国家铁路局收取并上缴国库。无线电频谱资源是属于国家所有的非传统自然资源，也是国家战略性稀缺资源；一方面，无线电频谱资源是航空、铁路、水上等国民经济重要行业赖以发展的基础资源；另一方面，无线电频谱资源的开发利用也带来巨大的经济效益。无线电频谱资源有偿使用制度是基于国家对战略性稀缺资源进行有效管理而产生和制定的，是国家开展无线电频谱资源管理工作的基本制度，是实现国有资源有效管理和提高无线电频谱利用效率的有效途径。依据《条例》规定，任何使用无线电频率的组织和个人都应当按照国家有关规定缴纳无线电频率占用费。

（三）明确无线电台（站）设置、使用审批分工

基于制式无线电台在使用性质上的特殊性，根据《条例》规定，《办法》明确国家铁路局对在铁路机车上设置、使用的制式无线电台（站）实施许可；在铁路机车上设置、使用的部分非制式无线电台（站），由国家无线电管理机构委托国家铁路局实施许可，其他无线电台（站）由无线电管理机构负责审批。为了便于掌握各类电台的使用情况，国家铁路局应当将制式无线电台执照及无线电台识别码核发情况定期通报国家无线电管理机构。

无线电台（站）是无线电管理的重要内容之一，设置有固定台址的无线电台（站），需要占用特定的物理空间（依托建筑物或独立设置），如果无线电台（站）或其周边建筑物设置不当，可能会导致区域内电磁环境恶化、通信效能下降，甚至对其他正在合法使用的无线电台（站）产生有害干扰。因此，台站建设布局既要遵守无线电管理相关规定，又要符合城乡规划。《办法》明确，国家铁路局牵头规划用于运营指挥调度、列车运行控制等涉及铁路运营安全的无线电台（站）的建设布局和台址，做好台站周边的电磁环境监测和保护工作。此外，由于无线电台（站）使用一定年限后设备会自然老化，可能会导致发射频率、发射功率、天线增益、天线高度等技术指标出现偏差，干扰其他正常使用的合法台（站）。《办法》要求无线电台（站）设置、使用人加强日常管理和维护，保证无线电台（站）性能指标符合国家无线电管理相关规定和铁路有关技术标准要求；必须对台（站）设施和设备进行合理的维护，保证其本身正常工作需要的同时，有效避免对其他合法无线电台（站）产生有害干扰。

（四）细化无线电发射设备管理规范

《办法》要求，研制铁路无线电发射设备使用的无线电频率应当符合国家无线电频率划分规定。我国无

无线电频率划分规定反映了当今世界无线电技术的发展趋势、无线电业务应用情况，反映了与国际频率划分的一致性及遵守国际电信联盟《无线电规则》的要求。只有严格按照我国无线电频率划分规定研制出的设备才具备投入使用的条件，才能确保在后续生产、销售、使用环节技术管理上的一致性，预防出现干扰。同时，按照我国无线电频率划分规定来研制无线电发射设备，可确保产品与国际主流无线电技术发展方向一致，便于我国无线电产品向国际推广，是保障我国相关产业可持续发展的重要基础。

无线电发射设备广泛应用于社会生活的各个领域，抓好无线电发射设备的管理，是从源头上防止和减少无线电干扰、维护电波秩序的重要手段。《办法》规定，销售需要取得型号核准的铁路无线电发射设备，应向省级无线电管理机构办理销售备案。除了免许可的微功率短距离无线电发射设备以外，在型号核准制度的基础上，加强对销售应当取得型号核准的无线电发射设备的单位或企业的管理，加大打击销售未经型号核准无线电发射设备的力度，避免和减少不合规、不合法的无线电发射设备流入市场。

《办法》明确，研制、生产、销售和维修大功率铁路无线电发射设备，应采取措施有效抑制电波发射，不得对依法设置、使用的无线电台（站）产生有害干扰。在研制、生产、销售和维修大功率无线电发射设备时，即使符合无线电频率划分规定，由于时域、空域以及发射方向和仰角等因素，无线电发射设备产生的电磁辐射也可能对合法的无线电台（站）产生有害干扰，此种情况严重扰乱空中电波秩序，影响其他合法无线电设备的正常使用，应采取措施有效抑制电波发射，避免发生相关干扰。

（五）完善铁路无线电监测和干扰查处机制

《办法》要求分别在国家和省级层面建立铁路无线电频率保护工作机制，由无线电管理机构、铁路管理机构和有关铁路运输企业参加。在实际工作中，2010年，工业和信息化部、铁道部就建立了铁路无线电专用频率保护工作长效机制，部分省级无线电管理机构和地方铁路局也建立了相应工作机制，加强了对铁路无线电频率的保护，确保铁路运行安全畅通。随着无线电技术的快速发展和广泛应用，电磁环境日益复杂，无线电干扰时有发生，影响铁路无线电业务安全，加强铁路无线电监测和干扰查处工作十分重要。《条例》规定，国务院相关部门的无线电监测站负责对本系统（行业）的无线电信号实施监测，国务院有关部门应加强无线电监测设施建设，成立相应的监测机构，由其负责对本系统（行业）的无线电信号实施监测，确保无线电信号在频率、功率、使用目的等方面与频率许可、设台许可相一致，避免对其他合法无线电应用产生影响。同时，当本系统（行业）合法使用的无线电台（站）受到影响时，应具备初步监测的能力。

《办法》明确，铁路部门、铁路运输企业应加强无线电管理基础设施、技术设施和队伍建设，增强监测能力和干扰源查找能力，在受到干扰时及时自查。铁路部门和省级无线电管理机构在规划建设无线电监测网（站）时，统筹考虑铁路行业使用的无线电频率保护需要。无线电管理机构和无线电监测站做好日常无线电监测和干扰查处工作，及时处理铁路方面的投诉。铁路系统合法设置、使用的无线电台（站）如果受到有害干扰，可以向无线电管理机构投诉，无线电管理机构将根据《无线电干扰投诉和查处暂行办法》相关规定，及时组织相关技术机构进行监测定位，依法查找、处置相关干扰，并将查处情况向投诉人进行反馈。考虑到铁路无线电业务的专业属性，《办法》还规定，省级无线电管理机构可以与地区铁路管理机构联合开展行政执法，进一步强化铁路无线电领域事中事后监督管理。

规范管理 满意服务

WAPI产业联盟连续第十一年通过质量管理体系认证

WAPI产业联盟 周 园



2021年8月，WAPI产业联盟（中关村无线网络安全产业联盟）再度以优异成绩通过GB/T19001-2016 idt ISO 9001:2015质量管理体系认证评审，这也是联盟连续第11年在质量管理体系认证工作中获得“优秀”评价。目前联盟经上述质量管理体系所认证的业务范围包括：与无线网络和网络安全接入技术相关的“学术交流、技术研发、成果转化、产业研究、咨询培训、国际交流及测试服务”。

WAPI产业联盟是国内首家自成立之日起秘书处采用专职人员、不依托任何单位独立运作的新型社会组织和协同创新载体，自2006年成立之初就建立了专职化、专业化的秘书处，制订了“立足产业，标准引领，技术标准研制与产品验证同步进行，产业与市场互为促进和谐发展”的工作方针，为产业和成员提供规范高效的服务。2011年，为规范自身业务和运行管理，WAPI产业联盟主动探索并尝试用国际质量管理体系实施联盟业务管理和内部管理。经过11年的自我要求和持续打磨，联盟秘书处已依据“积极创新、服务产业，开拓进取、持续改进”的质量方针，养成了“重策划、讲规矩、按流程、强落实、擅风控、持续改进”的工作规范和工作作风，产业和市场服务能力持续提升。

依据质量管理要求，WAPI产业联盟随时关注本领域生态环境变化和成员服务需求变化，结合变化校正自身的管理和服 务。在日常工作中，注重本行业组织特色、强化风险意识、加强事前防范、加强学习型组织建设，创新和服务成绩获政府、企业、市场的高度认可。2019年，WAPI产业联盟荣获5A级中国社会组织。

截至2021年9月，在标准化方面，联盟已组织制定（参与制定）并发布（获发布）了137项标准，包括：国际标准(ISO/IEC) 14项，欧洲标准3项，国家标准41项，国家军用标准4项，行业标准7项，团体标准68项；在产业成果转化方面，WAPI在全球已实现了百亿级芯片产量，芯片已达500多个型号，移动终端和网络侧设备等已超过17000款，在政务、军队、海关、金融、能源、交通、医疗、教育等行业广泛应用，有效保护了这些重要行业领域的网络安全和数据资产不受侵害。

《关键信息基础设施安全保护条例》与WAPI行业发展研究

WAPI产业联盟 简 练

【编者按】网络安全是共同的而不是孤立的。新《标准化法》、《密码法》等，已明确了要走“安全自主可控、国产化”的发展路线。2021年7月30日，国务院发布《关键信息基础设施安全保护条例》（以下简称《条例》），并于9月1日正式施行。《条例》是我国针对关键信息基础设施安全保护的专门性行政法规，也是指导国家网络安全保障工作的基础性行政法规，旨在通过配套立法进一步明确关键信息基础设施安全保护的具体要求，保障国家关键信息基础设施安全。《条例》的发布和实施标志着我国网络安全保护进入了以关键信息基础设施安全保护为重点的新阶段。

综合上述法律及条例，经研究分析WAPI产业联盟得出如下结论：在各行各业开展无线局域网（WLAN）关键信息基础设施建设中，只有符合WAPI国家标准的产品才符合法律要求，才符合行业自身的根本利益。使用Wi-Fi不仅涉嫌违法，也必将置我国命脉行业的生产办公于极大安全风险隐患中。以下是与此相关的相关政策和行业发展研究，供参考。

一、《条例》出台背景

2017年6月1日，《中华人民共和国网络安全法》（以下简称《网络安全法》）正式生效施行。作为我国网络安全的基本法，《网络安全法》提出了网络安全法治的基本制度框架，主要包括国家网络安全战略、关键信息基础设施保护制度、网络安全等级保护制度、个人信息保护制度等。其中，关键信息基础设施保护是《网络安全法》规定中的核心制度。在《网络安全法》第三章“网络运行安全”中，以“关键信息基础设施的运行安全”共计9条（第三十一至三十九条）对关键信息基础设施安全保护的基本要求、职责分工履行义务和采取措施等方面作了基本法层面的总体制度安排，并规定关键信息基础设施的具体范围和安全保护办法由国务院制定。

关键信息基础设施是国家重要的战略资源，关系国家安全、国计民生和公共利益，具有基础性、支撑性、全局性作用，保护关键信息基础设施安全是国家网络安全工作的重中之重。出台实施《条例》是完善我国网络空间治理，强化关键信息基础设施安全保护，维护国家安全和利益发展的应时应势之举，意义重大，影响深远。

世界各国高度重视关键信息基础设施安全，美欧等通过立法或发布政策文件将关键基础设施安全的网络安全保护提升到国家安全战略层面。围绕关键信息基础设施安全的网络攻防已成为国家间战略博弈的重要领域和网络空间高强度对抗的主战场。

习近平总书记在网络安全和信息化工作座谈会上指出，“金融、能源、电力、通信、交通等领域的关键信息基础设施是经济社会运行的神经中枢，是网络安全的中中之重，也是可能遭到重点攻击的目标.....我们必

须深入研究，采取有效措施，切实做好国家关键信息基础设施安全防护。”习近平总书记的重要指示为我们开展关键信息基础设施安全保护工作指明了方向。

《条例》的出台实施，是践行习近平总书记关于网络强国的重要思想，贯彻党中央、国务院重大决策部署的重要举措，是落实网络安全法有关要求，完善我国关键信息基础设施安全保护工作的法治保障，也是网络空间领域贯彻总体国家安全观，应对当前国际形势新变局，维护网络空间主权安全的应有之义。

二、《条例》内容要点

《条例》坚持总体国家安全观和习近平总书记关于网络强国的重要思想，坚持安全发展、改革创新、问题导向的指导方针，坚持综合协调、分工负责、依法保护，充分发挥行政法规的引领和推动作用，加快推进关键信息基础设施安全保障体系建设。具体来说，《条例》主要内容有以下几个亮点：

一是明晰了关键信息基础设施的定义，并按照抓重点、保关键的思路，围绕关键、信息、基础这三个要素科学界定了关键信息基础设施的范围。

关键信息基础设施是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。这是我国网络安全保护的重中之重，是各行各业安全生产的基础，保关键信息基础设施就是保国家安全。

其中能源、电信等关键信息基础设施是其他行业和领域关键信息基础设施安全保障的重要基础和支撑，具有极端重要性，是安全保护的重中之重。《条例》针对能源、电信等关键信息基础设施首次提出了“优先保障”要求，同时强调“能源、电信行业应当采取措施，为其他行业和领域的关键信息基础设施安全运行提供重点保障。”

二是明确了保护工作部门职责，在充分考虑重点行业、领域业务及网络安全需求的特殊性、专业性的前提下，将行业领域主管监管部门明确为关键信息基础设施安全保护部门，组织领导和监督管理本行业、本领域关键信息基础设施安全保护工作。

三是强化了运营者安全管理责任，切实保障人财物投入，为安全保护工作的物质基础提供了法律保障。《条例》特别强调建立“一把手负责制”，明确了运营者主要负责人负总责。运营者应当设置专门安全管理机构，配备相应人员和运行经费，并按《条例》规定开展网络安全检测、风险评估、网络产品和服务采购以及重大事件、重大威胁、设施变化等信息报告工作。应配合国家相关部门开展的安全检测、检查等工作。

四是规定了国家保障和促进措施。《条例》明确了建立网络安全信息共享机制、完善监测预警和应急体系、组织开展检查检测、能源和通信服务优先保障、加强安全保卫和防范打击违法犯罪、出台相应标准指导规范等6个方面的保障措施。为体现国家重点支持，《条例》从人才培养、财政金融、技术创新、产业发展、军民融合、表彰奖励、宣传教育等7个方面提出了促进措施。

五是确立了监督管理体制。《条例》规定，在国家网信部门统筹协调下，国务院公安部门负责指导监督关键信息基础设施安全保护工作；国务院电信主管部门和其他有关部门依照本条例和有关法律、行政法规的规

定，在各自职责范围内负责安全保护和监督管理工作；省级人民政府有关部门依据各自职责对关键信息基础设施实施安全保护和监督管理。

三、关于落实《条例》要求，提升关键信息基础设施安全保护能力水平的几点思考

“安全是发展的前提，发展是安全的保障”。《条例》的发布，促进了网络安全在信息化建设中话语权和地位的不断提升，未来网络安全产业发展空前提速。如何落实《条例》要求，有以下几点思考：

一是强化意识，深刻认识关键信息基础设施安全保护工作的重要性。从事关键信息基础设施运营和保护工作的单位和个人应充分意识到，做好关键信息基础设施安全保护工作不仅事关自身系统安全和业务稳定运行，更关乎国计民生，要深刻认识到确保关键信息基础设施安全的极端重要性，站立高位、保持清醒、敢于担当、勇于作为，以国家网络安全为己任，严格落实相关法律、政策、制度的要求。

二是摸清家底，精准掌握关键信息基础设施安全运行情况。掌握关键信息基础设施安全运行的网络和数据资产信息，是国家主管监管部门和保护工作部门开展指导监督工作的重要前提；对于运营者而言，更是落实主体责任，加强防护工作的必要手段。一方面，应全面梳理关键信息基础设施网络产品和服务情况，在掌握关键信息基础设施网络资产的基础上，进一步梳理组件级的型号信息、配置设置信息等，支撑供应链网络攻击发生后的快速定位和准确研判。另一方面，应厘清关键信息基础设施承载的数据资产，梳理数据采集、加工、传输情况，分析数据流动条件和路径。此外，对于涉及控制类系统的关键信息基础设施，应在上述措施基础上，重点加强分析识别，最大限度地掌握触发或可能触发控制动作的协议、指令情况，以及可能触及核心控制设备、系统的数据流及具有操作权限的人员情况。

三是提升能力，全面加强关键信息基础设施安全防护。运营者应重点从脆弱性和风险隐患自查自纠、安全事件和威胁分析研判、极端极限情况下关键信息基础设施的持续稳定运行等能力入手，加强相应的手段建设，逐步培养网络安全专业队伍，注重防护措施有效性的检验评价，强化网络安全防护持续运营理念；对于网络安全学术界、企业、研究机构而言，应针对关键信息基础设施的特殊性、重要性，以风险识别、评估、防范、化解为关注重点，从理论、方法、技术多个层面加强研发攻关，为关键信息基础设施安全防护提供技术支撑。

四是制定标准，加快建设关键信息基础设施安全标准体系。法律法规只会列举几条或几款主要要求，但往往很难穷尽，更重要的是规定相应的保护制度，明确主管部门。后续由主管部门建立和实施保护制度，并组织制定标准，在标准中提出具体的安全要求。而落实这些标准，特别是落实安全保护方面的基础标准、主要标准，才能算是真正意义上落实了《条例》的责任义务要求。

五是全面贯通，合力推动关键信息基础设施安全保护工作。一方面，《条例》中的信息共享、监测预警、应急处置、检查检测等措施需要各有关部门进一步体系化、制度化、常态化推动完善；另一方面，《条例》中对运营者“采购网络产品和服务可能影响国家安全的”情况的相关要求与国家网络安全审查制度一脉相承，运营者应在落实网络安全审查、保障关键信息基础设施供应链安全的工作过程中进一步提升主动性。

四、WAPI与关键信息基础设施安全保护

网络安全是共同的而不是孤立的。无论《网络安全法》、《密码法》、《标准化法》，还是上述《条例》，都已明确了要走安全自主可控、国产化的发展路线，更明确了具体要求。落实关键信息基础设施保护制度，需要国家关键信息基础设施安全保护主管部门、保护工作部门、运营者、产业群体、社会组织、科研机构等各个层面通力合作，共筑国家网络安全屏障。

安全自主可控的无线网络是现下各命脉行业的“关基建设刚需”。在无线局域网（WLAN）关基建设中，只有符合WAPI国家标准的产品才符合法律要求，才符合行业关键信息基础设施的根本利益。使用Wi-Fi不仅涉嫌违法，也置各命脉行业的生产办公于极大安全风险隐患中。

无线局域网是各行各业关键信息基础设施建设普遍采用的建网方式，具有高带宽、高性价比、组网便利等特点。目前全球无线局域网技术已形成相对统一的技术体系，但在安全方面只有两条路线：一个是美国主导的Wi-Fi安全技术802.11i，另一个是采用了国产密码技术的国家标准WAPI（无线局域网鉴别与保密基础结构）。WAPI因产业成熟度高、不增加采购成本、建设配套条件丰富、对行业的信息通道安全和数据资产安全能形成有效保护，越来越受到用户的青睐，已广泛服务政务、国防、公安、海关、能源、交通、医疗、教育等行业，支持这些行业建成了安全自主可控、向网络化智能化数字化发展的新型信息基础设施。越来越多行业在制定标准时已明确要求：本行业的专用无线局域网（WLAN）通信模块，应符合GB 15629.11系列国家标准、应使用WAPI安全机制。

在协同各行各业WAPI关基建设过程中，WAPI产业联盟针对用户对WAPI技术和产品的需求，本着抓住“标准”和“检测”牛鼻子的思路，发挥了社会组织公共技术平台“小平台解决大问题”的作用：

第一、在关基标准方面，联盟已发起并组织产业群体共同制定了《关键信息基础设施无线局域网》系列团体标准。该系列标准，在整体架构设计上，既包括普遍适用于关基行业无线局域网建设的《通用要求》，也包括针对不同行业特定需求的《行业扩展要求》，兼顾了标准体系的统一性、通用性、扩展性以及行业的特殊性和定制化。具体涉及到每个垂直行业，又通过“技术要求”和“测试方法”两类标准，为安全无线局域网应用部署和行业产品/机具的合规好用提供了标准化依据。

第二、在关基检测服务方面，联盟测试实验室密切贴合市场需求，严格依据国家标准和团体标准，提供无线局域网鉴别与保密基础结构（WAPI）协议测试、互操作测试、整改咨询测试、系统测试等。上述测试具有WAPI测试项目更加全面准确、测试颗粒度更高、定制化更强的特点，有效解决了当前市场上WAPI检测能力局限于“行政许可合规性质”，无法有效满足各命脉行业开展WAPI关基建设中的精细化和定制化测试需求的问题。并在诸如WAPI与11ac、WAPI与11ax，WAPI协议完整性检测等方面，具有突出优势。因此联盟出具的测试报告已被关基建设单位广泛采信，作为其WAPI项目采购依据。此外，联盟还密切关注国内检测机构的市场化转型需求和机构改革前瞻性发展需求，密切关注一些重要行业用户基于设计、建设、验收、运行监督检查一体化的管理考虑，提供包括但不限于“WAPI检测能力建设与提升、技术扩展和设备升级、咨询、培训”等服务。

第三、作为我国首家专注于网络安全且最具规模的产业联盟，WAPI产业联盟的目标非常清晰：就是要

实打实地解决网络安全卡脖子问题，把WAPI等国家自主可控的网络安全技术，通过标准化产业化的手段，服务市场应用。协同各行各业构建安全可控的信息基础设施，支撑和保障我们国家的网络安全。在过去的15年间，WAPI产业联盟持续关注无线网络和网络安全技术的原始创新和标准化工作，相关网络安全技术创新已覆盖无线局域网、物联网、有线以太网、无线个域网、电子标签、同轴双向网络、传感器网络、有线局域网、无线城域网、未来网络、磁域网络等领域。已开展了170余项标准的制修订，已发布（获发布）国际标准（ISO/IEC）14项、欧洲标准3项，国家标准41项，国家军用标准4项，行业标准7项，团体标准68项，为构建最基础最共性的网络安全架构体系提供有效支撑。2021年，联盟依据《关键信息基础设施安全保护条例》等法律法规要求，结合能源交通等命脉行业的安全自主可控以太网（TLSec）、安全虚拟专用网（TISec）、安全无线局域网（WAPI）关基需求，已开展了有关共性技术平台建设和服务。

关键信息基础设施安全保护条例划重点： 关基运营者八大必须要做的事

2021年9月1日，《关键信息基础设施保护条例》（以下简称条例）正式施行，关键信息基础设施运营者（以下简称运营者）在关键信息基础设施安全保护中承担主体责任，必须要做到以下八件事，以符合条例规定避免相关处罚。

（一）落实一把手责任制，重视关键信息基础设施安全保护制度建设

运营者应当建立健全网络安全保护制度和责任制，保障人力、财力、物力投入。运营者的主要负责人对关键信息基础设施安全保护负总责，领导关键信息基础设施安全保护和重大网络安全事件处置工作，组织研究解决重大网络安全问题。

处罚：对运营者未建立健全网络安全保护制度和责任制的，由有关主管部门依据职责责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处10万元以上100万元以下罚款，对直接负责的主管人员处1万元以上10万元以下罚款。

（二）设置专门安全管理机构，负责关键信息基础设施安全保护工作

运营者应当设置专门安全管理机构，并对专门安全管理机构负责人和关键岗位人员进行安全背景审查。专门安全管理机构具体负责本单位的关键信息基础设施安全保护工作，履行职责包括建立健全网络安全管理、评价考核制度，拟订关键信息基础设施安全保护计划；组织推动网络安全防护能力建设，开展网络安全监测、检测和风险评估；制定本单位应急预案，定期开展应急演练，处置网络安全事件；认定网络安全关键岗位，组织开展网络安全工作考核，提出奖励和惩处建议；组织网络安全教育、培训；履行个人信息和数据安全保护责任，建立健全个人信息和数据安全保护制度；对关键信息基础设施设计、建设、运行、维护等服务实施安全管理；按照规定报告网络安全事件和重要事项。

处罚：对运营者未设置专门安全管理机构的，未进行安全背景审查的，未履行规定职责的，由有关主管部门依据职责责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处10万元以上100万元以下罚款，对直接负责的主管人员处1万元以上10万元以下罚款。

（三）必须“给人给钱给权”，做好关键信息基础设施安全保障

运营者应当保障专门安全管理机构的运行经费、配备相应的人员，开展与网络安全和信息化有关的决策应当有专门安全管理机构人员参与，安全保护措施应当与关键信息基础设施同步规划、同步建设、同步使用。

处罚：对运营者开展与网络安全和信息化有关的决策没有专门安全管理机构人员参与的，安全保护措施未与关键信息基础设施同步规划、同步建设、同步使用的，由有关主管部门依据职责责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处10万元以上100万元以下罚款，对直接负责的主管人员处1万元以上10万元以下罚款。

（四）网络安全检测和风险评估，每年至少一次并按要求报送情况

运营者应当自行或者委托网络安全服务机构对关键信息基础设施每年至少进行一次网络安全检测和风险评估，对发现的安全问题及时整改，并按照保护工作部门要求报送情况。

处罚：对运营者未对关键信息基础设施每年至少进行一次网络安全检测和风险评估，未对发现的安全问题及时整改，或者未按照保护工作部门要求报送情况的，由有关主管部门依据职责责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处10万元以上100万元以下罚款，对直接负责的主管人员处1万元以上10万元以下罚款。

（五）应对重大事件和重大威胁，应按规定报告保护工作部门和公安机关

关键信息基础设施发生重大网络安全事件或者发现重大网络安全威胁时，运营者应当按照有关规定向保护工作部门、公安机关报告。重大网络安全事件和威胁包括但不限于“发生关键信息基础设施整体中断运行或者主要功能故障、国家基础信息以及其他重要数据泄露、较大规模个人信息泄露、造成较大经济损失、违法信息较大范围传播等”。

处罚：对运营者在关键信息基础设施发生重大网络安全事件或者发现重大网络安全威胁时，未按照有关规定向保护工作部门、公安机关报告的，由保护工作部门、公安机关依据职责责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处10万元以上100万元以下罚款，对直接负责的主管人员处1万元以上10万元以下罚款。

（六）关键信息基础设施发生变化，应及时报告保护工作部门

关键信息基础设施发生较大变化，可能影响其认定结果的，运营者应当及时将相关情况报告保护工作部门。再有，运营者发生合并、分立、解散等情况，应当及时报告保护工作部门，并按照保护工作部门的要求对关键信息基础设施进行处置，确保安全。

处罚：对运营者在关键信息基础设施发生较大变化，可能影响其认定结果时未及时将相关情况报告保护工

作部门的，发生合并、分立、解散等情况，未及时报告保护工作部门，或者未按照保护工作部门的要求对关键信息基础设施进行处置的，由有关主管部门依据职责责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处10万元以上100万元以下罚款，对直接负责的主管人员处1万元以上10万元以下罚款。

（七）按规定采购安全可信的网络产品和服务，并签订安全保密协议

运营者应当优先采购安全可信的网络产品和服务；采购网络产品和服务可能影响国家安全的，应当按照国家网络安全规定通过安全审查；应当按照国家有关规定与网络产品和服务提供者签订安全保密协议，明确提供者的技术支持和安全保密义务与责任，并对义务与责任履行情况进行监督。

处罚：运营者采购可能影响国家安全的网络产品和服务，未按照国家网络安全规定进行安全审查的，由国家网信部门等有关主管部门依据职责责令改正，处采购金额1倍以上10倍以下罚款，对直接负责的主管人员和其他直接责任人员处1万元以上10万元以下罚款。

（八）配合国家相关部门安全检查等工作，接受相关部门提供的技术支持和协助

运营者对国家相关部门组织开展的网络安全信息共享机制工作、保护工作部门开展的关键信息基础设施网络安全检查检测工作，以及公安、国家安全、保密行政管理、密码管理等有关部门依法开展的关键信息基础设施网络安全检查工作应当予以配合。同时，运营者应接受国家有关部门和保护工作部门针对网络安全事件应对处置等关键信息基础设施安全保护工作的技术支持和协助。

处罚：运营者对保护工作部门开展的关键信息基础设施网络安全检查检测工作，以及公安、国家安全、保密行政管理、密码管理等有关部门依法开展的关键信息基础设施网络安全检查工作不予配合的，由有关主管部门责令改正；拒不改正的，处5万元以上50万元以下罚款，对直接负责的主管人员和其他直接责任人员处1万元以上10万元以下罚款；情节严重的，依法追究相应法律责任。

总之，运营者应依照《条例》和有关法律、行政法规的规定以及国家标准的强制性要求，在网络安全等级保护的基础上，采取技术保护措施和其他必要措施，应对网络安全事件，防范网络攻击和违法犯罪活动，保障关键信息基础设施安全稳定运行，维护数据的完整性、保密性和可用性。关键信息基础设施发生重大和特别重大网络安全事件，经调查确定为责任事故的，除应当查明运营者责任并依法予以追究外，还应查明相关网络安全服务机构及有关部门的责任，对有失职、渎职及其他违法行为的，依法追究责任。

最后，关键信息基础设施是网络安全的中中之重，除了运营者的主体责任和保护工作之外，也需要国家相关部门、网络安全服务机构、高校和科研机构、联盟团体等社会各界力量的共同努力，有组织有体系的开展关键信息基础设施安全保卫、保护和保障工作。

联盟人谈标准创新系列（四）

【编者按】 WAPI产业联盟是国内首家专注于网络安全且目前最具规模的产业联盟，是国家科技部首批A类产业技术创新战略联盟和国家标准委首批团体标准试点单位。15年间，联盟在推动技术产业创新和成果转化、服务市场用户和产业链需求、促进行业可持续发展等方面，开展了很多务实工作，在标准创制与实施上成果显著。2015-2017年期间，联盟承接了国家标准委委托的首批国家团体标准试点工作，当时全国入选的联盟仅有7家。其中的重要工作之一就是通过试点工作，完成国家在技术创新和团体标准方面的发展规划。

截至2021年9月，WAPI产业联盟已组织开展了170余项标准的制修订，为构建最基础最共性的网络安全架构体系提供有效支撑，其中发布（获发布）国际标准（ISO/IEC）14项、欧洲标准3项，国家标准41项，国家军用标准4项，行业标准7项，团体标准68项。基于TePA安全架构形成的14项国际标准，为我国在物联网、有线以太网、无线个域网、电子标签、同轴双向网络、传感器网络、有线局域网、无线城域网、未来网络、磁域网络等等众多领域形成了标准国际化超前布局，为解决网络安全“卡脖子”问题做出有力支撑。

今年“十四五”规划纲要全文35处40次提及标准化工作，联盟社会组织正在成为组织和开展高质量标准化工作的重要力量。因此，《在路上》开辟“联盟人谈标准创新系列”专栏，分享WAPI产业联盟秘书处专职化工作人员在标准化方面的实践与思考，也希望藉此和业界同仁多多交流。

本系列文章的版权为原作者本人所有，转载或者引用本文内容请注明来源及原作者。

周 园：浅谈如何以平台推动团体标准创新和应用

WAPI产业联盟 周 园

摘 要：新《标准化法》赋予了团体标准相应的法律地位，进一步鼓励了各界产业联盟等社会组织，根据市场和创新需要制定和采用技术要求更高的团体标准，特别是在通信技术网络安全等领域。团体标准的天然属性是“应产业市场需求而生，又服务于产业市场”。产业联盟通过搭建科学的团体标准工作平台可以推动团体标准创制、提升团体标准质量，填补本领域产业应用过程中无标可依的空白，解决标准产业市场脱节、标准滞后和标龄过长等问题，帮助企业降低研发成本、提升产品质量、提高劳动生产率，实现经济效益的增长；同时，为今后行业标准和国家标准的制修订奠定基础，抢占标准的话语权和制高点。

关键词：平台建设，团体标准，标准创新，标准应用

一、背景

2018年1月，实施了新修订的《中华人民共和国标准化法》，在本次修订中，我国的标准化体系在原有国家标准、行业标准、地方标准和企业标准的基础上新增了团体标准。^[1]这进一步鼓励了各界社会组织和产业联盟，根据市场和创新需要制定和采用技术要求更的团体标准，特别是在通信技术网络安全等领域。团体标准具有制定周期短、灵活性强的特点，可快速响应创新和市场对标准的需求。在标准管理上，对团体标准不涉行政许可，由社会组织和产业技术联盟自主制定发布，通过市场优胜劣汰。^[2]产业联盟搭建科学的团体标准工作平台可以推动团体标准创制、提升团体标准质量、促进团体标准转化和应用。

WAPI产业联盟于2006年3月7日成立，是国内首家专注于网络安全且较具规模的产业联盟，是国家首批A类产业技术创新战略联盟，国家首批团体标准试点单位，也是中关村标准化示范单位，北京市5A级社会组织。是国内首家自成立之日起秘书处采用专职人员、不依托任何单位独立运作的新型社会组织和协同创新载体。目前，WAPI产业联盟成员107家，开展了170余项标准的制修订，其中发布（获发布）国际标准（ISO/IEC）14项、欧洲标准3项，国家标准41项，国家军用标准4项，行业标准7项，团体标准68项。鉴于WAPI产业联盟标准工作的成绩，其标准工作平台具有一定的参考性，本文将以WAPI产业联盟为案例，浅析平台如何推动团体标准的创新和应用。

二、标准工作平台的构成

（一）组织架构

WAPI产业联盟标准工作平台依循GB/T 20004.1《团体标准化 第一部分：良好行为指南》要求^[3]建章建制，形成了包括决策层、协调层和编制层的三层标准化组织结构，按期推进各项工作开展。



图1：WAPI产业联盟标准化机构建设情况

1、决策层：联盟标准工作平台的决策机构为无线网络安全标准化委员会。该委员会是标准化战略与发展层面的特设组织，负责团体标准的战略规划，对与团体标准化活动相关的政策、制度和标准化文件等进行决策。

无线网络安全标准化委员会由75位来自国际、国内大专院校、科研院所、企事业单位、检验检测机构的无线网络和网络安全领域专家组成。

委员性质构成如下：

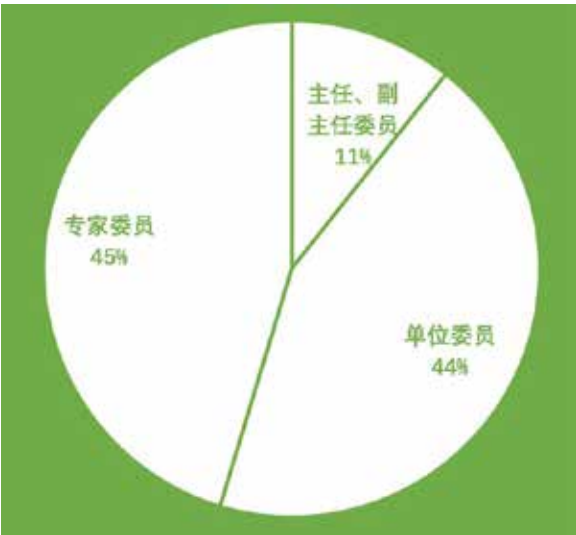


图2：无线网络安全标准化委员会委员构成

委员所在单位性质构成如下：

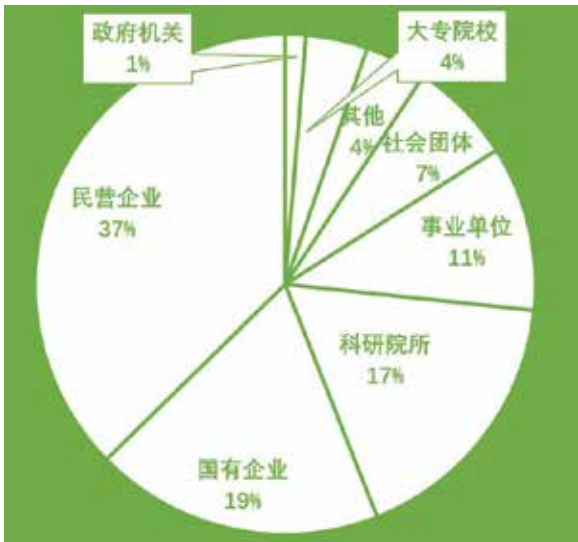


图3：无线网络安全标准化委员会委员所在单位性质构成

2、协调层：联盟标准工作平台协调层包括管理协调和技术协调两部分工作。管理协调工作由WAPI产业联盟标准化部负责，负责制定标准化工作的各项管理规章、制度和文件；管理、组织和协调联盟标准化工作，处理有关标准的制修订程序、编写规则、知识产权管理等具体事项，以及标准制定中出现的争议；开展与组织外其他单位的沟通和合作；协调和推动标准的产业化应用，促进标准国际化进程，为标准的实施提供有效支撑等。

标准委员会下设工作组，工作组是标准化工作的技术协调层。负责联盟标准化工作的计划制定、技术审查、技术协调等。

3、编制层：在工作组下设立标准项目组，由各项目组组长牵头，负责开展标准的编制工作。

（二）制度规范

联盟标准工作平台遵循《国家标准化法》、国家标准GB/T20004.1《团体标准化第1部分：良好行为指南》要求，结合十余年标准化工作实践经验，健全团体标准化相关制度，完善了团体标准化工作机制和工作文件体系，形成了《标准化工作管理办法》、《无线网络安全标准化委员会导则》等制度文件。

以下是制度文件清单节选：

序号	类别	文件名称
1	组织管理	标准化工作管理办法V3.0
2	组织管理	标准制修订业务流程V2.0
3	组织管理	无线网络安全标准化委员会导则
4	组织管理	WAPI产业联盟章程 修改稿
5	组织管理	WAPI产业联盟成员协议
6	程序规则	团体标准制修订工作程序
7	程序规则	标准文本模板
8	程序规则	项目立项建议书
9	程序规则	项目编辑单位申请表
10	程序规则	标准编制说明模板
11	程序规则	标准意见处理表
12	程序规则	无线网络和网络安全标准化委员会单位委员申请表（含保密义务说明）
13	程序规则	团体标准编写规则文件（参与制定并采纳中国标协《团体标准的结构和编写指南》）
14	知识产权	必要专利信息披露表
15	知识产权	必要专利实施许可声明表
16	知识产权	通用必要专利实施许可声明表
17	知识产权	已披露的标准清单表

表1：制度文件清单节选

三、标准工作平台的运行与管理

标准工作平台深挖产业市场需求，组织成员单位，按期、按计划开展团体标准的制修订工作。在标准推进过程中标准工作平台坚持公平、公正、公开的原则，基于“三稿三审”的标准制定流程，充分调动大专院校、科研机构、企事业单位等各方面的参与积极性，实现协商一致，在保障技术严谨性和文字严密性的基础上缩短标准制定周期，使标准及时发挥在无线网络和网络安全工作中的基础性和规范性作用。

同时联盟标准工作平台注重和创新对标准的全生命周期管理，探索引用国际标准和国家标准。自2010年起，联盟标准工作平台采用国际质量管理体系（GB/T19001—2008 idt ISO 9001:2008和GB/T19001—2016 idt ISO 9001:2015）开展标准业务管理。结合无线网络和网络安全领域的生态环境、成员需求、标准演进和可持续发展等要素，形成了相应的质量管理手册、程序文件、配套质量记录文件等。因此，标准化平台运行实现流程化、规范化；进度管理、标准审查在标准制定各个阶段发挥作用。质量管理体系保障了标准工作平台运行质量，提速团体标准创新周期，提升团体标准水平。

标准化工作的重中之重在于“人”，行业群体标准能力建设可提升团体标准综合水平。标准化人才的培养与支持已列入国务院《国家标准化体系建设发展规划（2016—2020年）》，要求加强标准化专业人才、管理人才培养和企业标准化人员培训，满足不同层次、不同领域的标准化人才需求^[4]。联盟标准工作平台通过组织会议、活动、沙龙等不同形式，定期开展团体标准培训。培训要落实的目的：一是强化团体标准在联盟内部的实施，提升成员的标准转化能力，树立一批标准实施示范项目；二是通过标准的研讨、宣贯和培训，建设、壮大标准化人才队伍。

四、依托标准工作平台 WAPI产业联盟团体标准制订和应用情况

标准工作平台致力于解决企业想做但做不了的问题，结合快速发展的市场和成员需求，组织制定了包括产品方案、互联互通、测试比对等团体标准。这些标准会将快速在联盟产业群体中实施，其中一些团体标准在经过市场验证后，被国家标准采纳，转化为国家标准。这有效的充实了国家现行标准序列、增加了标准的有效供给，提升了企业的标准竞争力。

截止至2021年6月，WAPI产业联盟共发布团体标准68项，其中41项因技术先进，与市场需求贴合度高，被国家标准采纳，转化为国家标准。国家标准转化率达60.29%。

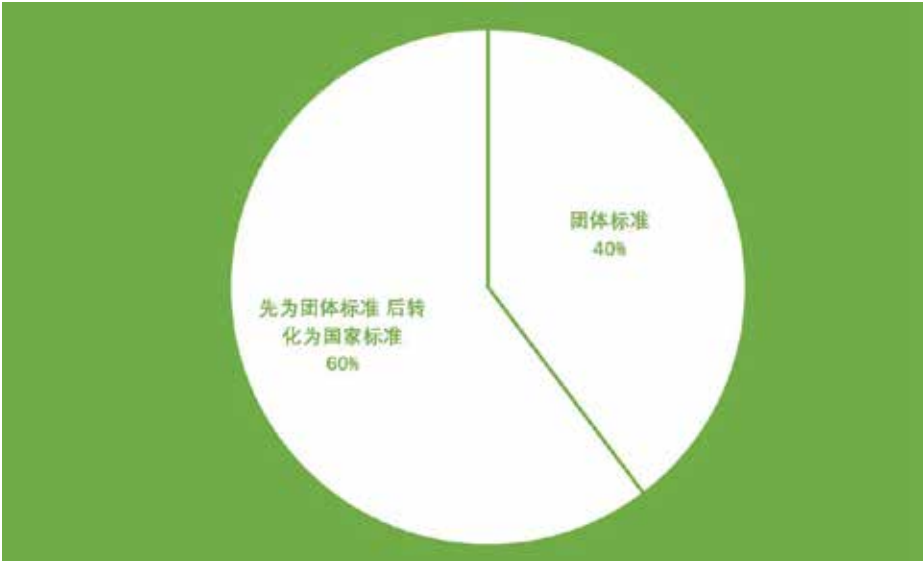


图4：WAPI产业联盟团体标准转化为国家标准转化率

依托标准工作平台，WAPI产业联盟促进技术成果转化、推进市场应用落地的经验，获得了国家标准管理部门的肯定。2015年6月，WAPI产业联盟获批成为首批国家团体标准试点单位。这对联盟的成员的意义上，畅通了以标准规范产品、有效对接市场的渠道。企业参与团体标准制修订，将进一步增加标准话语权，提高综合竞争力。标准工作平台持续开展技术融合创新、标准化与产业化互为促进工作，促进WAPI等无线网络和网络安全技术标准在相关行业、领域的市场应用。

标准的价值在于应用，市场对团体标准的接受程度是团体标准发展的关键。标准工作平台专注于无线网络和网络安全领域，所制定的团体标准均来自于产业需求，应用于市场。目前WAPI技术标准已全面产业化，覆盖从芯片设计到整机、系统集成、测试等产业链各环节。WAPI已经成为全球无线局域网芯片的标准配置。截至2021年6月，支持WAPI的无线局域网芯片超过500款型号、全球累计出货量超过170亿颗，移动终端和网络侧设备等已超过17000款，电信运营商已将WAPI作为集采网络设备支持的基本功能，除公共无线局域网外，WAPI已广泛服务于海关、金融、能源、政务、公安、交通、医疗、教育等行业，成为行业物联网的关键组成部分。^[5]

五、结语

团体标准的天然属性是“应产业市场需求而生，又服务于产业市场”。通过团体标准的制修订和转化，可填补本领域产业应用过程中无标可依的空白，解决标准产业市场脱节、标准滞后和标龄过长等问题，帮助企业降低研发成本、提升产品质量、提高劳动生产率，实现经济效益的增长；同时，为今后行业标准和国家标准的制修订奠定基础，抢占标准的话语权和制高点。

为服务好标准创新和应用，建议标准工作平台做好以下工作：

1、坚持专职化、专业化、职业化的原则，持续开展制度建设和组织运行机制建设，合理引用已有国家标准、国际标准管理团体标准，推动标准产业共同体稳定、有序、高效开展合作。

2、持续发挥平台作用，贴合市场需求及时制定、发布团体标准，以标准带动技术、产业和市场协同发展；注重团体标准对市场的规范、引导和推动作用；努力提升标准的易用性，进一步扩大标准实施范围，助推产业优化升级。

参考文献

【1】《中华人民共和国标准化法》1988年12月29日第七届全国人民代表大会常务委员会第五次会议通过 2017年11月4日第十二届全国人民代表大会常务委员会第三十次会议修订

【2】国发.[2015]13号《深化标准化工作改革方案》的通知

【3】国家质检总局,国家标准委.[2016]7号.GB/T 20004.1《团体标准化 第一部分：良好行为指南》要求

【4】国务院办公厅.《国家标准化体系建设发展规划（2016-2020年）》

【5】WAPI产业联盟.《WAPI标准产业应用及环境监测报告》202106

作者周园，系WAPI产业联盟秘书长助理/会员服务部总监 无线网络安全标准化委员会委员。

习近平：

中国支持中关村开展新一轮先行先试改革

9月24日，国家主席习近平在2021中关村论坛视频致贺中指出，当前，世界百年未有之大变局加速演进，新冠肺炎疫情影响广泛深远，世界经济复苏面临严峻挑战，世界各国更加需要加强科技开放合作，通过科技创新共同探索解决重要全球性问题的途径和方法，共同应对时代挑战，共同促进人类和平与发展的崇高事业。

习近平强调，当今世界，发展科学技术必须具有全球视野，把握时代脉搏，紧扣人类生产生活提出的新要求。中国高度重视科技创新，致力于推动全球科技创新协作，将以更加开放的态度加强国际科技交流，积极参与全球创新网络，共同推进基础研究，推动科技成果转化，培育经济发展新动能，加强知识产权保护，营造一流创新生态，塑造科技向善理念，完善全球科技治理，更好增进人类福祉。

习近平强调，中关村是中国第一个国家自主创新示范区，中关村论坛是面向全球科技创新交流合作的国家级平台。中国支持中关村开展新一轮先行先试改革，加快建设世界领先的科技园区，为促进全球科技创新交流合作作出新的贡献。

习近平：

让数字文明造福各国人民

9月26日，国家主席习近平向2021年世界互联网大会乌镇峰会致贺信中指出，数字技术正以新理念、新业态、新模式全面融入人类经济、政治、文化、社会、生态文明建设各领域和全过程，给人类生产生活带来广泛而深刻的影响。当前，世界百年变局和世纪疫情交织叠加，国际社会迫切需要携起手来，顺应信息化、数字化、网络化、智能化发展趋势，抓住机遇，应对挑战。

习近平强调，中国愿同世界各国一道，共同担起为人类谋进步的历史责任，激发数字经济活力，增强数字政府效能，优化数字社会环境，构建数字合作格局，筑牢数字安全屏障，让数字文明造福各国人民，推动构建人类命运共同体。

国务院：

对关键信息基础设施实行重点保护

国务院公布的《关键信息基础设施安全保护条例》自2021年9月1日起施行。《条例》强调了国家对关键信息基础设施实行重点保护，强调任何个人和组织不得实施非法侵入、干扰、破坏关键信息基础设施的活动，不得危害关键信息基础设施安全。明晰了关键信息基础设施安全保护的监管体制和工作机制，明确了关键信息基础设施认定的基本规则，强化了关键信息基础设施运营者的主体责任义务，构建了关键信息基础设施安全的保障、促进机制和制度。

《条例》为关键信息基础设施的安全提供了体系化保护，也为各个责任主体落实关键信息基础设施安全保护责任提供了法律依据。

国务院：

扩大科研项目经费管理自主权 加大科研人员激励力度

8月13日，国务院办公厅《关于改革完善中央财政科研经费管理的若干意见》打出的“组合拳”，主要归纳为“做加法”和“做减法”两大类。

在做加法上，在经费来源方面，分500万元以下、500万元至1000万元和1000万元以上三档，规定项目单位可以在现有基础上提升10%、10%和7%，并强调对数学等纯理论基础研究项目，提升比例可达不超过60%。在加大科技成果转化激励力度方面，从整体上提升了项目单位激励科研人员的间接费用比重，设置了更合理的奖励机制，对一些“投入大、产出周期长”的基础性项目进行有意识扶持，这释放了一个明显信号：激励不搞平均主义，要让真正有科研能力、作出了重要科研贡献的人员尝到更多甜头。强化两个“扩大”：扩大从稳定支持科研经费中提取奖励经费试点范围，试点单位从中科院所属部分研究所，扩大到所有中央级科研院所；扩大了劳务费开支范围，将项目聘用人员的住房公积金纳入劳务费科目列支，这有利于营造一种更公平公正的科研竞争合作交流氛围，极大激发科研人员全身心投入科研活动中。

在做减法上，针对科研经费使用过程中预算限制多这一屡被诟病的症结，《意见》在能放则放、应放尽放的主基调下，给出了非常具体的应对：包括：扩大预算编制自主权，抓重点、放枝节；扩大预算调剂自主权，根据各项费用的不同情况，将调增权、调剂权下放到项目单位或项目负责人。“买酱油的钱可以用来打醋，根据实际情况灵活使用。”针对科研人员抱怨较多的报销繁琐，《意见》提出，全面落实科研财务助理制度，改进财务报销管理方式，允许项目承担单位对符合条件的费用实行包干制。通过让“专业的人干专业的事”，进一步将科研人员从繁琐的报销事务中解放出来，将精力投入科研。《意见》还规定，扩大结余资金留用自主权，避免突击花钱，取消结余资金的两年使用期限，让科研单位和科研人员不必再担心“过期作废”，也将摆脱被动花钱的尴尬。

《关键信息基础设施安全保护条例》： 关基运营者8大必须做

《条例》明确，关键信息基础设施运营者在关键信息基础设施安全保护中承担主体责任，必须做到以下八件事，违反将予以相关处罚：

- (一) 落实一把手责任制，重视关键信息基础设施安全保护制度建设。
- (二) 设置专门安全管理机构，负责关键信息基础设施安全保护工作。
- (三) 必须“给人给钱给权”，做好关键信息基础设施安全保障。
- (四) 网络安全检测和风险评估，每年至少一次并按要求报送情况。
- (五) 应对重大事件和重大威胁，应按规定报告保护工作部门和公安机关。
- (六) 关键信息基础设施发生变化，应及时报告保护工作部门。
- (七) 按规定采购安全可信的网络产品和服务，并签订安全保密协议。
- (八) 配合国家相关部门安全检查等工作，接受相关部门提供的技术支持和协助。

国家市场监督管理总局： 深化改革，促进检验检测行业做优做强

9月14日，国家市场监督管理总局在《关于进一步深化改革促进检验检测行业做优做强的指导意见》中重点提出，一要坚持深化改革，推动检验检测机构市场化发展，鼓励社会资本进入检验检测行业，鼓励民营企业和其他社会资本投资检验检测服务。二要坚持创新驱动，完善检验检测创新体系，加强共性技术平台建设与关键核心技术攻关，提升自主创新能力，实现关键检验检测技术自主可控。三要坚持市场主导，激发市场活力，提升质量竞争力，完善市场要素资源供给，引导行业品牌建设，增强检验检测行业发展内生动力。四要坚持目标导向，对标国际先进水平，积极参与国际规则和标准制定，加强国际相关制度、标准和技术的跟踪研究。鼓励检验检测机构开展“一带一路”国家和地区的实验室共建、实验室间比对等业务。

肖亚庆：

繁荣开源生态，打造开放、公平、公正、非歧视的数字经济发展环境

8月2日，工业和信息化部党组书记、部长肖亚庆在2021全球数字经济大会中强调：做大做强数字经济，要加强核心技术攻关，统筹锻长板、补短板，构建自主可控、安全可靠的信息技术体系，建设高水平产业共性技术平台，繁荣开源生态。要加快建设新型数字基础设施，发展高效协同的融合基础设施，着力营造良好数字生态，保障网络安全、数据安全，携手打造开放、公平、公正、非歧视的数字经济发展环境。

田玉龙：

推进工业和信息化领域密码应用向纵深发展

8月25日，工业和信息化部党组成员、总工程师田玉龙在工业和信息化部商用密码应用推进标准工作组成立大会暨第一次全体成员会议中指出，密码是保障网络安全的核心技术和基础支撑。推进工业和信息化领域密码应用向纵深发展。要做好顶层设计，加快构建工业和信息化领域完备的商用密码应用标准体系；要坚持创新驱动，推动新兴技术与密码技术深度融合和协同创新；要坚持急用先行，围绕制造强国、网络强国战略重点领域加快急需标准研制；要汇聚工作合力，促进密码应用推进工作支撑机构积极发挥作用。

张工：

标准化是推动可持续发展的有效途径

7月28日，国家市场监管总局党组书记、局长张工在2021青岛国际标准化大会中指出，标准化是推动可持续发展的有效途径。要以标准规制维护市场公平竞争秩序，以标准引领激发市场主体活力，以标准支撑促进安全与发展，以标准联通助力构建“双循环”新发展格局。张工强调，要共商标准技术合作，助推产业创新发展；共建国际标准体系，支撑全球绿色发展；共享标准实践成果，共创健康安全未来；共聚标准合作共识，促进世界互联互通。要在统筹活力和秩序、发展和安全、国内和国际上，充分发挥标准的作用，推动经济和社会可持续、高质量发展。

中共北京市委：

强化联盟的标准规范和引领作用，建设全球数字经济标杆城市

8月3日实施的《北京市关于加快建设全球数字经济标杆城市的实施方案》提出：要打造中国数字经济发展“北京样板”、全球数字经济发展“北京标杆”，加快建设全球数字经济标杆城市。其中强调，要推动新一代信息技术和城市基础设施深度融合，建设国际领先的网络基础设施，建成新一代工业互联网。强化标准规范和引领，鼓励行业协会、产业联盟、龙头企业等主体参与各类标准制定，积极争取国家数字经济领域标准化试点建设，积极参与国际标准制定，依托“一带一路”等国际平台，加强在基础设施建设、数字化转型、国际标准化等方面的国际合作。

北京市科委：

北京市高新技术企业认定实行“报备即批准”

9月16日，北京市科学技术委员会、中关村科技园区管理委员会，北京市财政局，国家税务总局北京市税务局联合发布的《北京市高新技术企业认定“报备即批准”政策试点工作实施方案》，对在京从事集成电路、人工智能、生物医药、关键材料等领域生产研发类规模以上企业认定高新技术企业时，满足从业一年以上且在中国境内发生的研究开发费用总额占全部研究开发费用总额的比例不低于50%条件的，实行“报备即批准”。认定为高新技术企业即可按规定享受所得税优惠等相关政策，加强事中事后监管，对发现不符合高新技术企业认定标准的按有关规定进行处理。

北京市经信局：

推动新基建标准化建设，支持核心技术攻关

7月22日，北京市经济和信息化局在《关于加快新型基础设施建设支持试点示范推广项目的若干措施》中重点指出：筹建由高等院校、科研院所、相关企业组成的新型基础设施建设标准化技术委员会。围绕新型网络、数据智能、可信安全等前沿技术，鼓励制定相关国家标准、行业标准、地方标准和团体标准，促进新型基础设施的互通、融合。要围绕新型基础设施，支持研究建立各行业各领域的建设导则和工程实施规范；围绕新型网络、数据智能、生态系统、可信安全等基础设施，加强关键核心技术攻关和产业化应用。对符合条件的项目，将通过科研项目（课题）经费给予支持。

范一飞：

切实加强数据治理和信息保护

9月24日，人民银行副行长范一飞在“第十届中国支付清算论坛”上谈数据垄断、数据安全、数据治理及信息保护中强调：在数据治理及信息保护方面，要贯彻总体国家安全观，切实加强数据治理和信息保护。数据作为一种新型生产要素的重要性与日俱增，数据风险与安全问题也愈发突出。全球经贸交易、技术交流、资源分享等跨国合作日益频繁，数据跨境流动不可避免。在此背景下，数据保护与治理不仅关乎数据的开发利用与安全问题，而且与国家主权、国家安全、公共利益等休戚相关。产业各方要学好用好个人信息保护相关法律法规，要落实“信息安全”原则，保障数据安全和风险可控。

刘家义：

以标准引领提升助力新时代现代化强省建设

7月28日，山东省委书记、省人大常委会主任刘家义在2021青岛国际标准化大会中指出：山东省大力实施标准化战略，开展标准化综合改革试点，标准化工作取得了积极进展和成效。立足新发展阶段，更加需要标准化引领，更加积极地实施标准化战略，全面推动标准化创新发展，深化国际标准化合作，开拓“创新、开放、合作、共赢”的标准化发展新局面。将聚焦高质量发展，大力推动产业发展标准化，大力推动标准化与可持续化，以标准引领提升助力新时代现代化强省建设。

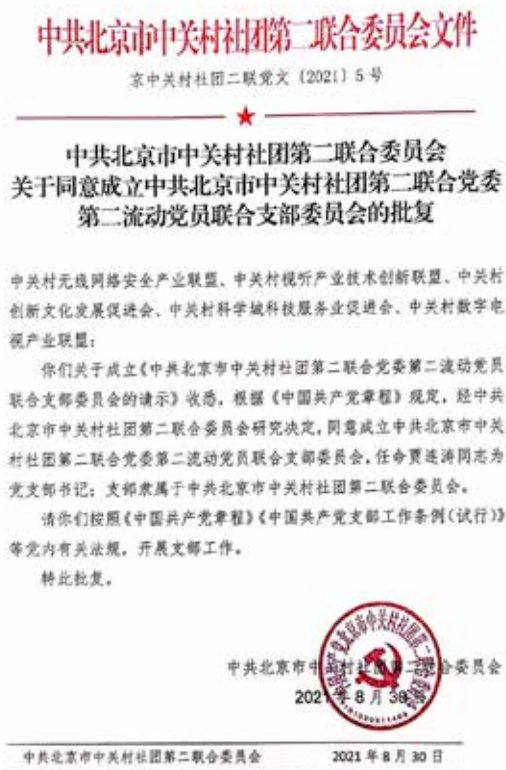
方滨兴：

人工智能赋能网络攻击安全威胁的应对策略

中国工程院方滨兴院士科研团队在中国工程院院刊《中国工程科学》2021年第3期撰文中谈到，为有效应对人工智能赋能网络攻击在政治安全、经济社会安全和国防安全三方面的安全威胁，应从防范安全威胁、构建对等能力角度加强智能化网络攻防体系建设和能力升级；要加强人工智能安全数据资产的共享利用，采取以数据为中心的人工智能网络攻防技术发展路径；要加强对抗评估和测试验证，促进人工智能网络攻防技术尽快具备实用性。建议以国家实验室等权威机构为依托，利用区块链等新型技术构建人工智能数据靶场和人工智能攻防对抗靶场，形成安全可信、激励机制合理的共享利用框架。

WAPI产业联盟等5家联盟获批成立流动党员联合支部

WAPI产业联盟 周 园



2021年8月30日，WAPI产业联盟和4家社会组织成立中共北京市中关村社团第二联合党委第二流动党员联合支部的申请获批。

WAPI产业联盟（中关村无线网络安全产业联盟）自2006年成立以来，坚决拥护中国共产党的领导，坚持以党的政治路线、中心工作和方针政策指导联盟日常工作。2021年8月20日，WAPI产业联盟、中关村视听产业技术创新联盟、中关村创新文化发展促进会、中关村科学城科技服务促进会、中关村数字电视产业联盟5家单位，向中共北京市中关村社团第二

联合委员会提出成立中共北京市中关村社团第二联合党委第二流动党员联合支部的申请。中关村社团第二联合委员会收到申请后，根据《中国共产党章程》规定，并展开调研决定：同意该申请，任命贾连涛同志为党支部书记，支部隶属于中共北京市中关村社团第二联合委员会。

WAPI产业联盟秘书处同志们表示，要更加紧密团结在党中央周围，牢记联盟初心使命，增强四个意识、坚定四个自信、做到两个维护。在党的领导下，做好网络安全创新联合体的本职工作。

联盟积极响应中关村联合护航行动 新增开放2个共性技术平台1项产业研究

WAPI产业联盟 刘剑昕

2021年8月3日，中关村产业技术联盟联合会发布“联合护航行动”资源开放清单（二十二），WAPI产业联盟的2个共性技术平台和1项产业研究报告再度名列其中。上述免费向中关村示范区企业开放的资源是：能源/电力行业无线网络安全共性技术平台、自主可控无线网络安全检测能力比对平台、自主可控安全无线局域网技术产业研究报告。

其中，能源/电力行业无线网络安全共性技术平台，重点面向该行业有安全无线网络建设需求的用户、参建厂商和集成商等，解决其关键信息基础设施建设和业务融合中的共性技术难题，迅速形成合规产品，服务规模建设。平台的服务包括但不限于：共性关键技术研发、标准创制、模拟环境搭建、相关测试等。服务贯穿能源行业关基的设计、施工、验收、监督检查等全过程。

自主可控无线网络安全检测能力比对平台，面向具备安全无线局域网（WAPI）检测能力或者有建设需求的检测机构和行业用户，关注其WAPI检测基建质量，保障其检测系统的准确性、一致性、可靠性。该平台的服务包括但不限于：共性关键技术研发、比对测试样品研发、比对测试等。平台的“公平秤”作用，也为CNAS等国家认可机构的期间核查工作提供了客观依据。

此外，联盟还围绕政府关注的“推动自主创新技术的产业化和应用，解决卡脖子”问题，围绕市

场用户希望“中立的产业组织提供安全无线局域网（WAPI）技术、产业、应用综合情况并据此开展本行业新基建”的需求，发布了《自主可控安全无线局域网技术产业研究报告》。《报告》结合联盟15年来在本领域的工作积累以及对全球无线局域网和网络安全技术产业的研究与实践，通过对产业链上下游系统详实的调研，如实呈现了自主可控安全无线局域网（WAPI）的技术、标准、产业、产品、市场、国际化等发展和演进情况，研究成果具系统性、专业性、客观性、中立性、完整性。《报告》既有较高的学术价值，也对支持市场用户开展WAPI新基建建设、企业开展技术创新和产业化实践具有指导作用。

通过开放上述平台和产业研究报告，WAPI产业联盟以实际行动服务了政府、市场用户和企业，践行了《“十四五”北京国际科技创新中心建设战略行动计划》中“前瞻部署基础研究，推进关键核心技术攻关，构建先发优势”等核心要求，发挥了联盟创新联合体的集群竞争优势。这也是联盟积极响应《中关村国家自主创新示范区发展建设规划》要求，扎扎实实“重点发展信息安全等前沿信息产业，加快构建前沿信息生态，开展行业政策研究、服务产业链协同创新和会员服务”等工作的实际体现。通过上述平台的开放，将服务全国更多企业、更多命脉行业开展安全、自主、可控新基建建设，形成立足北京（中关村）、辐射（服务）全国的创新联合优势。

跨界合作：

WAPI产业联盟与中国智慧能源产业联盟协同创新基础网络安全

WAPI产业联盟 简 练

2021年8月4日，为进一步加强能源工业互联网平台建设中的基础网络连接安全，WAPI产业联盟（中关村无线网络安全产业联盟）和中国智慧能源产业联盟（中关村智慧能源产业联盟）展开交流探讨。

据中国智慧能源产业联盟介绍，该联盟致力于打造“信息资源整合平台”、“科技创新孵化平台”、“产业应用推广平台”、“产融结合服务平台”四大服务平台，工作重点包括能源工业互联网平台建设和数据共建共享。当前，随着能源行业面临的网络安全风险在不断增加，针对能源行业的新型攻击和破坏手段也不断出现，网络安全需求也发生了新的变化。如何依据新《标准化法》、《密码法》，打造安全可控的数据链路基础网络，如何推动安全自主可控的发展路线，是能源工业互联网平台建设的核心关注。

WAPI产业联盟是国内首家专注于网络安全且目前最具规模的产业联盟，产业服务目标非常清晰：就

是要实打实地解决网络安全卡脖子问题，把WAPI等国家自主可控的网络安全技术，通过标准化产业化的手段，服务市场应用。协同各行各业构建安全可控的信息基础设施，支撑和保障我们国家的网络安全。成立15年来，WAPI产业联盟以国际领先的基础共性技术TePA和WAPI，带动无线网络和网络安全技术产业创新和健康高效发展，构建以TePA三元对等鉴别为核心的安全技术体系，落实技术标准的成果转化，组织产业群体在无线有线一体化网络和网络安全领域开展顶层设计、技术研发与标准化、产业化与应用成果转化工作，在基础网络安全解决方案方面拥有丰富经验。

交流中，中国智慧能源产业联盟和WAPI产业联盟在“网络安全是共同的而不是孤立的”方面达成高度共识，双方在能源工业互联网平台建设的基础网络连接安全、有线无线一体化、网络层安全等方面达成初步合作意向。

WAPI产业联盟支持香河智慧家居产业安全创新发展 参加“科技促进香河智慧家居产业引领与提升对接交流会”

WAPI产业联盟 简 练

2021年8月27日，为贯彻落实《北京市通州区与河北省三河、大厂、香河三县市协同发展规划》的要求，加快推进京津冀产业创新能力和业态质量的协同发展，搭建精准对接交流合作平台，通州区科学技术委员会和廊坊市科学技术局，围绕香河县未来的产业发展和家居产业在新形势下面临转型的需求，联合组织“科技促进香河智慧家居产业引领与提升对接交流会”。WAPI产业联盟（中关村网络安全产业联盟）、北京技术交易促进中心、中关村工业互联网产业联盟作为支持单位参会，共同探讨香河未来产业发展需求和香河智慧家居城创新引领与提升的科技方案。

会议由首都创新大联盟理事长陈红主持。北京市通州区科委和廊坊市科技局领导为会议致辞，香河县发改局、香河县科工局、香河县家具城发展中心、香河县经开区等相关单位领导、香河县爱依瑞斯、富都华创、御娇龙、喜临门等家具龙头企业代表分别介绍了智慧家居/家具产业集群现有情况及发展需求。首都创新大联盟主席团常务主席徐克伟就香河智慧家居创新引领与提升提出方案。

WAPI产业联盟市场总监简练围绕网络安全和各产业协同创新的工作经验和成果，分享了相关情况和体会。网络安全是共同的而不是孤立的。当前无论《网络安全法》、《密码法》、《标准化法》，还是

最新发布的《关键信息基础设施安全保护条例》，都已明确了要走安全自主可控、国产化的发展路线，明确了相关具体要求。无线局域网是各行各业关键信息基础设施建设普遍采用的建网方式，具有高带宽、高性价比、组网便利等特点。目前全球无线局域网技术已形成相对统一的技术体系，但在安全方面只有两条路线：一个是美国主导的Wi-Fi安全技术802.11i，另一个是采用了国产密码技术的国家标准WAPI（无线局域网鉴别与保密基础结构）。WAPI因产业成熟度高、不增加采购成本、建设配套条件丰富、对行业的信息通道安全和数据资产安全能形成有效保护，越来越受到用户的青睐，已广泛服务政务、国防、公安、海关、能源、交通、医疗、教育等行业，支持这些行业建成了安全自主可控、向网络化智能化数字化发展的新型信息基础设施。值得关注的是越来越多行业在制定标准时已明确要求：本行业的专用无线局域网（WLAN）通信模块，应符合GB 15629.11系列国家标准、应使用WAPI安全机制。这方面同样适用香河智慧家居产业，通过开展安全自主可控的智慧家居规划与布局，在新形势下推动提升和转型。

简练表示，WAPI产业联盟愿意根据香河以及京津冀产业创新协同发展需要，提供标准创新、技术产业创新和市场应用服务等，以实际行动去加快推进京津冀产业创新能力和业态质量的协同发展。

WAPI产业联盟召开2021年第三次标准工作及项目组会议 (总第119次)

WAPI产业联盟 刘剑昕

2021年9月16日，WAPI产业联盟2021年第三次标准工作及项目组会议以网络会议方式召开。会议包括：报告2021年第三季度技术标准产业工作、新技术/产业动态分享、讨论并审议在研标准项目、讨论拟立项项目建议、讨论标准国际化工作、标准化知识交流与培训等。来自无线网络安全技术国家工程实验室、中国电子技术标准化研究院、中国电信股份有限公司、新华三技术有限公司、华为技术有限公司、西电捷通公司、北京数字认证股份有限公司、北京华信傲天网络技术有限公司、迈普通信技术股份有限公司、深圳航天科创实业有限公司、北京神州数码云科信息技术有限公司、高通无线通信技术(中国)有限公司、瑞晟微电子(苏州)有限公司、北京紫光展锐科技有限公司、联想(北京)有限公司、北京比邻科技有限公司、广州广电计量检测股份有限公司、巷子科技(北京)有限公司、四川诚平网络科技有限公司、西安芯语慧联信息科技有限公司、南京博丰通讯科技有限公司、重庆源盾科技有限公司、四川岁月文明科技有限公司、重庆华联众智科技有限公司、江苏省电子信息产品质量监督检验研究院(江苏省信息安全测评中心)、陕西省网络与信息安全测评中心、重庆邮电大学、ISO/IEC JTC 1/SC 6国内技术对口单位、工业和信息化部宽带无线IP标准工作组等单位的代表，无线网络安全标准化委员会委员参加会议。

WAPI产业联盟市场总监简练表示，近几年来，各行业对安全的无线局域网需求旺盛。随着WLAN应用场景不断丰富、技术不断演进，WAPI产业联盟贴合行业应用需求发布多项技术标准和测试标准，



联盟测试实验室同步开展了相关检测能力建设，并不断更新无线局域网鉴别与保密基础结构(WAPI)测试项，通过标准和测试两大抓手落实创新成果转化，服务市场应用需求。作为新型科技创新联合体，在多年服务市场过程中，WAPI产业联盟紧密贴合市场需求，坚持技术规范与测试规范并重，坚持技术标准与工程化验证工作同步开展，保障了技术标准成果能够快速转化、广泛推广。

无线网络安全标准化委员会副主任委员黄振海表示，在我们标准产业共同体关注的网络通信和网络安全领域，在国际技术演进、国家引导政策、技术标准、产品支撑技术平台、产业/行业方面展现出了新的演进趋势和进展。WAPI产业在重要行业应用的步伐不断加快，关键基础技术、产品、测评技术、网络系统建设等新的标准需求不断涌现，电力网络、公共安全、铁路网络等关键信息基础设施落地取得新的进展；技术标准和法律、行政法规、部门规章、政策文件等构成的产业合规性体系，在网络建设中发挥着越来越基础的指导作用。希望大家共同努力，面向技术

演进发展，紧扣产业应用实际需求，协同做好技术标准工作，通过不同供应商的技术洞察和实践经验反馈，促进共同提升。

简练报告了第三季度标准产业市场工作及媒体宣传工作情况：国家标准GB/T 40349—2021《家用和类似用途电器专用WLAN通信模块技术规范》获发布，WAPI成必备安全能力；4项团体标准进入报批阶段，有望近期发布；19项团体标准正在不同阶段推进中，进展顺利；多家厂商十余款产品通过了联盟测试并获得测试报告；联盟发布新版测试项，为市场用户的WAPI采购、验收、监督检查等提供支撑；联盟开发了便携式WAPI网络运维检查工具，满足WAPI网络现场检查需求；外部媒体宣传与联盟自媒体双管齐下，标准宣传推广成效显著。

黄振海报告了第三季度团体标准和国际标准工作情况：在团体标准项目进展方面，完成报批待发布2项；进入报批阶段4项；完成送审稿函审12项；完成公开征求意见3项；形成草案稿4项。在标准国际化方面，SC6国内技术对口工作稳步推进，第三季度共对内流通国际提案文件77份，向国际上反馈投票/意见21份；在WG7中期会议和SC6第43次全会及工作组会议中，我国主导/参与的多项国际标准提案获推进。

在新技术/产业动态分享环节，北京数字认证股份有限公司侯鹏亮向会议介绍了国家标准GB/T 39786《信息系统密码应用基本要求》的编制工作，对该标准的编制思路及技术路线进行了详细的解读。

无线网络安全标准化委员会委员郑骊做《2021年第二次项目组集中会议要点回顾》报告。她回顾了2021年第二次项目组集中会议决议，通报了上次会议决议的执行情况。

在已立项项目讨论阶段，项目组对已立项的《GB/T 39786 实施指南：无线局域网密码应用基本要求》（草案稿）、《无线局域网安全技术规范》（草案稿）、《无线局域网系统》（第1~3部分，设计、施工、验收）（征求意见稿）、《信息技术 系统间远程通信和信息交换 原子密钥建立与实体鉴别》（第1~7部分）（送审稿）、T/WAPIA 007《无线局域网产品工程化实现指南》（4项修改单送审稿）、《信息安全技术 证书管理测试规范》（送审稿）等进行了介绍，与会专家针对上述标准进行了热烈讨论，并根据会上意见形成了相关决议。

在拟立项项目建议和讨论环节，中国电信股份有限公司高波介绍了《WAPI规模部署网络技术规范》立项建议和计划内容，会议建议提案单位进一步完善标准名称及范围，尽快提交立项申请材料。南京博丰通讯科技有限公司张庆松介绍了关于提升无线局域网物理层效率的研究方向建议，会议建议提交技术报告以便进一步讨论。

在标准国际化专题研讨环节，ISO/IEC JTC 1/SC 6国内技术对口单位秘书处李玉娇报告了2021年8—9月SC6第43次全会和工作组会议总体情况及我国主导/参与项目的推进情况，对下一步工作进行规划，并向与会专家介绍了申请注册专家的工作流程，为与会专家参与标准国际化工作提供有效信息。

在标准化知识交流与培训环节，郑骊分享了团体标准编制过程中常见的问题，结合GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草说明》对常见问题进行了解读和说明，并分享了标准分类号检索查询方式，为与会专家参与标准制修订工作提供了有效信息。

WAPI产业联盟团体标准

《GB/T 39786 实施指南：无线局域网密码应用基本要求》正式立项

WAPI产业联盟 简 练

经无线网络安全标准化委员会评审，WAPI产业联盟团体标准《GB/T 39786 实施指南：无线局域网密码应用基本要求》于日前正式立项，并面向业界公开征集参编单位。该标准是按照国家标准GB/T 39786-2021《信息安全技术信息系统密码应用基本要求》的原则和要求，为指导、规范无线局域网（WLAN）系统密码应用的规划、建设、运行、测评而制定。

2021年3月，国家市场监督管理总局、国家标准化管理委员会发布公告，正式发布了国家标准GB/T 39786-2021《信息安全技术信息系统密码应用基本要求》（以下简称密评新国标），并于2021年10月1日起实施。密评新国标是贯彻落实《中华人民共和国密码法》、指导我国商用密码应用与安全性评估工作开展的纲领性、框架性标准。该标准分五个级别，从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个方面提出了密码应用技术要求；从管理制度、人员管理、建设运行和应急处置四个方面提出了密码应用管理要求。它对于规范引导信息系统密码合规、正确、有效应用具有重要意义。密评新国标发布后，各行业/领域可在此基础上，针对自身应用需求，制定相应的行业标准/团体标准，进一步规范和指导本行业信息系统密码应用。

在无线局域网（WLAN）领域，统一的密码应用标准尚属空白，为确保产品在设计、研发、生产和部署环节的一致性和互通性，WAPI产业联盟牵头组织了《GB/T 39786实施指南：无线局域网密码应用基本要求》团体标准项目的创新工作，计划在密评新国标基础上，研究分析密码应用规范性要素，结合



WLAN领域信息系统建设方运营方的密码应用需求，结合WLAN领域产品开发/生产厂商、技术研究机构的密码应用能力，从WLAN系统的物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个技术层面，和管理制度、人员管理、建设运行和应急处置四个管理层面，形成WLAN领域较为全面的密码应用基本要求实施指南。

该团体标准立项后，WAPI产业联盟测试实验室、无线网络安全技术国家工程实验室、西电捷通公司、紫光展锐公司、陕西省网信安全测评中心、北京华信傲天网络技术有限公司、工业和信息化部宽带无线IP工作组等单位已经正式申请成为参编单位。北京数字认证股份有限公司、国家信息技术安全研究中心、中国电信股份有限公司、新华三技术有限公司、深圳市智开科技有限公司、西安芯语慧联信息科技有限公司等多家单位的申请手续正在办理过程中。

西电捷通公司便携式WAPI无线接入鉴别综合网关 通过联盟测试

WAPI产业联盟 王立华



2021年7月23日，西电捷通公司的便携式WAPI无线接入鉴别综合网关(以下简称便携式WAPI网关)，型号：WLG4125通过了WAPI产业联盟无线局域网鉴别与保密基础结构（WAPI）互通性、完整性及扩展功能测试。联盟为上述产品出具了测试报告。

该便携式WAPI网关支持无线接入点（AP）、鉴别服务器（AS）和证书签发服务器（CIS）功能，能够为用户提供证书管理、身份鉴别和无线接入一体化服务。该产品体积小可随身携带、内置高容量电池、即开即用，可满足户外无电源供电等场景下的WAPI网络临时搭建。此外，该便携式WAPI网关还支持终端实体证书管理（CMEE）扩展功能，可开放专门用于下载证书的服务集标识（SSID），用户的终端可通过连接该SSID使用CMEE功能，自主生成密钥并实时申请证书，实现证书自动下载。

据西电捷通公司介绍，该产品叠加了IP安全可信

（TISec）终端功能，能提供远程IP安全接入能力，可实现跨互联网/专网建立IP端到端安全连接。更值得一提的是，该产品内置的硬件安全模块已通过了国家权威认证，不仅对密钥存储进行安全保护，也对密钥的使用过程进行了硬件级安全防护。该产品支持通过4G（选配）、以太网等方式连接广域网/互联网，支持IPv4和IPv6双协议栈；在无外接电源的情况下续航可达10小时，满足移动办公，以及智能设备的无线网络连接需要。

目前，联盟实验室已依据最新版无线局域网鉴别与保密基础结构（WAPI）功能测试项目（2021年07月版），针对该产品多种功能合一的特点，对上述产品进行了WAPI协议互通性、完整性及扩展功能测试，并分别出具AP、AS和CIS的测试报告，为后续行业用户产品选型和采购提供必要依据。

广西线材厂WAPI系列产品通过联盟测试

WAPI产业联盟 王立华

2021年8月9日，广西电力线路器材厂有限责任公司（以下简称广西线材厂）的无线局域网系列产品通过了WAPI产业联盟无线局域网鉴别与保密基础结构（WAPI）互通性、完整性及性能测试。联盟为上述产品出具了测试报告。

本次测试通过的设备包括：室内/室外无线接入点（AP）、接入点控制器（AC）、鉴别服务器（AS）、客户前置设备（CPE）。其中，AP、CPE设备均支持2.4/5GHz双频接入，通信速率支持802.11ac协议，AS设备具备漫游功能，可满足行业应用中大带宽、移动性、大连接的无线局域网应用需求。

联盟实验室依据2021年最新版无线局域网产品鉴

别与保密基础结构（WAPI）功能测试项目，对上述设备进行了协议互通性、完整性、功能及性能测试。测试过程中，联盟实验室和设备厂商通过远程联调形成紧密互动，对发现的未通过项，联盟实验室迅速进行分析定位，配合厂商远程调试和优化，完善产品的WAPI功能。

据广西线材厂介绍，此次测试通过的WAPI快速切换CPE设备，支持在任意AP间实现毫秒级切换能力，可满足安防监控、高清视频等实时数据无间断、不卡顿的高速传输。本次测试通过的WAPI系列产品，将服务于广西电力智能数字化控制、智能线路巡检、智能变电站等应用建设。



恩智浦（中国）管理有限公司加入WAPI产业联盟

WAPI产业联盟 周 园



2021年9月1日，经联盟理事会批准，恩智浦（中国）管理有限公司正式加入WAPI产业联盟，联盟会员单位增至107家。

恩智浦（中国）管理有限公司（以下简称“恩智浦”）是一家专注于芯片设计及解决方案的厂商，一直以来秉持“智慧生活 安全连结”的理念，希望通过领先技术推动更便捷智能安全的生活。恩智浦注重技术创新，公司研发的高性能应用解决方案，可以推动万物感知、万物连接、万物安全。目前，恩智浦拥有超过60年的专业技术及经验，在全球30多个国家设有业务机构，员工达29,000人，2020年全年营业收入86.1亿美元。

据恩智浦介绍，目前公司的W8987、W8897、W8977、W8801等型号无线局域网芯片已支持WAPI，并应用于车载互联网、智能手机、智能家居、IOT设备中。恩智浦表示，未来将持续开发WAPI芯片，服务新的产品和领域。

中国电科院：提升工作效率 完成变电站巡检机器人检测

中国电科院

2021年7月9日，在国家电网公司特高压交流试验基地的变电站智能巡检机器人试验场，中国电科院检测团队利用入网集中检测技术手段，按照最新编制的行业标准，实现了样品检测环境、安全风险和统一评定标准的有效控制，同时提升了检测工作效率。

变电站巡检机器人是未来智能变电站运维技术发展的重点方向之一，当前市场上的产品多达数十种，为了帮助产品制造商提升产品性能指标，保障产品质量，适应国家电网公司“立体巡检+集中监控”模式，中国电科院以解决实际问题为导向，依据国内首个变电站巡检机器人试验检测方法的行标，制定科学检测方案，对30种样品开展基本性能、巡检能力、监控后台、安全接入功能等性能集中检测，快速出具检测报告，此次集中检测较以往缩减检测周期10天。

中兴通讯上半年营收情况可喜

中兴通讯

2021年8月27日，中兴通讯发布2021年半年度报告指出：面对内外部环境的机会和挑战，中兴通讯立足有质量增长，以技术创新为本，坚持技术竞争力引领，积极推进业务拓展，实现营业收入530.7亿元人民币，同比增长12.4%。

其中，无线产品方面，中兴通讯率先发布业界首个无线智能编排方案，并在辽宁大连完成全球首个商用网络验证。服务器及存储产品多年连续入围运营商集采，在2019-2021年度连续中标中国移动PC服务器集采最大份额，目前已应用于全球超40个国家和地区。

华大电子首次发布数字人民币钱包芯片

腾讯网

2021年9月3日-9月7日，2021年中国国际服务贸易交易会期间，华大电子首次发布数字人民币钱包芯片产品及方案，为数字人民币的安全健康发展保驾护航。

数字人民币钱包是数字人民币的载体，人民银行通过打造多种钱包产品，开放钱包生态，实现数字人民币线上线下全场景应用。2020年，数字人民币硬钱包亮相于试点应用场景中。

数字人民币硬钱包具有开立、充值、提现、同步、离线收付款等功能，具有不可重复花费、不可非法复制伪造、交易不可篡改及抗抵赖等特性。“双离线”作为硬钱包的突出亮点，可以保证无网络情况下支付的正常进行，满足在地下室、停车场、山区、飞机甚至是地理灾害等特殊环境下的支付需求。安全芯片作为数字人民币硬钱包的核心，其高安全性、高可靠性为数字人民币钱包的存储和交易提供了安全保障。

华大电子首次发布基于安全芯片的多种不同形态的数字人民币硬钱包产品和解决方案，包括数字人民币卡式钱包、数字人民币钱包模组产品、数字人民币可穿戴钱包产品、数字人民币异形钱包、数字人民币钱包终端、支持数字人民币钱包ESAM、数字人民币钱包安全芯片等，能够满足加油站缴费、充电桩充电、交通出行、车联网支付等广泛的智慧民生以及小额高频支付场景的需要。华大电子安全芯片产品采用国产CPU核，满足可用可控的需求，其安全性达到国际、国内领先水平，取得国际最高安全等级SOGIS CC EAL 6+认证、取得国内商用密码二级、EAL4+等国家权威机构的资质认证，保证了数字人民币钱包的功能性和安全性。

新华三：致力做政府数字化变革“背后的力量”

新华三

随着政务场景与创新技术的逐步融合，政府正向着“全面智治、有效协同”的方向加速演进，实现数据驱动的社会治理，打造诚信高效的营商环境，提供普惠便利的民生服务，激活社会发展的新要素和新价值，助力数字经济的高质量发展。政府数字化变革的融合推进，也意味着数字政府基础架构和业务平台的升级重塑。

近期，新华三集团立足“云智原生”战略和全面升级的“数字大脑2021”，以“芯-云-网-边-端”融合共生，构建“四横四纵”框架，助力政府数字化变革新动能全面提升。

工信部：

2023年网络安全产业规模将超过2500亿元

人民网

2021年7月12日，工信部发布《网络安全产业高质量发展三年行动计划（2021—2023年）（征求意见稿）》（简称《行动计划》）。《行动计划》明确提出，到2023年，网络安全产业规模超过2500亿元，年复合增长率超过15%。一批网络安全关键核心技术实现突破，达到先进水平。新兴技术与网络安全融合创新明显加快，网络安全产品、服务创新能力进一步增强。

《行动计划》提出，到2023年，网络安全技术创新能力明显提高，产品和服务水平不断提升，经济社会网络安全需求加快释放，产融合作精准高效，网络安全人才队伍日益壮大，产业基础能力和综合实力持续增强，产业结构布局更加优化，产业发展生态健康有序。网络安全产业规模超过2500亿元，年复合增长率超过15%。一批网络安全关键核心技术实现突破，达到先进水平。新兴技术与网络安全融合创新明显加快，网络安全产品、服务创新能力进一步增强。

《行动计划》要求，到2023年，一批质量品牌、经营效益优势明显的具有网络安全生态引领能力的领航企业初步形成，一批面向车联网、工业互联网、物联网、智慧城市等新赛道的“专精特新”中小企业群体迅速成长，网络安全产品、服务、解决方案单项冠军企业数量逐步壮大。电信等重点行业网络安全投入占信息化投入比例达10%。

同时，《行动计划》提出，重点行业领域安全应用全面提速，中小企业网络安全能力明显提升，关键行业基础设施网络安全防护水平不断提高。建成一批网络安全人才实训基地、公共服务平台和实训靶场，创新型、技能型、实战型人才培养力度显著加大，多层次网络安全人才培养体系更加健全，网络安全人才规模质量不断提高。产融对接更加精准高效，资本赋能作用持续加大。网络安全产业结构进一步优化，产业聚集效应显著增强。以产品服务能力为导向的健康市场秩序不断完善，大中小企业融通发展的产业格局基本形成。

重点任务方面，《行动计划》提出了产业供给强化行动、安全需求牵引行动、产融合作深化行动、人才队伍建设行动、产业生态优化行动等。

《行动计划》还指出，鼓励地方在财政投资的信息化项目中同步配套建设网络安全技术措施，在项目验收阶段加强对网络安全方面的评审。鼓励重点行业企业加大网络安全投入，单独列支网络安全预算，推动网络安全技术、产品和服务部署应用。

全国医疗机构网络信息安全管理办法将出台

经济参考报

2021年8月11日，一消息人士在中国互联网大会上透露：“全国医疗机构网络信息安全管理办法正在起草中，不久将会出台。”新冠疫情暴发后，全球医疗健康数据频繁受到黑客攻击，国内开始重视医疗健康数据的价值，希望通过立法、加强监管等多维度方式提升医疗健康数据的整体安全水平。

医疗健康数据广泛应用在日常生活的多种场景中。比如，通过大数据高效分析用药成分、剂量时间等情况，寻找合理用药的最佳组合；通过大量临床数据进行科学分析找到病因，并进行临床病因分析和慢病监测；通过对基因序列大量分析，快速筛查和预测疾病和潜在基因缺陷的基因组学分析；对患者进行远程疾病数据采集后，结合大量临床病因数据分析，实现远程医学诊疗；通过智能可穿戴设备收集数据，实现人体生命体征检测，预警潜在健康风险，进行健康管理；应用大数据等算法，制定医保支付标准，并基于此进行精准的医保决策分析等等。

卫健委医院管理研究所副所长王凯表示，医疗行业关系国计民生，医疗数据一旦遭到篡改、破坏和泄露，势必对医疗机构的声誉、医患双方的隐私及健康安全构成严重威胁，甚至影响社会的和谐稳定。

基于医疗大健康数据的敏感性，2016年至今，国家相继出台了不少医疗健康数据安全政策进行规范，包括《关于促进和规范健康医疗大数据应用发展的指导意见》、《互联网诊疗管理办法》、《互联网医院管理办法》、《远程医疗服务管理规范》、《国家健康医疗大数据标准、安全和服务管理办法》、《人类遗传资源管理条例》、《数据安全法》等法律法规。但“即使有如此多法规，医疗健康数据安全事件频发，数据安全形势非常严峻。”中国信通院云计算与大数据研究所副所长魏凯表示，尤其是疫情后，数据安全的风险进一步加剧了。

2020年4月，世界卫生组织发表声明称，疫情期间遭受网络攻击数量同比增长5倍。奇安信集团发布网络安全系列报告指出，2020年疫情暴发后，医疗卫生行业史上首次超过政府、金融、国防、能源、电信等领域，成为全球APT（黑客以窃取核心资料为目的，针对客户所发动的网络攻击和侵袭行为）活动关注的首要目标。全球23.7%的APT活动事件与医疗卫生行业相关。中国首次超过美国、韩国、中东等国家和地区，成为全球APT活动的首要地区性目标。

据悉，目前医疗健康不安全风险主要体现在八个方面：一是在线医疗数据：检验报告、诊断结果、既往病史等健康医疗数据存在因漏洞攻击、病毒感染等，导致的非法访问、窃取篡改和恶意上传等风险；二是医联体访问数据：医联体以及第三方服务机构人员在对敏感数据进行访问浏览的过程中，均可能导致医患隐私等重要信息面临泄露风险；三是临床科研数据：临床科研数据涉及人口学资料、检查信息、检验信息、药品医嘱、诊断信息、病例以及患者报告，传输过程中一旦发生泄露，后果非常严重；四是医保数据：医保数据涉及与第三方机构对接，在系统对接、数据传输、数据使用、数据存储、数据销毁等环节面临安全风险；五是医疗设备维保数据：医疗器械厂商在进行远程医疗设备维护保养时，数据将面临非授权访问、不安全链接、隐私数据泄露、维护记录保存不当等安全风险；六是健康大数据中心数据：分类分级机制缺失导致将非法登录、越权访问、异常调阅、冒名查询、批量窃取、明文泄露等数据安全隐患；七是可穿戴健康设备数据：可穿戴设备数据在采集、存储、使用阶段均存在着不同程度的安全隐患；八是医疗健康APP数据：移动应用涉及众多在线健康医疗服务、存在泄露个人健康状况数据、支付数据、卫生资源数据以及公共卫生信息的隐患。

针对上述，需要多维度提升数据安全整体水平。魏凯表示，一方面加强监管，推动制定、完善卫生健康行业数据安全管理办法出台。另一方面，制定完善医疗健康数据安全配套标准体系，建立行业合作机制，协同创新、开放共享。



美国NSA警告公共网络是黑客攻击的温床

秦安战略

美国国家安全局（NSA）当地时间周四发布的一份题为《公共环境下无线设备的安全保护》公共服务公告，敦促安全团队注意员工使用Wi-Fi网络时面临的无线威胁。该公告将蓝牙技术和近场通信(NFC)列入其令人担忧的协议清单。NSA警告称，攻击者以远程办公人员为目标，窃取公司数据。NSA建议，机构应寻求保护企业网络和个人无线设备的最佳实践。这些建议虽然范围不大，但确实为系统管理员提供了一个可靠的备忘清单，可以与他们在家工作的员工和移动工作人员分享。

远程办公已经成为当前一种重要的新工作方式，许多人在家或在旅行中远程办公。虽然家庭网络的所有者可以采取步骤确保这些网络的安全，但很难确保公共网络(例如，会议或酒店Wi-Fi)的安全。无论何时，保护个人和公司数据都是至关重要的，尤其是在公共场所远程办公时。为了确保数据、设备和登录凭证的安全和不受损害，网络安全是用户和企业的关键优先事项。

尽可能避免连接到公共Wi-Fi，因为在使用公共Wi-Fi网络时，风险会增加。尽可能使用公司或具有强大的认证和加密的个人Wi-Fi热点，因为它将更安全。

如果用户选择连接到公用无线网络，他们必须采取预防措施。通过公共Wi-Fi发送的数据，特别是不需要口令即可访问的开放公共Wi-Fi，很容易受到盗窃或操纵。即使一个公共的无线网络需要一个口令，它也可能不会加密经过它的流量。如果Wi-Fi网络确实加密了数据，如果恶意参与者知道预先共享的密钥，他们就可以解密它。恶意行为者有时也会迫使网络使用不安全的协议或过时的加密算法(降级到不安全的协议)。此外，恶意行为者可以设置一个假的访问点，也被称为邪恶的双胞胎，以模仿附近的公共Wi-Fi，导致该行为者能够访问通过网络发送的所有数据。可以使用开源工具捕获未加密的网络流量或容易解密的流量，从而暴露敏感数据。

到目前为止，远程办公的员工可能已经掌握了公共Wi-Fi热点的网络卫生技术。但是，美国国家安全局建议：“通过公共Wi-Fi传输的数据——尤其是不需要口令就能访问的公共Wi-Fi——很容易被窃取或操纵。”

建议还包括对假接入点的警告，假接入点可能会隐蔽盗取用户凭证，并浏览“邪恶双胞胎”接入点检索到的其他个人数据。

美国国家安全局的无线警告虽然都是一些最最基本的要求，但仍然被太多的人忽视。专家表示，遗憾的是，实用和基本的建议仍然需要推广。

NTT应用安全公司的Setu Kulkarni表示：“我担心的是，这些‘禁止项’根深蒂固，存在着不易改变、有时不可避免的行为。”“例如，虽然很容易说‘不要把设备靠近其他未知的电子设备’，但这可行吗？”

Kulkarni补充说，在理想的情况下，公司应该制定一个关键的员工网络安全规则，那就是避免在工作用设备中保留个人信息。执行合规变得更加棘手。

Tripwire的蒂姆·欧林(Tim Erlin)表示：“这些建议在2021年和2015年一样重要，但随着远程工作的增多，越来越多的人使用公共Wi-Fi。”“虽然这些技巧很有用，但普通用户可能很难理解如何执行它们。要让普通用户遵守推荐设置，确实有大量工作要做。”

浅谈2021版无线局域网设备测试规范

WAPI产业联盟 王立华

一、前言

近日，T/WAPIA 037.2—2021《GB/T 32420实施指南 第2部分：无线局域网设备测试》（以下简称2021版测试规范）即将由WAPI产业联盟发布，该标准是在T/WAPIA 037.2—2019《GB/T 32420实施指南 第2部分：无线局域网设备测试》的基础上进行修订。主要增补了802.11ax模式和管理帧保护等项目的测试方法，使联盟测试标准体系与技术标准体系的发展保持一致。为产业开展无线局域网（WLAN）设备新功能测试提供支撑。

二、《GB/T 32420实施指南》制定背景——紧跟技术发展，服务市场需求

多年来，WAPI产业联盟始终坚持技术规范与测试规范协同发展、互为促进。2010年联盟发布了T/WAPIA 002—2010《无线局域网接入点技术要求与测试方法》、T/WAPIA 003—2010《无线局域网接入控制器技术要求与测试方法》、T/WAPIA 004—2010《无线局域网站点技术要求与测试方法》、T/WAPIA 005—2010《无线局域网鉴别服务器技术要求与测试方法》等4项团体标准，填补了国内WLAN测试规范的空白，实施后取得了良好的效果。并因满足了国家发展WLAN技术和产业的迫切需要，已被转化为国家标准GB/T 32420—2015《无线局域网测试规范》并实施。

近几年来，各行业对安全的无线局域网需求旺盛，市场用户对无线局域网检测提出了更高更精细的要求，为进一步推进GB/T 32420—2015的实施，WAPI产业联盟规划了《GB/T 32420实施指南》系列团体标准，在国家标准基础上进一步提升技术指标和测试方法，并于2019年发布了T/WAPIA 037.2—2019《GB/T 32420实施指南 第2部分：无线局域网设备测试》（以下简称2019版测试规范）。

在无线局域网行政许可合规性测试中，每年有几千款产品依据国家标准GB/T 32420—2015开展测试。在行业市场中，对产品的检测有着精细化程度高、定制化强、功能多样化等特点，《GB/T 32420实施指南》系列团体标准在国家标准基础上贴合行业市场测试需求，进一步丰富了测试项目并新增了测试方法，提升了技术指标，具有测试项目更加全面、测试颗粒度更高的特点，为行业市场安全的无线局域网产品应用提供测试保障。

三、2021版测试规范修订背景——测试标准体系与技术标准体系发展保持一致

随着无线局域网技术的不断演进，WAPI产业联盟相继发布了T/WAPIA 007.10—2020《无线局域网产品工程化实现指南 第10部分：WAPI与IEEE 802.11ax》和T/WAPIA 010.3—2021《信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第11部分：无线局域网媒体访问控制和物理层规范 第3号修改单：管理帧保护技术规范》两项技术标准。为保证测试标准体系与技术标准体系保持一致，更好地为产业开展无线局域网设备测试提供支撑，依据上述两项技术标准在2019版测试规范中新增补了802.11ax模式和管理帧保护等项目的测试方法，为2021版测试规范能够全面、适宜地指导开展无线局域网设备的测试工作提供保障。

四、2021版测试规范修订内容

2021版测试规范是在2019版测试规范基础上进行修订，主要修订内容包括：增补了IEEE 802.11ax模式WAPI协议符合性和性能测试、管理帧保护测试、WPI过程中SM4-GCM算法工作模式测试、CMEE终端证书管理的测试、WLAN其他设备测试以及针对工程化实现问题进行测试项目优化等。

1、IEEE 802.11ax模式测试

随着WLAN对更高速率的应用需求，越来越多支持IEEE 802.11ax模式的设备将出现在WLAN应用中。为正确的指导设备厂商、用户单位、检测机构开展802.11ax模式的设备测试验证工作，在2021版测试规范中，增加了对IEEE 802.11ax模式的测试，为这类设备的测试提供了测试依据。测试内容涉及：MAC层测试、功能测试、性能测试和空中接口物理层测试。其中MAC层测试和功能测试的测试方法与其它无线模式的测试方法一致，在2021版测试规范中未增加独立的测试用例。

2、WPI过程中SM4-GCM算法工作模式测试

为满足设备在IEEE 802.11ac、IEEE 802.11ax模式数据高速率传输的能力，在数据的加解密方面，部分芯片已采用SM4-GCM算法工作模式来提升算法性能。SM4-GCM算法工作模式的测试验证成为了数据高速率传输模式下的关键测试内容之一。在2021版测试规范中增加了对SM4-GCM算法工作模式的测试，满足了厂商对此项的测试验证需求。

由于SM4-GCM算法工作模式是应用在WPI过程中的，2021版测试规范没有设计独立的测试用例，而是将其融于“加密功能”测试中。既通过“强制配置基准设备的信标帧、探测响应帧，或关联请求帧”，来判定被测设备是否具备支持SM4-GCM算法工作模式的能力。

3、管理帧保护测试

早期的无线局域网技术标准对数据帧的安全保护较强，但对管理帧的保护不足。2012年，WAPI产业联盟制定并发布了团体标准2012版管理帧保护技术规范，实现了对部分管理帧（如解除关联和解除链路验证帧）的保护。随着Action帧等更多类型的管理帧被定义和广泛使用，管理帧保护的范围也需要同步扩大，2018年，联盟启动了对2012版管理帧保护标准的修订工作，于2021年3月正式发布了2021版管理帧保护技术规范，与此同时，在2021版测试规范中增加了管理帧的策略选择、密钥管理和数据处理等若干内容，明确了管理帧保护的测试方法和测试流程。

4、WLAN其他设备的测试

在无线局域网测试规范和2019版测试规范中，无线局域网设备类型一直被分为终端（STA）、无线接入点（AP）和鉴别服务器（AS）三个大类，并据此设计测试用例。随着WLAN市场规模化应用，应用场景愈加丰富，其中出现了多形态、多功能属性以及新类别的产品。如何定义上述产品以及如何进行测试成为了行业市场迫切需要解决的问题。

在2021版测试规范新增定义了一组“WLAN其他设备”。包括接入点控制器（AC）设备、WAPI网关、智能移动通信终端等，明确了上述设备的定义，同时设计了对应的测试方法。另外新增一类无线局域网设备类型——证书签发服务器（CIS），该设备主要提供对STA、AP和AS的证书签发管理服务，在2021版测试规范中增加了此类设备的测试方法。

5、CMEE终端实体证书管理测试

终端实体证书管理（CMEE）是一套完整的、普适性的证书管理和安全传输的解决方案，通过该功能，用户可自动生成密钥并在线获取证书，实现证书自动下载功能，可应用在WLAN网络的证书申请、颁发、更新等多个环节，是对WLAN证书管理应用的有益补充。新版测试规范中也明确了针对CMEE安全应用的测试方法和测试流程，涉及STA、AP、AS和CIS。

6、针对工程化实现问题进行测试项目优化

在使用2019版测试规范进行实际业务测试中，发现了一些由于工程化实现的问题而导致测试结果与被测设备状态存在一定偏差的现象。

例如，在对某款设备进行密钥更新测试中，依据2019版测试规范的要求对被测设备分别进行单播密钥更新、组播密钥更新和基密钥更新的测试，并顺利通过测试；但是在实际的应用中偶然发现，对该设备连续进行单播密钥更新、组播密钥更新和基密钥更新，或两两组合连续更新时，大概率出现更新后无法连通对端的情况。虽然最后生产厂商确认是因为工程化实现出了问题，但是也可以看出测试方法、测试流程设计方面还是存在一定的缺陷。因此在2021版测试规范中，增加了一些测试用例或修订了测试流程，保证测试规范的严谨性，更好的为生产厂商提供测试服务。

五、结束语

随着WLAN技术不断演进、应用场景不断丰富，相应的技术标准与测试规范也将与时俱进。2021版测试规范的发布，一方面增补了802.11ax 模式下的 WAPI 协议符合性测试和性能测试，为无线局域网设备更高速率的功能、性能测试提供了有力支撑；另一方面完善了管理帧保护功能测试方法，进一步提升设备安全性。此外，该标准还增补了终端证书管理、证书签发服务、WAPI 网关等新功能测试项目，具备了作为新型WLAN设备测试依据的完备性和适宜性。

在2021版测试规范制修订过程中，联盟测试实验室同步开展了新增测试项的检测能力建设，目前已具备上述所有新增测试项的检测能力，同时发布了无线局域网鉴别与保密基础结构（WAPI）最新测试项，并依据新版测试项开展测试服务。在多年服务市场过程中，联盟坚持技术规范与测试规范并重，坚持技术标准与工程化验证工作同步开展，这也使得，联盟大多数团体标准发布之日，即是相关产品推向市场之时。

作者王立华，系WAPI产业联盟测试工程师 无线网络安全标准化委员会委员。

WAPI 产业联盟成员单位名录

中国移动通信集团公司	弘浩明传科技股份有限公司	吉翁电子（深圳）有限公司
中国电信集团公司	京信通信技术（广州）有限公司	北京汇为永兴科技有限公司
中国联合网络通信集团有限公司	北京城市热点资讯有限公司	福建星网锐捷网络有限公司
国家密码管理局商用密码检测中心	优比无线技术（深圳）有限公司	北京新岸线移动多媒体技术有限公司
国家无线电监测中心检测中心	南京智达康无线通信科技股份有限公司	广东欧珀移动通信有限公司
北大方正集团有限公司	上海欣民通信技术有限公司	上海贝尔股份有限公司
西电捷通无线网络通信股份有限公司	福建三元达通讯股份有限公司	成都鼎桥通信技术有限公司
北京中电华大电子设计有限责任公司	新华三技术有限公司	飞天联合（北京）系统技术有限公司
北京六合万通微电子技术有限公司	北京傲天动联技术股份有限公司	中国电力科学研究院
广州杰赛科技股份有限公司	中兴通讯股份有限公司	锐迪科微电子（上海）有限公司
深圳市明华澳汉科技股份有限公司	武汉虹信通信技术有限责任公司	苏州汉明科技有限公司
无锡中太数据通信有限公司	广州市卓纪思网络科技有限公司	神州数码网络(北京)有限公司
青岛海尔科技有限公司	赛芯电子技术（上海）有限公司	北京必虎科技股份有限公司
海信集团有限公司	雷凌科技股份有限公司	北京市政务网络管理中心
联想（北京）有限公司	瑞晟微电子（苏州）有限公司	天津赞普科技股份有限公司
华为技术有限公司	联发博动科技（北京）有限公司	北京数字认证股份有限公司
大唐移动通信设备有限公司	四川天邑信息科技股份有限公司	上海连尚网络科技有限公司
北京朗波芯微技术有限公司	湖南城市热点无线通信有限公司	深圳市瑞科慧联科技有限公司
大唐微电子技术有限公司	珠海市魅族科技有限公司	深圳市信锐网科技术有限公司
上海鼎芯科技有限公司	深圳市雄脉科技有限公司	福建新大陆通信科技股份有限公司
北京天一集成科技有限公司	奥泰尔科技（深圳）有限公司	北京比邻科技有限公司
北京联信永益信息技术有限公司	北京网贝合创科技有限公司	天津市电子机电产品检测中心
深圳鑫金浪电子有限公司	网件（北京）网络技术有限公司	高通无线通信技术（中国）有限公司
深圳市普天宜通科技有限公司	上海市数字证书认证中心有限公司	中科开创（广州）智能科技发展有限公司
北京汉铭信通科技有限公司	北京创原天地科技有限公司	北京华信傲天网络技术有限公司
西安大唐电信有限公司	阿德利亚科技（北京）有限责任公司	南京博洛米通信技术有限公司
深圳共进电子股份有限公司	深圳市华讯方舟软件信息有限公司	广西新海通信科技有限公司
北京华安广通科技发展有限公司	迈创智慧供应链股份有限公司	上海麓慧科技有限公司
深圳国人通信有限公司	科通宽带技术(深圳)有限公司	深圳市智开科技有限公司
东蓝数码有限公司	邦讯技术股份有限公司	南方电网数字电网研究院有限公司
美国安移通网络公司北京代表处	惠州市宝丰信息科技有限公司	深圳航天科创实业有限公司
北京五龙电信技术公司	晨星软件研发（深圳）有限公司	南方电网深圳数字电网研究院有限公司
北京同耀通电科技有限公司	卓望数码技术（深圳）有限公司	广西电力线路器材厂有限责任公司
北京登合科技有限公司	迈普通信技术股份有限公司	广西通量能源技术有限公司
宇龙计算机通信科技（深圳）有限公司	北京汇通融业科技发展有限公司	恩智浦（中国）管理有限公司
上海润欣科技有限公司	上海寰创通信科技有限公司	

【注：截至2021年9月，联盟正式成员已达107家，以加入联盟的时间先后排序。】

WAPI Alliance
产 | 业 | 联 | 盟



地 址：北京市海淀区知春路27号量子芯座1608室

邮 编：100191

电 话：010-82351181

传 真：010-82351181 ext. 1901

邮 箱：wapi@wapia.org

网 址：<http://www.wapia.org.cn>