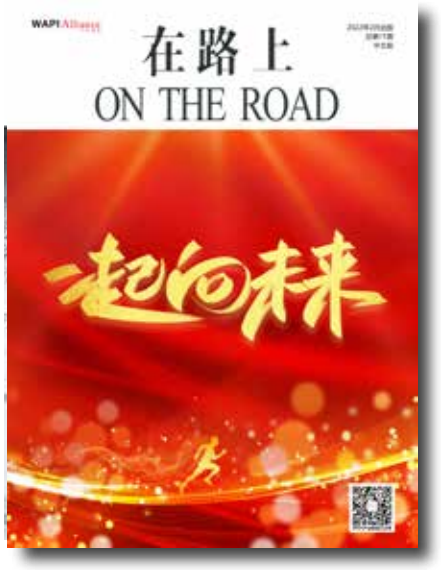
WAPI Alliance
产业联盟

2022年2月出版
总第71期
中文版

在路上
ON THE ROAD



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技术股份有限公司

广州杰赛科技股份有限公司

西电捷通公司

深圳市明华澳汉智能卡有限公司

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　　刘剑昕　　米　东

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标准产业应用及环境监测报告：

WAPI产业联盟公众号

媒体聚焦
Media Focus

特别报道
Special Report

联盟关注
Alliance Concerns

政经要闻
Policy News

联盟工作
Alliance Work

新成员
New Member

成员与市场
Member & Marketing

产业技术论坛
Industry & Technology Forum

中国电子报等：

WAPI产业联盟无线局域网产品自我声明信息服务平台获好评

【编者按】2021年，结合市场用户对合规安全无线局域网产品选型方面的需求，WAPI产业联盟创新开展了无线局域网产品自我声明信息服务平台建设，并面向企业和市场用户提供公益开放服务。经过近一年的建设和运行，平台受到市场用户和企业高度肯定和好评，对我国无线局域网产业市场的健康、有序、高效发展起到了积极促进作用，更好地维护了消费者权益和服务经济社会发展。中国电子报/电子信息产业网、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，结合市场用户对合规安全无线局域网产品选型方面的需求，WAPI产业联盟创新开展了无线局域网产品自我声明信息服务平台建设，并面向企业和市场用户提供公益开放服务。经过近一年的建设和运行，平台受到市场用户和企业高度肯定和好评，对我国无线局域网产业市场的健康、有序、高效发展起到了积极促进作用，更好地维护了消费者权益和服务经济社会发展。

“自我声明”主要是生产者为确认其产品能够满足适用标准相关要求所做出的承诺，它有助于企业产品研发、生产、上市的提速增效，有效降低制度性交易成本，激发企业自主创新，加快产品提质升级。

无线局域网产品自我声明信息服务平台，是由生产者（制造商）采用自我声明方式证明其所提供的无线局域网产品能够持续符合适用标准。平台创新之处在于：第一、强化了企业主体责任，推进了产业诚信生态建设；第二、极大方便了市场用户，市场用户可通过该平台对合规安全无线局域网产品进行“一站式”产品选型。第三、发挥了产业联盟公共平台作用，以实际行动响应政府开展科技管理创新、协助政府简政放权、提升市场管理效率、形成社会共治。

当前安全无线局域网WAPI被越来越多的产品使用和集成，几乎涉及所有具有无线局域网功能的产品、装备。在各行各业开展本行业WAPI关键信息基础设施建设过程中，也向联盟提出了一些“卡脖子”问题，例如：面对数量庞大的产品种类、型号，如何管理才能提升产业整体效率？面对复杂的技术规格和参数，不大懂技术的用户如何快速查找、甄别和判断？不具备底层技术修改能力的整机厂商、设备集成商，如何选择上游供货商？企业们如何低成本地证明自己，并在降低制度性交易成本的基础上取得用户信任？——这些都急需由专业的第三方社会组织提供一站式信息服务平台来解决上述问题。结合上述，WAPI产业联盟于2021年启动了“无线局域网产品自我声明信息服务平台”建设和服务，该平台属于联盟公益服务性质，面向全社会开放，截至2021年底，已服务了几十家企业百余款产品，消除了市场用户在合规产品采购和选型中的“梗阻”，解决了“市场和企业迫切需要、但做不了、又必须有人做”的难题。

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/20211230/114683.html

飞象网：http://www.cctime.com/html/2021-12-30/1604807.htm

通信世界等：

联盟发布首套全国产WAPI MCU物联网终端模组

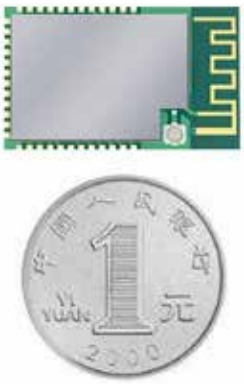
【编者按】2022年2月，WAPI产业联盟组织西安芯语慧联信息科技有限公司、西电捷通公司、北京三凯威科技有限公司三家成员联合技术攻关，研制成功了TH6160系列产品，这是首套全国产化、高安全、低功耗的WAPI MCU物联网终端模组。它有效满足了“低功耗物联网设备快速实现安全无线局域网连接”的市场需求，解决了此前“普通模块功耗偏高、低功耗模块需要二次开发”产业难题，填补了WAPI MCU产品的市场空白，保障了各行各业用户实施WAPI安全方案时的高效率、系统性和完整性。目前，该系列产品已通过了WAPI产业联盟的无线局域网鉴别与保密基础结构（WAPI）互通性及完整性测试，产品间互联互通性能良好。通信世界、中国电子报/电子信息产业网、飞象网、新浪、东方财富网等媒体对此进行了报道。

以下是通信世界的报道。

2022年2月，WAPI产业联盟发布TH6160系列产品，这是首套全国产化、高安全、低功耗的WAPI MCU（微控制单元）物联网终端模组。它有效满足了“低功耗物联网设备快速实现安全无线局域网连接”的市场需求，解决了此前“普通模块功耗偏高、低功耗模块需要二次开发”产业难题，填补了WAPI MCU产品的市场空白，保障了各行各业用户实施WAPI安全方案时的高效率、系统性和完整性。

TH6160系列产品是WAPI产业联盟组织西安芯语慧联信息科技有限公司、西电捷通公司、北京三凯威科技有限公司三家成员联合技术攻关研制成功的。目前，该系列产品已通过了WAPI产业联盟的无线局域网鉴别与保密基础结构（WAPI）互通性及完整性测试，产品间互联互通性能良好。

当前，物联网终端产品的特点是：第一、需求碎片化、产品多样化、成本敏感化、流通垂直化；第二、行业领域的专用机具/设备生产厂商众多且分散，每家厂商不可能都具备独立开发 WAPI 产品的能力。WAPI MCU产品的推出，通过简单适配就让行业专用机具/设备快速具备了 WAPI 能力，既有效解决了厂商独立开发 WAPI 产品周期长、成本高的问题，又满足了市场需要各类 WAPI 物联网产品快速上市的需求。



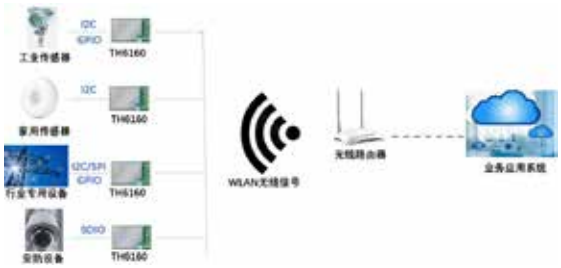
图：TH6160物联网终端模组与一元硬币尺寸比较

TH6160物联网终端模组是工业级设计产品，具有全国产化、高安全、低功耗、稳定性高、扩展性强、体积小等特点。它符合GB 15629.11国家标准，基于全国产第6代WLAN MCU低功耗芯片和国家权威机构认证的硬件安全密码芯片，内部运行高可靠实时操作系统（RTOS），支持2.4GHz 1T1R射频收发，支持IEEE 802.11 b/g/n/ax速率集，提供WLAN、TCP/IP、MQTT、http等多种网络协议通信能力和丰富的AT指令集，提供串

图：TH6160物联网终端模组接口示意图

图：UART串口转WLAN透传模式应用示意图

图：RS232/485工业接口转WLAN透传模式应用示意图



图：主控模式应用示意图

口、SPI、SDIO、IIC、GPIO等多种物理接口，能轻松实现诸如串口转WLAN、IIC转WLAN等常用模式，可广泛服务于传感器远程监测与控制、工业自动化、智能电网、智慧环保、智能家居、可穿戴设备、智能语音设备、智能安防设备、智慧仓储无线系统、智能开关、无线继电器、仪器仪表、无人机等物联网应用场景，帮助用户高效便捷地实现产品和应用方案部署。

本次联盟同步发布的还有基于TH6160系列模组的一站式物联网安全解决方案TH6160-Solution，包括TH6160系列模组、远程管理服务器、以及数据安全网关，用于对模组的远程管理、精准控制、OTA升级、状态监测、数据安全隧道、数据流转等等，可快速实现与第三方产品或系统的对接，大大缩短用户网络部署周期。

参数类型	TH6160无线安全终端模组参数
WLAN参数	支持WLAN STA/SoftAP/STA+SoftAP/Monitor工作模式; 支持2.4GHz、1T1R、MU-MIMO和MU-OFDMA射频能力; 支持WAPI安全模式，符合GB 15629.11系列国家标准，已通过WAPI联盟相关检测; 支持Wi-Fi 6相关技术能力，支持IEEE 802.11b/g/n/ax; 支持WMM QoS能力，支持双载波调制技术（DCM）;
硬件参数	基于全国产的第6代WLAN技术SoC芯片组研制; 240MHz主频MCU，可做主控接传感器等外设，也可做为从设备为其它主控设备提供WLAN通信能力; 内含一颗国家权威机构认证的硬件安全密码芯片，保障WAPI证书私钥的硬件级安全防护性; 输入电压3.0~3.6V，标准电压3.3V; 可扩展支持RS485等工业接口;
物理接口	2路UART接口; 1路高速SPI接口; 2路I2C接口; 1路SDIO接口; 丰富的GPIO接口;
天线方式	支持板载天线或IPEX外接天线
软件能力	内部运行实时操作系统（RTOS）; 支持丰富的AT指令集，易于使用和被集成; 支持TCP/UDP/MQTT/HTTP等多种常用的物联网通信协议; 支持多种工作模式，支持低功耗能力，省电模式下电流小于10uA; 支持可信计算能力，保障模组使用的安全性和可靠性; 支持WAPI证书在线申请能力且私钥芯片内本地生成; 支持固件本地升级或远程OTA升级能力; 支持模组精准化及批量化远程管理能力; 支持其它个性化软件功能定制服务;

部分媒体新闻链接:

通信世界: http://www.cww.net.cn/article?id=557584

中国电子报/电子信息产业网: http://www.cena.com.cn/iot/20220211/115083.html

飞象网: http://www.cctime.com/html/2022-2-11/1608967.htm

新浪: http://jiaju.sina.com.cn/news/20220211/689782013089054796 7.shtml

东方财富网: https://finance.eastmoney.com/a/202202112274115614.html

中国标准化等：

WAPI产业联盟发布新版无线局域网设备测试规范

【编者按】日前，WAPI产业联盟发布团体标准T/WAPIA 037.2—2021《无线局域网测试 第2部分：设备测试规范》（以下简称2021版测试规范）。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》（以下简称2019版测试规范）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，为测试无线局域网新设备、新功能提供支撑。此事引起业界和媒体广泛关注。2022年01月21日，中国标准化、飞象网、中国电子报/电子信息产业网等媒体对此进行了报道。

以下是中国标准化的报道。

日前，WAPI产业联盟发布团体标准T/WAPIA 037.2—2021《无线局域网测试 第2部分：设备测试规范》（以下简称2021版测试规范）。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》（以下简称2019版测试规范）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，为测试无线局域网新设备、新功能提供支撑。

相较2019版测试规范，2021版测试规范主要修订了如下内容：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等。它一方面为测试无线局域网设备更高速

率的功能性能提供了有力支撑；另一方面完善了管理帧保护功能测试方法，成为更具完备性和适宜性的新型WLAN设备测试依据。

图：WAPI产业联盟团体标准

WAPI产业联盟（中关村无线网络安全产业联盟）是该标准的第一起草单位，起草单位还包括：国家无线电监测中心检测中心、西电捷通公司、无线网络安全技术国家工程实验室、天津市无线电监测站、国家密码管理局商用密码检测中心、中国网络安全审查技术与认证中心、北京大学深圳研究生院、重庆邮电大学、中国电信集团上海研究院、北京五龙电信技术公司、WAPI产业联盟测试实验室、湖北经济学院、北京海尔广科数字技术有限公司、中国通用技术研究院、珠海市魅族科技有限公司、迈普通信技术股份有限公司、工业和信息化部宽带无线IP标准工作组。标准修订过程中，广泛征求了业界各方意见，芯片厂商、设备厂商、检测机构对此非常关注并充分表达了意见，为标准发布后依标开展测试达成了共识。

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。结合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/WAPIA010.3—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》两项团体标准。与此同时，与技术演进相匹配的测试规范也同步开展，目的就是保证测试标准体系与技术标准体系的一致性和及时性，更好地为产业开展无线局域网设备测试提供支撑。

据介绍，目前WAPI产业联盟测试实验室已完成了配套测试工具开发和测试能力建设，具备了依据2021版测试规范开展WLAN设备测试的条件，可随时为产业和市场提供服务。

部分媒体新闻链接：

中国标准化：https://mp.weixin.qq.com/s/MC7oEq1zM5DZTJLJfLOX7A

中国电子报/电子信息产业网：http://www.cena.com.cn/infocom/20220121/114958.html

飞象网：http://www.cctime.com/html/2022-1-21/1607338.htm

飞象网等：

WAPI产业联盟发布《无线局域网接入控制》系列团体标准标准国际化进入CD阶段

【编者按】日前，WAPI产业联盟发布T/WAPIA 043.1—2021《无线局域网接入控制 第1部分：组网架构规范》和T/WAPIA 043.2—2021《无线局域网接入控制 第2部分：调度平台技术规范》2项团体标准。该系列标准符合无线局域网（WLAN）规模组网的发展趋势，填补了国内外WLAN云管理技术标准体系空白，推动了WLAN组网新技术演进。该系列标准的国际化工作，正在ISO/IECJTC 1/SC 6推进，目前处于委员会草案（CD）阶段。

此事引起业界和媒体广泛关注。飞象网、中国电子报/电子信息产业网等媒体发布了相关报道。

以下是飞象网的报道。

日前， WAPI产业联盟发布T/WAPIA 043.1—2021《无线局域网接入控制第1部分：组网架构规范》和T/WAPIA 043.2—2021《无线局域网接入控制第2部分：调度平台技术规范》2项团体标准。该系列标准符合无线局域网（WLAN）规模组网的发展趋势，填补了国内外WLAN云管理技术标准体系空白，推动了WLAN组网新技术演进。

上述标准的起草单位包括：中国电信集团有限公司、WAPI产业联盟（中关村无线网络安全产业联盟）、西电捷通公司、新华三技术有限公司。符合标准的产品已在中国电信省级公司部署和应用。

WLAN组网有大量设备管理、部署和维护等需求，在大规模部署WLAN网络时，面对数量众多不同区域的接入点（AP），如何更加合理和智能地为AP分配最佳的接入控制器（AC），让WLAN网络规模部署和运营更加便捷、高效和降低成本，成为当前规模部署WLAN网络的核心需求。WLAN云管理技术是构建运营级WLAN

网络的核心关键技术，通过云AC组网架构，实现了AP灵活智能地接入合适的AC，可有效构建"大容量、高可靠、可管理、可扩展"的运营级WLAN网络。该技术补充和完善了现有WLAN规模部署，极大地提升了设备管理运维效率，市场潜力巨大。

据WAPI产业联盟介绍，上述两项联盟团体标准的国际化工作，正在ISO/IEC JTC 1/SC 6推进，目前处于委员会草案（CD）阶段。

图：WAPI产业联盟《无线局域网接入控制》系列团体标准

WAPI产业联盟是国家标准委首批团体标准试点单位和中关村国家自主创新示范区标准化示范单位，多年来持续组织和推动"标准制定、标准产业化和应用、标准走出去"等工作。截至2021年12月，联盟已组织制定（参与制定）并发布（获发布）了152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83项。在无线局域网、物联网、有线以太网、无线个域网、电子标签、传感器网络、有线局域网、无线城域网、未来网络、磁域网等领域完成了技术标准的国际超前布局。

部分媒体新闻链接：

飞象网：http://www.cctime.com/html/2022-1-27/1607929.htm

中国电子报/电子信息产业网：http://www.cena.com.cn/infocom/20220128/115004.html

中国电子报等：

WAPI产业联盟创新并发布原子密钥建立与实体鉴别系列7项团体标准

【编者按】日前， WAPI产业联盟发布《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》7项原子密钥建立与实体鉴别（AKEA）系列团体标准，首次提出原子密钥建立与实体鉴别的概念，并定义了多种具体的原子密钥建立与实体鉴别机制，在国内相关领域属于首创。中国电子报/电子信息产业网、飞象网等媒体对此进行了报道。

以下是中国电子报的报道。

日前， WAPI产业联盟发布《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》7项原子密钥建立与实体鉴别（AKEA）系列团体标准，首次提出原子密钥建立与实体鉴别的概念，并定义了多种具体的原子密钥建立与实体鉴别机制，在国内相关领域属于首创。

原子密钥建立与实体鉴别AKEA作为网络信息安全技术领域一类基础共性技术，包括具体的封装协议及资源，可与IP、WLAN等多种网络通信协议相结合，增强其网络安全性。AKEA技术体系中提出了安全通道建立机制，可被采纳并应用于WLAN、LAN、IP层以及应用层等，满足网络安全访问和保密通信等需求。AKEA使用不可还原且不可分割的消息交换序列，为两个对等实体提供实体身份鉴别和密钥建立，任何实体在收到最后一条消息之前都无法完成对其对等实体的身份鉴别或密钥建立，可满足目前和未来网络通信领域中合法客户端访问合法网络以及保密通信的安全需求。该标准在实际应用中可结合不同需求，通过配置相关安全能力参数，

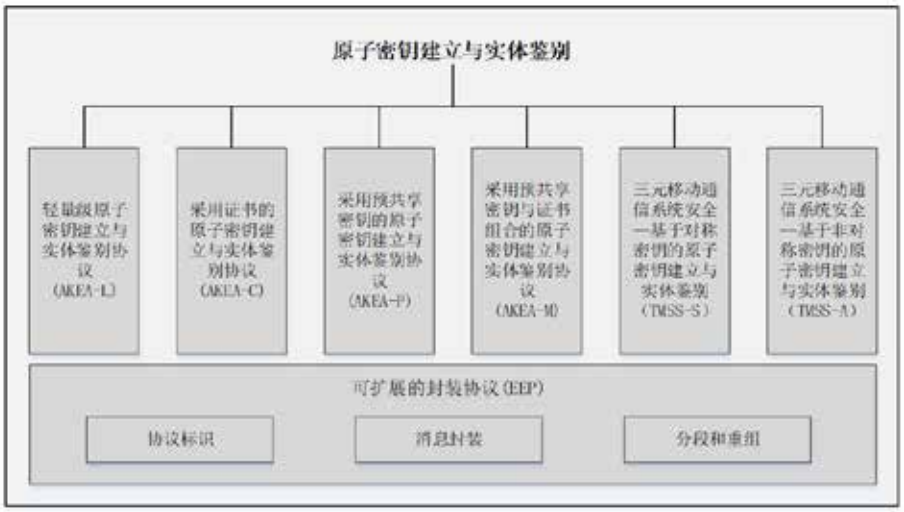
在完成实体鉴别和密钥建立功能时为全网络或局部网络提供多安全级别的差异化保障能力。该系列技术标准还提供了一种量子安全中期演进架构，以融合运用经典公钥密码与分组密码体制的方式，为网络空间提供抗量子计算攻击的纵深防御能力。

从全球技术标准体系的演进来看，网络空间安全相关的标准化工作主要集中在ISO/IEC JTC1 SC27，依据SC27标准的实际分布情况，与网络安全协议直接相关的主要有密码算法系列标准、实体鉴别系列标准（ISO/IEC 9798系列）和密钥管理（ISO/IEC 11770系列）系列标准等。其中，实体鉴别系列标准专注于实体之间的身份鉴别，密钥管理系列标准专注于在两实体之间建立起共享密钥。随着安全需求的不断发展，在实际的通信环境中，那种仅需要身份鉴别或仅需要实体之间保密通信（需要完成密钥建立）的场景非常少见，若要在一个完整过程中既实现实体鉴别又实现保密通信，就需要实体鉴别机制和密钥建立机制二者的结合。此前业界将二者简单叠加、组合的做法存在密钥传输等安全问题，亟需一种原子概念，并同时实现实体身份鉴别和密钥建立两个功能的新机制。

图：WAPI产业联盟原子密钥建立与实体鉴别系列7项团体标准

本次WAPI产业联盟发布的7项AKEA系列团体标准的创新性非常强。第一、它基于三元对等安全架构，具备身份保护能力、抗字典攻击能力，充分考虑了区块链等新技术应用中的技术特性，提供了传统非对称密码算法向后量子密码算法演进阶段协议的安全能力提升。第二、在安全性方面，充分考虑了已知和预测的各种应用技术需求，提出了通用的技术组件供其调用；多种技术机制完备且设计合理，满足了各种应用场景；在协议设计过程中，使用多种密码机制保证消息传递过程中的保密性和完整性；在同步实现密钥建立与实体鉴别过程中，利用哈希链、身份保护、完整性校验以及签名验签等方式，保证了协议设计的原子性。

该系列团体标准规范了四种通用的原子密钥建立与实体鉴别协议，和两种针对移动通信系统的原子密钥建立与实体鉴别协议，具体包括：第1部分：服务和协议；第2部分：轻量级原子密钥建立与实体鉴别；第3部分：采用证书的原子密钥建立与实体鉴别；第4部分：采用预共享密钥的原子密钥建立与实体鉴别；第5部分：采用预共享密钥与证书组合的原子密钥建立与实体鉴别；第6部分：三元移动通信系统安全–基于对称密钥的原子密钥建立与实体鉴别；第7部分：三元移动通信系统安全–基于非对称密钥的原子密钥建立与实体鉴别。



图：原子密钥建立与实体鉴别团体标准体系架构

该系列团体标准的起草单位包括：西电捷通公司、无线网络安全技术国家工程研究中心、中关村无线网络安全产业联盟（WAPI产业联盟）、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、北京数字认证股份有限公司、中国网络安全审查技术与认证中心、中国通用技术研究院、国家信息技术安全研究中心。

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/20220214/115105.html

飞象网：http://www.cctime.com/html/2022-2-14/1609036.htm

飞象网等：

WAPI产业联盟发布团体标准《信息安全技术 证书管理测试规范》

【编者按】日前，WAPI产业联盟发布团体标准T/WAPIA 044—2021《信息安全技术 证书管理测试规范》。该标准为产品符合T/WAPIA 038—2019 《信息安全技术 终端实体证书管理》中规范的终端实体证书管理协议要求、安全数据传输要求、证书安全管理要求等提供了测试方法。标准的推出，保障了产业更好地依标高质量开发产品，使用户能够更便捷、更安全地对身份凭证进行管理和使用。十余年来，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，并在测试规范制订过程中，同步开展相关测试能力的建设。以技术规范引导、规范市场，以测试规范检验、验证产品功能实现。目前，联盟测试实验室已经依据《信息安全技术 证书管理测试规范》完成了配套测试工具开发和测试能力建设，并纳入到扩展功能测试项目中，可随时为产业和市场提供服务。

此事引起了业界和媒体广泛关注。2022年1月27日，飞象网、中国电子报等媒体对此进行了报道。以下是飞象网的报道。

日前，WAPI产业联盟发布团体标准T/WAPIA 044—2021《信息安全技术 证书管理测试规范》。该标准为产品符合T/WAPIA 038—2019《信息安全技术 终端实体证书管理》中规范的终端实体证书管理协议要求、安全数据传输要求、证书安全管理要求等提供了测试方法。标准的推出，保障了产业更好地依标高质量开发产品，使用户能够更便捷、更安全地对身份凭证进行管理和使用。

图：WAPI产业联盟团体标准

该标准起草单位包括：西电捷通公司、无线网络安全技术国家工程研究中心、WAPI产业联盟（中关村无线网络安全产业联盟）、北京数字认证股份有限公司、国家无线电监测中心检测中心、国家信息技术安全研究中心、中国通用技术研究院、广州广电计量检测股份有限公司、国家密码管理局商用密码检测中心、中国网络安全审查技术与认证中心、北京计算机技术及应用研究所。

该标准规定了证书管理测试要求及方法，主要内容包括：被测两个实体的要求、密码算法实现的正确性要求、证书格式的正确性要求、证书管理协议符合性要求、终端实体多个功能操作测试方法、证书颁发实体多个功能操作测试方法以及证书管理安全性测试方法等等。

2019年，WAPI产业联盟发布了技术规范《信息安全技术 终端实体证书管理》，规范了证书认证系统中实体证书管理的安全操作，包括证书的申请、更新、恢复、撤销、查询、获取等，为实体安全连接的建立及数据传输提供了保障。该技术规范发布后已有多家厂商依据标准完成了产品的开发工作，但是无法对标准符合性进行验证。为解决这一问题，WAPI产业联盟迅速组织了《信息安全技术 证书管理测试规范》的创制工作，分别从终端实体和证书颁发实体两部分提出了要求和测试方法，同时按照证书的不同用途详细规定了签名证书、加密证书和密钥交换证书的安全操作的测试方法，为证书管理工程化实现的测试验证提供保障。

十余年来，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，并在测试规范制订过程中，同步开展相关测试能力的建设。以技术规范引导、规范市场，以测试规范检验、验证产品功能实现。目前，联盟测试实验室已经依据《信息安全技术 证书管理测试规范》完成了配套测试工具开发和测试能力建设，并纳入到扩展功能测试项目中，可随时为产业和市场提供服务。

部分媒体新闻链接：

飞象网：http://www.cctime.com/html/2022-1-26/1607768.htm

中国电子报/电子信息产业网：http://m.cena.com.cn/infocom/20220127/114998.html

国家发改委解读“十四五”规划《纲要》：强化国家战略科技力量

国家发改委 规划司

国家战略科技力量是体现国家意志、服务国家需求、代表国家水平的科技中坚力量，强化国家战略科技力量是新时代实现我国科技自立自强，支撑全面建设社会主义现代化国家的必然选择，是加快建设科技强国的重要任务。《纲要》提出，要坚持创新在我国现代化建设全局中的核心地位，把科技自立自强作为国家发展的战略支撑，强化国家战略科技力量。

一、国家战略科技力量建设取得历史性成就

党的十八大以来，以习近平同志为核心的党中央把科技创新摆在国家发展全局的核心位置，以前所未有的力度强化国家战略科技力量，战略性科技任务实施取得重大突破，战略性创新平台体系不断完善，战略性资源空间布局不断优化，重要科研主体能力不断提升，推动我国科技事业实现跨越式发展，发生了历史性、整体性、格局性重大变化。

（一）战略性科技任务实施取得重大突破

基础研究和应用基础研究取得重大原创性成果。铁基超导材料保持国际最高转变温度，量子反常霍尔效应、多光子纠缠世界领先，中微子振荡、干细胞、利用体细胞克隆猕猴等取得重要原创性突破，“悟空”、“墨子”、“慧眼”、碳卫星等系列科学实验卫星成功发射。战略高技术研究有力支撑国家核心竞争力提升。载人航天和探月工程取得“天宫”“神舟”“嫦娥”“长征”等系列重要成果，北斗全球系统全面建成，载人深潜、深地探测、国产航母、大型先进压水堆和高温气冷堆核电、天然气水合物勘察开发、纳米催化、金属纳米结构材料等加快进入世界先进行列。重大装备、工程引领产业向中高端迈进。复兴号高速列车迈出从追赶到领跑的关键一步，超超临界燃煤发电、特高压输变电、杂交水稻、海水稻等世界领先，移动通信、语音识别、第三代核电“华龙一号”、掘进装备等跻身世界前列。

（二）战略性创新平台体系不断完善

国家重大科技基础设施“创新利器”作用进一步发挥。已布局建设57个重大科技基础设施，中国“天眼”、全超导托卡马克、散裂中子源等一批设施处于国际先进水平，为前沿科学研究探索、产业关键技术开发提供了极限研究手段。推动科研设施与仪器开放共享，已有4000余家单位9.4万台（套）大科学仪器和82个重大科研设施纳入开放共享网络。产业创新平台建设体系化拓展。面向集成电路、生物育种、先进高分子材料和智能制造等战略性新兴产业领域布局建设一批国家产业创新中心。围绕解决实验室技术熟化、工程化和成果转化问题，建设一批国家工程研究中心，为关键核心技术和装备突破、科研成果工程化实验验证创造有利条件，解决了一大批经济社会发展中的现实问题。

（三）战略性资源空间布局不断优化

加快打造创新发展战略高地，初步形成“3个国际科技创新中心+4个综合性国家科学中心”创新空间布局。北京国际科技创新中心建设成果丰硕，怀柔综合性国家科学中心建设形成基本框架体系，在空间科学、物质科学、能源科学等领域建设一批国家重大科技基础设施和科教基础设施，原始创新能力显著提高，人工智能、量子信息、生命健康等技术长板不断做强。上海具有全球影响力的科技创新中心建设成绩斐然，张江综合性国家科学中心建设集中度、显示度不断提升，正在加速形成国内最大、国际领先的光子与微纳电子重大科技基础设施集群，集成电路、人工智能、生物医药3大产业创新高地建设进展迅速。粤港澳大湾区国际科技创新中心建设成效初显，大湾区综合性国家科学中心建设顺利起步，5G等领域产业优势不断显现。安徽合肥综合性国家科学中心聚焦能源、信息、生命、环境等领域，加快国家重大科技基础设施等重大平台建设，原始创新能力不断提高。

（四）战略性科研体系水平不断提升

中国科学院“率先行动”计划第一阶段目标任务全面完成，解决了一大批事关国家全局的重大科技问题，突破了一大批制约发展的关键核心技术，取得了一大批一流水平的原创成果。“双一流”大学建设全面启动，42所大学加快建设世界一流大学，95所大学加快建设世界一流学科，高等院校基础研究和人才培养能力显著提升。首批国家实验室挂牌组建，加快组织实施重点领域产学研用协同攻关，聚集培养高水平人才和创新团队。国家重点实验室体系加快优化重组，科技创新基础能力不断强化。

二、新时期、新形势对强化国家战略科技力量提出新要求

“十四五”时期，全球百年未有之大变局加速演进，国际力量对比深刻调整，创新成为影响和改变全球竞争格局的关键变量。进入新发展阶段，贯彻新发展理念，构建新发展格局，对强化国家战略科技力量提出新要求。

（一）塑造国际竞争“非对称”优势，必须强化国家战略科技力量

新一轮科技革命和产业变革深度演进，以群体突破、跨界融合为特征，各学科、各领域间深度交叉融合、广泛扩散渗透，国与国之间的科技较量已经下沉到由基础研究、共性基础技术、基础科学教育、重大科技基础设施等构成的系统能力对抗上来。目前，我国在科技创新系统能力上与发达国家还有差距，需要采取“非对称”赶超战略。实现“非对称”赶超，塑造“非对称”优势，必须要依靠国家战略科技力量，通过发挥国家战略科技力量建制化优势，在关系国家发展全局的关键领域下功夫，带动科技创新系统能力提升。

（二）实现科技自立自强，必须强化国家战略科技力量

近年来，逆全球化趋势更加明显，全球产业链、供应链面临重大冲击，风险加大。我国生产体系内部循环不畅和供求脱节现象显现，“卡脖子”问题突出，结构转换复杂性上升。加快科技自立自强是应对新挑战、解决新问题的必然选择，是畅通国内大循环、塑造我国在国际大循环中主动地位的关键。要通过强化国家战略科技力量，更好地发挥新型举国体制优势，整合各方面力量开展协同攻关，加快提升自主创新能力，实现科技自立自强。

（三）提升国家创新体系整体效能，必须强化国家战略科技力量

进入新发展阶段，我国创新能力还不适应高质量发展要求，基础研究和原始创新能力不强，关键领域核心技术受制于人的格局没有从根本上改变，科技创新资源分散、重复、低效的问题还没有从根本上得到解决，实验室体系有待进一步完善，科研体系的引领作用有待进一步强化，企业技术创新能力有待进一步提高。国家战略科技力量是国家创新体系的关键组成部分，在各类创新主体组成的“创新金字塔”中，处于塔尖位置，要通过强化国家战略科技力量引领国家创新体系整体效能提升。

三、“十四五”时期强化国家战略科技力量的主要任务

《纲要》明确提出，“十四五”期间要制定科技强国行动纲要，健全社会主义市场经济条件下新型举国体制，打好关键核心技术攻坚战，提高创新链整体效能。重点做好以下几个方面的工作。

（一）整合优化科技资源配置

一是充分发挥国家作为重大科技创新组织者的作用。坚持战略性需求导向，确定科技创新方向和重点，着力解决制约国家发展和安全的重大难题。加快建立国家实验室、研究型大学、一流科研院所和创新型领军企业共同参与的高效协同创新体系。以重大科技任务攻关实施为统领，探索国家战略科技力量新型治理结构和运行机制，探索重大科技任务定向委托机制，加强重点领域产学研用协同攻关。

二是加快提升科研主体创新能力。聚焦量子信息、光子与微纳电子、网络通信、人工智能、生物医药、现代能源系统等领域组建一批国家实验室，支撑重大创新领域前沿实现突破。通过调整、充实、整合、撤销等方式，做大、做强、做优国家重点实验室，强化多学科交叉融合，提升承担和完成国家重大科技任务的能力。以加强基础学科发展和科教融合发展为目标，发展新型研究型大学，提升基础研究能力，培养创新型人才。以前沿为引领、以市场为导向，聚焦区域性、行业性重大技术需求，发展新型研发机构，探索新型研发组织形态，推动科研院所、高校科技资源向企业开放，促进各类创新要素向企业集聚，促进产学研用深度融合。

三是持续推动重大创新基地和平台优化布局。聚焦重点行业和产业发展需求，布局建设国家产业创新中心、国家工程研究中心、国家技术创新中心、国家制造业创新中心等创新基地。按照科学、技术和创新基本规律，进一步明确各类中心的战略定位和建设目标，通过多种方式进行优化提升，促进各类创新基地有序发展。

（二）加强原创性引领性科技攻关

一是实施一批具有前瞻性、战略性的国家重大科技项目。从国家急迫需要和长远需求出发，瞄准人工智能、量子信息、集成电路、生命健康、脑科学、生物育种、空天科技、深地深海等前沿领域，实施一批国家重大科技项目。推动重点领域项目、基地、人才、资金一体化配置。改进科技项目组织管理方式，实行“揭榜挂帅”等制度。

二是制定实施战略性科学计划和科学工程。用好国家实验室、综合性国家科学中心、国家重大科技基础设施等战略性创新载体和国际创新合作平台，发挥战略科学家的作用，适时牵头发起国际大科学计划和大科学工程，创新战略性科学计划和科学工程的发起、组织、建设、运行和管理方式。

（三）持之以恒加强基础研究

一是强化支持基础研究顶层设计。制定实施基础研究十年行动方案，兼顾国家紧迫需求与长远储备、目标导向和自由探索，优化重大科研任务部署，打造基础研究体系化力量，营造良好创新生态。布局一批基础学科研究中心，开展数学、物理、化学等基础学科前瞻性、引领性和独创性基础理论研究和前沿方向探索，培养和稳定一批基础学科人才，推动涌现更多“从0到1”重大原始创新成果。

二是探索基础研究经费多元投入机制。持续加大中央财政投入力度，引导地方政府围绕区域经济社会需求加大基础研究和应用基础研究投入。强化企业投入主体地位，推动出台企业投入基础研究税收优惠政策。鼓励社会力量以捐赠和建立基金等方式多渠道投入基础研究，加快形成多元投入格局和稳定投入机制。推动基础研究经费投入占研发经费投入比重提高到8%。

三是建立立符合基础研究规律的评价和激励机制。遵循科技创新规律，坚持分类评价，对自由探索、长期探索的基础研究实行长周期评价机制，创造有利于基础研究的良好科研生态，鼓励基础研究人员潜心致研，把冷板凳坐热。

（四）建设重大科技创新平台

一是加快完善区域创新空间布局。加快推进北京、上海、粤港澳大湾区国际科技创新中心建设，大力支持北京怀柔、上海张江、安徽合肥、大湾区综合性国家科学中心建设，加快打造引领高质量发展的动力源。围绕国家重大区域发展战略，支持有条件的地方建设区域科技创新中心，强化国家自主创新示范区、高新技术产业开发区、经济技术开发区等创新功能，引导创新要素集聚流动，构建跨区域创新网络，加快形成多层次、体系化的区域创新格局。

二是适度超前布局国家重大科技基础设施。按照“四个面向”要求，聚焦制约国家发展和安全的重大难题，布局建设一批具有前瞻性、战略性的国家重大科技基础设施，抢占事关长远和全局的科技战略制高点，为核心技术攻关和产业创新发展提供支撑。完善设施建设、运行、评价全周期管理机制，推动重大科技基础设施开放共享。

三是建设完善科技创新公共服务平台。集约化建设自然科技资源库、国家野外科学观测研究站（网）和科学大数据中心。构建国家科研论文和科技信息高端交流平台。加强科技创新基础支撑与条件保障类国家科技创新基地与平台建设。推进自然科技资源库、数据中心优化整合，加强科研论文原创发布（发表）平台、科技文献战略保障平台、科技信息深度整合平台、科技情报分析与技术监测平台之间的衔接融合。

关键信息基础设施安全保护标准体系解析

公安部网络安全等级保护中心 袁静

关键信息基础设施（以下简称“CII”）安全保护标准体系主要用于明确CII安全保护的标准化需求、环节和范围，指导国家CII安全保护标准体系建设。因此，CII安全保护标准体系设计应关注以下几个方面：

1. 结合国家安全标准现状，突出关键信息基础设施安全保护特点。根据《网络安全法》，CII安全保护以等级保护为基础，且CII一般由一至多个等级保护定级系统构成，所以CII安全保护标准体系应在等级保护标准基础上构建。因此，等级保护系列标准、已立项的保护技术标准等作为支撑标准纳入标准体系。

2. 标准应支撑CII安全保护管理工作。《网络安全法》、《关键信息基础设施安全保护条例》以及《公安部关于印送〈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〉的函》（公网安〔2020〕1960号）等法律法规中提出的各项保护工作应有相应标准予以支撑。因此，识别认定、检测评估、监测预警、应急处置、威胁管控等各项核心工作均应设立相应指导标准。

3. CII系列标准应形成体系。各CII标准应有明确的定位，不同标准之间内在的关联关系需清晰明确，标准内容之间应协调一致。

一、关键信息基础设施安全保护标准体系架构

根据上述设计思路，CII安全保护标准按照标准定位可分为重要标准、支撑标准以及特殊领域标准，按照标准应用的CII保护工作环节划分可分为识别认定类、安全保护类、检测评估类、监测预警类、主动防御类和事件响应处置类等标准。具体见图1关键信息基础设施安全标准体系框架。其中橙色模块为已发布的国家标准，绿色模块标准为已立项尚未发布的国家标准，蓝色模块为未立项标准。

图1 关键信息基础设施安全标准体系图

重要标准为开展CII安全保护相关工作所急需的必要标准，支撑标准为CII保护需参照的非针对CII提出的标准，特殊领域标准为根据特定领域CII的特点而定制的标准。

◆ 识别认定类标准包括关键信息基础设施要素识别指南、重要数据识别以及网络数据分类分级等，用于识别CII保护的关键资产；

◆ 安全保护类标准包括安全保护要求、控制措施、供应链安全、个人信息安全、特殊领域保护要求、人员及服务机构、产品、运维安全、风险管理等等；

◆ 检测评估类标准包括测评要求、检查评估指南、保障指标体系、防护能力评价方法、风险评估指南、个人信息出境评估指南等等；

◆ 监测预警类标准可包括安全预警指南、安全信息共享指南、信息报送与态势研判指南、威胁信息接口要求、监测服务指南等；

◆ 事件处置类标准可包括事件报告与处置指南、安全应急演练指南、应急响应计划等。

另外，各行业领域保护工作部门可在上述各环节通用标准基础上，牵头组织制定本领域的相关标准或工作指引。

二、重要标准定位

1. 识别认定类标准

识别认定类标准用于指导对CII的关键业务及资产、依赖关系等进行识别。

1） 关键信息基础设施要素识别指南标准定位：该标准用于CII确定之后，指导运营者划定CII的重点保护范围、确定关键资产、涉及多责任方的保护责任识别等。

使用范围：关键信息基础设施运营者。

与其他标准关系：

——与《CII安全保护要求》：本标准可用于指导保护工作部门及运营者落实《CII安全保护要求》中分析识别环节的工作。

——与《CII安全测评要求》：本标准可用于指导评估机构对被评估CII的业务、业务链以及资产的分析识别工作。

2. 安全保护类标准

安全保护类标准分为适用于所有CII的标准以及适用于特殊行业领域CII的标准。通用性的标准包括CII安全保护要求、CII安全控制措施、CII安全从业人员要求、CII安全服务机构要求、供应链安全管理要求、CII安全

运维要求等，各行业标准为根据CII的技术特性、系统特点等编制的特殊保护要求标准。

1） 关键信息基础设施安全保护要求标准定位：为通用性的保护指导标准，规定CII在分析识别、安全防护、检测评估、监测预警、主动防御、事件处置等方面的安全要求，是各CII开展安全保护工作时，需在等级保护要求基础上增强的最低要求。

使用范围：关键信息基础设施保护工作部门及运营者。

与其他标准关系：

——与GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求：在GB/T 22239第三级安全通用要求基础上的增强要求，不重复第三级安全通用要求。

——与《CII安全控制措施》：《CII安全控制措施》依据本标准中各要求项提出落地措施。——与《CII安全测评要求》：《CII安全测评要求》给出本标准中提出的各要求项的具体测评方法。

2） 关键信息基础设施安全控制措施标准定位：为《CII安全保护要求》提出的各项要求提供实施落地指导，该标准内容力求全面，针对《CII安全保护要求》的每一项安全要求，力争写出不同实现强度的安全控制措施，供CII保护工作部门及运营者在落地实施时选择参考。

使用范围：关键信息基础设施保护工作部门及运营者。

与其他标准关系：与《CII安全保护要求》关系见“1）关键信息基础设施安全保护要求”部分。

3. 检测评估类标准

检测评估类标准包括对CII的保护状况评估、安全保护能力评估以及评估机构要求等方面。涉及到的标准包括安全测评要求、测评过程指南、检查评估指南、防护能力评价方法、保障指标体系等。

1） 关键信息基础设施安全测评要求标准定位：该标准与《CII安全保护要求》为姊妹篇，定位类似于GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求，从第三方评估机构开展安全评估的角度，而非监管部门的安全检查角度，提出相应的安全评估方法。针对《CII安全保护要求》的各项要求内容，描述对应的测评方法。

使用范围：关键信息基础设施评估机构。

与其他标准关系：

——与《CII安全保护要求》：对于要求条款给出测评方法。

——与《CII安全测评过程指南》：共同指导CII检测评估活动。

——与GB/T 28448：在GB/T 28448单项测评结果基础上加强测评深度，评价融合等级测评结果。

——与《信息安全风险评估方法》：风险评估思路与其保持一致。

——与《CII安全防护能力评价方法》和《CII安全检查评估指南》：作为评价防护能力及检查评估结果的输入。

2） 关键信息基础设施安全测评过程指南标准定位：该标准与《CII安全测评要求》共同指导关键信息基础设施安全检测评估工作，定位类似于GB/T 28449-2018信息安全技术 网络安全等级保护测评过程指南，从第三方评估机构开展安全评估的角度，提出相应的安全评估过程及工作任务。

使用范围：关键信息基础设施评估机构。

与其他标准关系：与《CII安全测评要求》：共同指导CII检测评估活动。

3） 关键信息基础设施安全检查评估指南标准定位：该标准明确CII检查评估的方法、流程和内容，用于保护工作部门开展CII安全检查评估。

使用范围：关键信息基础设施保护工作部门。

与其他标准关系：《CII安全测评要求》作为本标准测评证据的输入。

4. 监测预警类标准

监测预警类标准主要用于指导运营者日常如何对CII进行监测、情报评估以及信息共享等，包括安全监测预计要求、网络安全预警指南、网络安全信息共享指南、网络安全信息报送与态势研判指南等。

1） CII安全监测预警要求标准定位：该标准针对CII安全监测预警工作提出规范要求，包括监测点的部署、监测数据的汇总及分析技术要求、监测数据的管理要求等等。

使用范围：关键信息基础设施运营者、监测服务机构、产品提供者。

与其他标准关系：为《CII安全保护要求》中监测预警相关要求内容的细化。

2） 关键信息基础设施安全威胁信息接口要求标准定位：规定漏洞信息、威胁信息进行安全共享时所采用的格式、接口、索引标签要求等，在此基础上开展威胁漏洞评级。

使用范围：关键信息基础设施运营者、网络安全服务机构、其他科研机构以及有关部门。

与其他标准关系：为《网络安全信息共享指南》在关键信息基础设施保护领域的特殊要求，相同内容应保持一致。

5. 主动防御类标准

主动防御类标准主要用于指导运营者落实《CII安全保护要求》中的相应条款。主要包括《关键信息基础设施主动防御技术要求》。

标准定位：该标准针对《CII安全保护要求》中的主动防御类条款，指导关键信息基础设施保护工作部门及运营者如何具体落实。

使用范围：关键信息基础设施保护工作部门、运营者、安全服务机构。

与其他标准关系：为《CII安全保护要求》中相关要求内容的细化。

6. 事件处置类标准

事件处置类标准主要用于指导保护工作部门、运营者在发生安全事件时如何快速处置，包括安全事件报告与处置指南、应急演练指南、应急体系框架、信息安全应急响应计划规范等

1） 关键信息基础设施安全事件处置要求标准定位：该标准指导CII运营者将其运营CII可能发生的安全事件分类分级，为不同类别不同级别事件的处置奠定基础。指导CII运营者不同类别和级别的事件如何进行处置，包括何种情况向保护工作部门汇报、何种情况向国家相关管理部门汇报等等。使用范围：关键信息基础设施运营者。

与其他标准关系：

——基于已有国标《GB/Z 20986-2007信息安全事件分类分级指南》，着眼在CII面临的安全事件。

——与《网络安全预警指南》中的报送内容及方式保持一致。

2） 关键信息基础设施安全应急演练指南标准定位：该标准规范CII的应急演练，尤其是跨部门、跨单位、跨行业的演练指导。

使用范围：关键信息基础设施保护主管部门、保护工作部门、运营者。

与其他标准关系：该标准应在《网络安全事件应急演练通用指南》的基础上提出关键信息基础设施的应急演练相关内容，包括机构组织、工作方案、脚本、流程、评估方案、保障措施等演练方案内容等，尤其应加强跨部门、跨单位、跨行业的演练指导内容。

标准体系完善是一个长期持续的过程，随着关键信息基础设施保护周边状况变化，以及主管部门管理工作的需要，需不断完善更新。

作者袁静，系公安部第三研究所评估中心 咨询部副主任。

国标委等17部委联合发文 促进团体标准规范优质发展

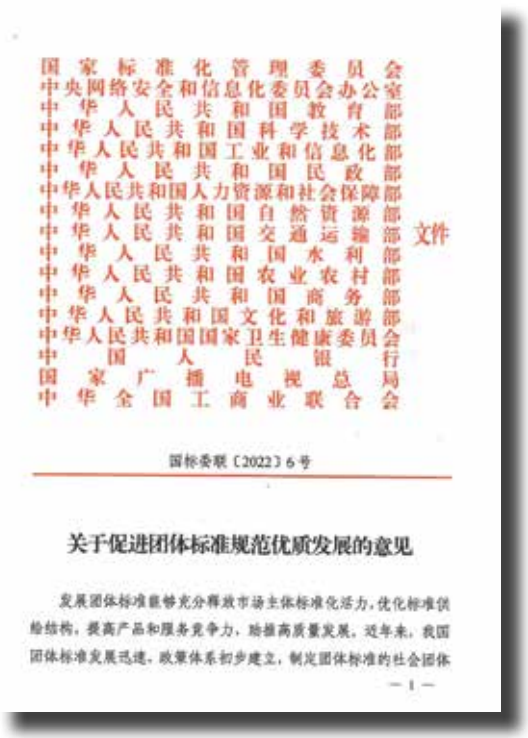
国家标准化管理委员会

2月23日，为进一步贯彻落实《国家标准化发展纲要》，规范团体标准化工作，助力团体标准优质发展，国家标准化管理委员会等17部门联合发布了《关于促进团体标准规范优质发展的意见》，从提升团体标准组织标准化工作能力、建立以需求为导向的团体标准制定模式、拓宽团体标准推广应用渠道、开展团体标准化良好行为评价、实施团体标准培优计划、促进团体标准化开放合作、完善团体标准发展激励政策、增强团体标准组织合规性意识、加强社会监督和政府监管、完善保障措施十个方面提出了指导意见。

WAPI产业联盟是国家标准委首批团体标准试点单位，十六年来，联盟围绕新技术、新产品、新业态和新基建的发展需要，先行制定满足产业快速发展和市场急需的团体标准，引导企业和市场执行团体标准；强化团体标准与国际标准、国家标准、行业标准、企业标准的有效衔接；促进团体标准被国家标准、行业标准引用，将技术水平高、实施效果好、满足产业发展重点需要的团体标准推进为行业标准、国家标准。截至目前，联盟已发布团体标准83项，其中36项已转化为国家标准。

后续，联盟将贯彻落实《意见》的具体要求，发挥社会组织的创新联合体作用，围绕产业链供应链需求，制定原创性、高质量的团体标准，服务市场需求。

《意见》原文如下：



国家标准化管理委员会
中央网络安全和信息化委员会办公室
中华人民共和国教育部
中华人民共和国科学技术部
中华人民共和国工业和信息化部
中华人民共和国民政部
中华人民共和国人力资源和社会保障部
中华人民共和国自然资源部
中华人民共和国交通运输部
中华人民共和国水利部
中华人民共和国农业农村部
中华人民共和国商务部
中华人民共和国文化和旅游部
中华人民共和国国家卫生健康委员会
中国人民银行
国家广播电视总局
中华全国工商业联合会

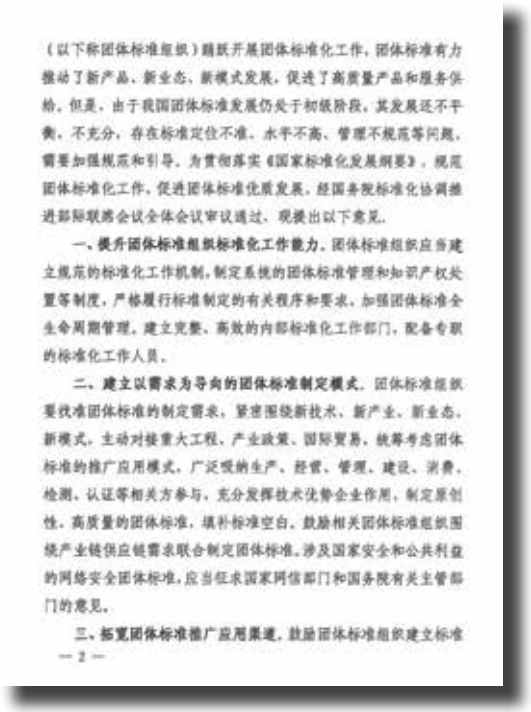
文件

国标委联〔2022〕6号

关于促进团体标准规范优质发展的意见

发展团体标准能够充分释放市场主体标准化活力，优化标准供给结构，提高产品和服务竞争力，助推高质量发展。近年来，我国团体标准发展迅速，政策体系初步建立，制定团体标准的社会团体

— 1 —



（以下称团体标准组织）踊跃开展团体标准化工作，团体标准有力推动了新产品、新业态、新模式发展，促进了高质量产品和服务供给。但是，由于我国团体标准发展仍处于初级阶段，其发展还不平衡、不充分，存在标准定位不准、水平不高、管理不规范等问题，需要加强规范和引导。为贯彻落实《国家标准化发展纲要》，规范团体标准化工作，促进团体标准优质发展，经国务院标准化协调推进部际联席会议全体会议审议通过，现提出以下意见。

一、**提升团体标准组织标准化工作能力。**团体标准组织应当建立规范的标准化工作机制，制定系统的团体标准管理和知识产权处置等制度，严格履行标准制定的有关程序和要求，加强团体标准全生命周期管理，建立完整、高效的内部标准化工作部门，配备专职的标准化工作人员。

二、**建立以需求为导向的团体标准制定模式。**团体标准组织要找准团体标准的制定需求，紧密围绕新技术、新产业、新业态、新模式，主动对接重大工程、产业政策、国际贸易，统筹考虑团体标准的推广应用模式，广泛吸纳生产、经营、管理、建设、消费、检测、认证等相关方参与，充分发挥技术优势企业作用，制定原创性、高质量的团体标准，填补标准空白。鼓励相关团体标准组织围绕产业链供应链需求联合制定团体标准。涉及国家安全和公共利益的网络安全团体标准，应当征求国家网信部门和国务院有关主管部门的意见。

三、**拓宽团体标准推广应用渠道。**鼓励团体标准组织建立标准

— 2 —

制定、检验、检测、认证一体化工作机制，推动团体标准在招投标、合同履约等市场活动中实施应用，打造团体标准品牌，大力开展团体标准宣传，提高社会对团体标准的认知度与认可度。标准化行政主管部门和有关行政主管部门按照国家有关规定开展团体标准应用示范工作。

四、开展团体标准化良好行为评价。国务院标准化行政主管部门完善团体标准化良好行为系列国家标准，鼓励团体标准组织根据团体标准化良好行为系列国家标准开展自我评价，自愿在全国团体标准信息平台上公开声明，进入团体标准化良好行为清单，提升团体标准组织的诚信和影响，供相关方使用团体标准时参考。团体标准的使用方或采信方，可以自行评价或委托具有专业能力和权威性的第三方机构进一步对团体标准组织标准化良好行为进行评价，作为使用和采信团体标准的重要依据。

五、实施团体标准培优计划。国务院标准化行政主管部门会同有关部门，紧贴国家战略性新兴产业、对接区域重大战略，聚焦科技创新和社会治理现代化，制定团体标准培优领域清单，建立培优团体标准组织库，选择具备能力的团体标准组织进行培优，建立对培优团体标准组织工作绩效的科学考核评估机制，形成有进有出的动态调整机制，培养一批优秀的团体标准组织，发挥标杆示范作用，带动团体标准化工作水平整体提升。

六、促进团体标准化开放合作。鼓励基于团体标准提出国际标准提案，支持符合条件的团体标准组织承担国际标准组织的国内技

术对口单位，推荐有能力的专家成为国际标准注册专家。鼓励团体标准组织建立吸纳外商投资企业和外国专家参与团体标准制定的机制。

七、完善团体标准发展激励政策。国务院标准化行政主管部门建立健全推荐性国家标准采信团体标准的机制，会同国务院有关行政主管部门共同推动将团体标准作为科研项目成果的重要考核指标之一。鼓励各部门、各地方将在助推经济社会高质量发展中取得显著成效的团体标准纳入奖励范围。鼓励企业、高等院校、科研机构等用人单位在职称评定中增加团体标准的评分权重。鼓励有关部门建立相关融资增信制度，激励企业通过执行团体标准提供高质量产品和服务。

八、增强团体标准组织合规性意识。团体标准组织应当加强诚信自律，依据章程规定的业务范围开展团体标准化工作；已有强制性标准的，不得重复制定团体标准；不得出现抄袭标准等侵犯标准著作权的行为；禁止利用团体标准化工作的名义进行营利和违法违规收费；不得利用团体标准从事法律法规禁止的事项。团体标准组织要建立完善投诉受理机制，发现确实存在问题的，要及时进行改正。

九、加强社会监督和政府监管。任何单位或者个人有权对违法违规的团体标准化行为进行投诉和举报。各级标准化行政主管部门加强对团体标准的监督，优化“双随机、一公开”监管模式，对违反法律法规，不符合强制性国家标准，侵犯标准著作权等问题依法依

规进行处理，通过全国团体标准信息平台向社会公布团体标准组织违法违规行为和处理结果，并向有关行政主管部门通报相关信息。充分发挥新闻媒体对团体标准的正面引导和监督作用，对团体标准组织形成约束力。

十、完善保障措施。各级标准化行政主管部门、有关行政主管部门要认识到位、措施到位、行动到位，做好工作安排部署，加强协同配合，形成工作合力。及时总结团体标准发展的经验和模式，解决和预防团体标准发展过程中的重大问题和潜在风险。进一步加强团体标准相关政策的宣传，提升业务指导和支持能力，促进团体标准组织间的交流合作，相互协调，推动专业标准化技术委员会、标准化研究机构服务支持团体标准化工作，为团体标准化工作提供专业化支撑。

（此件公开发布）

主送：各省、自治区、直辖市和新疆生产建设兵团市场监管局（厅、委）、网信办、教育厅（教委）、科技厅（委、局）、工业和信息化主管部门、民政厅（局）、人力资源社会保障厅（局）、自然资源主管部门、交通运输厅（局、委）、水利（水务）厅（局）、农业农村（农牧）厅（局、委）、商务主管部门、文化和旅游厅（局）、卫生健康委、中国人民银行省会（首府）城市中心支行以上分支机构、广播电视局、工商联、各有关社会团体。

抄送：国务院有关部门。

国家标准化管理委员会标准处　　2022年2月18日印发

2021年国内网络安全相关立法回顾及思考

中国信息安全　方　禹

【编者按】网络安全是网络空间的基础性保障问题，网络空间越来越成为社会治理的主要载体，网络安全问题不仅是国家安全的主要内容，也可能成为社会安全的底层逻辑。近年来，为应对日益严峻的网络安全形势，我国网络安全政策和法律体系不断完善，网络安全产业发展进入“快车道”。2021年，网络安全相关配套立法得以长足完善，同时网络法治精细化发展趋势，也使得部分领域从网络安全体系中抽离和分立，促进整体网络法治体系的结构化完善。本期与您分享中国信息通信研究院互联网法律研究中心方禹主任文章，对我国网络安全立法进行回顾和思考。

2021年，网络领域重要立法密集出台，网络法治体系进一步充实完善，是网络立法繁荣发展的重要一年。广义来看，《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》等相继出台实施，网络安全领域立法大为充实。同时，网络安全领域配套规则逐步明确清晰，为网络安全相关工作提供了确定的指引。

一、网络安全法律体系概述

2016 年，《网络安全法》正式出台，以网络安全法为基础和上位法依据，国家有关部门陆续出台配套法规、规章和规范性文件，逐步形成了系统的网络安全法律体系，主要覆盖网络运行安全、个人信息保护和网络内容管理等三个方面。

一是网络运行安全。《网络安全法》首要解决的就是网络作为对象的安全性问题，网络入侵、网络攻击等非法活动，对电信、能源、交通、金融等领域产生了严重威胁，云计算、大数据、物联网等新技术、新应用面临着更为复杂的网络安全环境。从体系上看，《网络安全法》对网络运行作出了一般性规定。在关键信息基础设施保护方面，出台了《关键信息基础设施安全保护条例》；在网络安全审查方面，出台了《网络安全审查办法》，并根据情况变化正在进行修订；在网络漏洞管理方面，出台了《网络产品安全漏洞管理规定》。通过系列配套规则，明确和完善了《网络安全法》相关要求。

二是个人信息安全。《网络安全法》对个人信息安全作出了原则性、概括性规定。以《网络安全法》为依据，在国家网信办统筹指导下，工信部起草了《移动应用程序个人信息保护管理规定》。国家网信办出台了《儿童个人信息网络保护规定》，牵头制定出台了《常见类型移动互联网应用程序必要个人信息范围规定》等配套规定。在《个人信息保护法》颁布实施前，《网络安全法》及其配套规定，为个人信息保护工作提供了依据和保障。

三是网络内容管理。《网络安全法》为网络内容管理提供了充实的上位法依据。国家网信办以《网络安全法》为基础，基本形成了“2+N”的网信法律体系。“2”是指两部部门规章，国家网信办修订出台《互联网新闻信息服务管理规定》，规范了互联网新闻信息服务活动；制定了《网络信息内容生态治理规定》，从治理的高度对网络信息内容管理提出了新要求。“N”是指一系列规范性文件，覆盖了音视频、网络直播、公众账号、移动应用程序、即时通信工具、跟帖评论、微博客等领域，为全面依法治网提供了有力的法治基础。

随着技术发展和普及，《网络安全法》时代的形势和客观条件都发生了变化。今年，《数据安全法》和《个人信息保护法》相继出台实施，《网络安全法》所规范的有关活动和对象也出现了变化和调整。

二、网络安全法律体系调整及内涵外延变化

伴随《网络安全法》的深入推进实施，特别是普法宣传、执法培训相关活动丰富化、常态化，《网络安全法》的生命力和活力持续得以释放。同时，在《网络安全法》实施过程中，网络技术与应用继续深入发展和普及，进一步改变人们生产、生活的组织方式，网络安全法律体系的内涵和外延出现变化和调整。

从网络法治体系的整体结构看，党的十八届四中全会和中央全面依法治国工作会议对法治建设及依法治网提出了总体性、纲领性要求。党的十八大以来，尤其是党的十九大以来，网络法治建设快速推进。网络法具有跨领域性，普遍认为网络法属于领域法学。法律科学不属于纯粹理论，而是实践理论。网络活动日益普及和丰富，网络空间逐步成为社会生活的基本载体，网络法治研究持续深入，即将或者已经能够支撑网络法成为独立的法律部门。学科的繁荣势必伴随着细分化、专业化的过程。从今年来看，网络安全法律体系作为网络法的主要组成部分，也发生了调整和变化，呈现出精细化、聚焦化的特点，有些内容逐渐独立成体系，从网络安全框架中剥离并与之并行。

按照 2016 年出台的《网络安全法》架构，相关法律主要包括网络设施和运行安全（包括关键信息基础设施）、网络信息安全等方面。其中，《网络安全法》以“网络信息安全”囊括了内容安全和个人信息安全，聚焦网络内容管理和个人信息权益。近年来，随着实践变化和理论研究深入，相应发生了一些变化，尤其表现为网络内容管理和个人信息保护逐步自成体系的趋势。

在网络内容管理方面，有关部门以《网络安全法》为上位法依据，出台了相关内容管理的部门规章和规范性文件，基本形成了完善的制度体系。党的十九大首次明确了“意识形态安全”的重要性，互联网和移动互联网技术发展，以及人工智能等新技术普及和应用，进一步拓展了网络空间的公共表达渠道和内容供给模式。2019 年底，国家互联网信息办公室出台《网络信息内容生态治理规定》，将管理思维转变为治理思维，体现多元主体共同参与，同时也将内容管理“二分法”（违法信息和合法信息）调整为“三分法”（违法信息、不良信息和合法信息）。在此基础上，网络内容管理立法体系相应进行了调整。今年以来，国家互联网信息办公室制定了《互联网用户公众账号信息服务管理规定》，启动了《互联网用户账号名称信息管理规定》修订工作。

在个人信息保护方面，《网络安全法》对个人信息保护做出了原则性、概括性规定，以保护个人信息为主要目的。而近年来，个人信息保护实践日益普遍，主体多元、类型多样、场景丰富，大规模收集、使用个人信息的活动越来越成为常态，侵害个人信息权益的行为更为普遍，个人信息保护已经成为广大人民群众最关心最直接最现实的利益问题之一。同时，个人信息具有丰富的数据价值，对其合理利用也是数字经济发展的基础之一。个人信息保护统一立法的全球趋势也十分明显。结合国内外情况，有必要制定全面性、基础性的个人信息保护法律。今年 8 月，《个人信息保护法》正式通过，并于 11 月起实施。《个人信息保护法》作为个人信息领域的基础性法律，对个人信息保护进行了整体安排和制度重构，立法目的既包括对个人信息的保护，也包括个人信息合理利用。《个人信息保护法》对《网络安全法》中有关个人信息保护的内容进行了大幅拓展和一定程度调整，规定了个人信息处理的合法性基础、个人信息处理者的义务、个人在个人信息处理活动中的权利、个人信息保护监管体制等主要内容，基本覆盖了个人信息保护的各个方面，下一步将继续形成个人信息保护法律体系。

从网络安全法律体系自身来看，其组成架构也发生了变化和调整。一方面，传统的网络安全问题还是比较突出，传统网络攻击形式，如分布式拒绝服务（DDos）攻击仍然呈现持续上升趋势，2021年 DDos 攻击的数量、规模较往年继续上升。《网络安全法》继续发挥应对传统网络安全的重要作用，今年以来，相关配套立法也相继出台，进一步规范网络安全相关工作。另一方面，5G、物联网等技术发展普及，不断改变网络连接方式和连接对象，物理空间和网络空间的边界不断融合、模糊，内生式网络安全问题不断产生，其中明显以数据为主要对象。网络治理问题很大程度上已经凸显为数据治理问题，网络安全问题正在不断聚焦成为数据安全问题。围绕数据展开的一系列讨论越来越丰富，越来越深入。相关数据立法工作也在加速推进，逐步形成数据治理顶层法律体系。数据安全、数据权属等问题倍受关注，各方都期待数据领域能够广泛达成共识，建立起明确的数据活动规则，谋求安全与发展平衡之道。

三、网络安全配套法规体系持续完善

今年，《网络安全法》已经实施了四年。2016 年，习近平总书记在网络安全和信息化工作座谈会上做重要讲话指出，维护网络安全，要“聪者听于无声，明者见于未形”。如今，《网络安全法》制定之时的所听所见也都成为现实的迫切问题。《网络安全法》的制度潜力不断释放，依然是网络治理领域的重要法治依据。2021 年，以《网络安全法》为上位法的配套规定相继出台，有关具体要求得以确定。

一是关键信息基础设施安全保护法律制度最终明确。关键信息基础设施保护是网络安全的重要部分，主要思路是将为社会运转提供基础性、关键性服务的设施列为关键信息基础设施，并予以保护。美国、德国、日本、澳大利亚等都通过立法对关键基础设施进行保护。今年 7 月，《关键信息基础设施安全保护条例》（以下简称《条例》）正式出台。作为《网络安全法》的重要配套立法，《条例》积极应对国内外网络安全保护的主要问题和发展趋势，为下一步加强关键信息基础设施安全保护工作提供了重要法治保障。《条例》界定了适用范围、监管主体、评估对象等关键信息基础设施安全保护相关基本要素，提出了安全保护要求及措施，确保对

象具体、权责清晰、任务明确，为安全保护工作开展提供系统指引和工作遵循。

关键信息基础设施的范围一直是各方面关心的核心问题。《网络安全法》中有关三同步、供应链安全、跨境数据流动、风险评估等要求都仅适用关键信息基础设施运营者。确定关键信息基础设施运营者是开展关键信息基础设施安全保护工作的基础，有关主体十分关心自己是否以及如何被列入关键信息基础设施范围的问题。《条例》对此采取了主管部门认定和单独通知的流程，规定由负责关键信息基础设施安全保护工作的部门制定认定规则，组织认定本行业、本领域的关键信息基础设施，及时将认定结果通知运营者，并报国务院公安部门。

二是网络漏洞管理进一步完善。网络漏洞是网络安全中的主要隐患之一，需要有效的机制措施来防范和消除风险。《网络安全法》要求网络产品、服务提供者发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当采取补救措施并通知用户和报告主管部门；要求网络运营者及时处理系统漏洞等安全风险；规定“向社会发布系统漏洞……等网络安全信息，应当遵守国家有关规定”。今年 7 月，工业和信息化部、国家互联网信息办公室、公安部联合制定出台《网络产品安全漏洞管理规定》，推动网络产品安全漏洞管理工作的制度化、规范化、法治化，提高相关主体漏洞管理水平，引导建设规范有序、充满活力的漏洞收集和发布渠道，防范网络安全重大风险，保障国家网络安全。

三是供应链安全要求进一步深化。供应链安全是适应网络安全全周期、长链条等特点的子命题之一。《网络安全法》中对关键信息基础设施运营者采购产品和服务，规定了国家安全审查（即网络安全审查）的要求。2020 年，国家互联网信息办公室会同国家发展和改革委员会、工业和信息化部、公安部等十二部门联合制定出台了《网络安全审查办法》，加强关键信息基础设施供应链安全，确保国家安全。今年 7 月，国家互联网信息办公室修订了该办法，并就《网络安全审查办法（修订草案征求意见稿）》向社会公开征求意见。征求意见稿将供应链安全的主体进一步扩大到数据处理者，调整范围覆盖数据处理活动，体现了数据活动在供应链安全中的风险因素。

四是具体领域进一步细化配套规则。7 月 5 日，国家互联网信息办公室会同国家发展和改革委员会、工业和信息化部、公安部、交通运输部制定出台《汽车数据安全管理若干规定（试行）》，对汽车数据处理活动中的重要数据和个人信息予以保护，维护国家安全、数据安全和个人权益。9 月 13 日，工业和信息化部发布《关于加强车联网卡实名登记管理的通知》，明确不同销售阶段车联网卡实名登记要求，防范车联网中的安全风险。9 月 15 日，工业和信息化部发布《关于加强车联网网络安全和数据安全工作的通知》，对车联网的网络安全和数据安全提出了基本要求。

五是反电信网络诈骗提上立法议程。今年 10 月，《反电信网络诈骗法（草案）》提交全国人大常委会首次审议，并向社会公开征求意见。草案的制定秉持了“小切入立法”以及“急用先行”的原则，对现实需求做出回应的同时，全面提升反电信网络诈骗工作的法治化、规范化水平。草案立足源头治理，打击“两卡”犯

罪，强化实名制管理，突出新技术整治，完善救济措施，对内建立全链条整治工作机制，对外积极稳妥推进国际执法司法合作。

四、数据安全、个人信息保护、算法等立法快速推进

《网络安全法》在网络治理过程中发挥了重要的作用，也将持续提供制度供给。与此同时，数据安全、个人信息保护、算法等领域问题凸显，场景越来越丰富，活动越来越频繁，亟需立法规制。从历史意义和广义来看，这些法律法规也可以纳入网络安全法律体系的视角。

一是数据安全领域确立基础性法律。数据是数字经济的基础性战略资源，数据治理能力是国家竞争力的体现。2017 年，习近平总书记提出“要加强政策、监管、法律的统筹协调，加快法规制度建设。要制定数据资源确权、开放、流通、交易相关制度，完善数据产权保护制度。”《数据安全法》今年 6月正式出台，数据治理制度实现从无到有的“突破”，成为我国数据安全领域基础性法律。《数据安全法》对数据分类分级、重要（核心）数据管理、数据安全审查等作出了明确规定，同时，在《网络安全法》的基础上，完善了跨境数据流动的管理要求，回应了关键信息基础设施以外的重要数据的跨境管理诉求。

二是跨境数据流动规则进一步构建完善。《数据安全法》《个人信息保护法》出台后，与《网络安全法》相衔接，完善了跨境数据管理制度。总体来看，跨境数据流动管理制度覆盖了关键信息基础设施运营者、重要数据处理者和个人信息处理者等主体，包括安全评估、认证、标准合同等具体手段。今年 10 月，国家互联网信息办公室对《数据出境安全评估办法（征求意见稿）》公开征求意见，该办法以《网络安全法》《数据安全法》《个人信息保护法》为上位法，细化和明确了我国跨境数据安全自由流动的具体规则，是我国数据治理框架性法律正式成型后，在数据出境安全管理系列规范中具有关键意义和地位的配套规则。

三是数据安全配套立法快速启动。今年 11 月，国家互联网信息办公室发布《网络数据安全管理条例（征求意见稿）》向社会公开征求意见，对网络数据处理活动中涉及的个人信息保护、重要数据安全管理、跨境数据流动规范等内容进行了全方位、多层次的细化规定。该条例将成为《数据安全法》的主要配套规则之一。

四是算法对经济和社会的影响逐步扩大，滋生了“大数据杀熟”“信息茧房”等损害公众利益，破坏正当竞争，扰乱社会秩序的行为。有关部门在高位阶立法对算法概括性要求的基础上，进一步深入推进，从内容安全、社会管理、市场秩序等多维度价值导向层面对算法推荐进行规范。

2021 年 8 月，国家互联网信息办公室发布了《互联网信息服务算法推荐管理规定（征求意见稿）》，对算法推荐技术作出专门管理规定。该规定以互联网信息服务为基础，从算法的公平公正及信息内容角度对算法推荐服务提出了各项具体细化的要求，明确了“算法推荐技术”的范围、算法推荐服务的监管原则与规则以及具体的分级分类、备案、安全评估等监管手段。9 月，国家互联网信息办公室、中宣部、教育部、科技部等九部委印发《关于加强互联网信息服务算法综合治理的指导意见》，提出要利用三年左右时间，逐步建立治理机制健全、监管体系完善、算法生态规范的算法安全综合治理格局。

五、下一步展望

网络安全是网络空间的基础性保障问题，网络空间越来越成为社会治理的主要载体，网络安全问题不仅是国家安全的主要内容，也可能成为社会安全的底层逻辑。2021年，网络安全相关配套立法得以长足完善，同时网络法治精细化发展趋势，也使得部分领域从网络安全体系中抽离和分立，促进整体网络法治体系的结构化完善。

目前，《数据安全法》和《个人信息保护法》已经相继实施，但部分事项还需要配套规定予以明确。《网络数据安全管理条例》《数据出境安全评估办法》等正在加快制定之中，但数据安全、个人信息保护从功能和目标上来看，需要结构化的制度体系，中短期内仍然有大量的配套立法任务。从下一步来看，一方面，要持续补齐，尽快出台数据跨境管理、数据安全管理相关配套立法，确定有关法律制度的具体要求，为具体执法监督提供指引。另一方，面也要观察总结，适时结合新的发展变化，调整、形成思路和方法，修订或者制定相关网络安全法律规定，为我国网络安全工作持续提供法治保障。

作者方禹，系中国信息通信研究院互联网法律研究中心主任。

国务院：

推进市场监管现代化

2022年1月27日，国务院印发《“十四五”市场监管现代化规划》，对推进我国市场监管现代化作出全面部署。

《规划》指出，“十四五”时期要以习近平新时代中国特色社会主义思想为指导，全面贯彻党的十九大和十九届历次全会精神，立足新发展阶段，完整、准确、全面贯彻新发展理念，构建新发展格局，坚持统筹发展和安全、效率和公平、活力和秩序、国内和国际，围绕“大市场、大质量、大监管”一体推进市场监管体系完善和效能提升，推进市场监管现代化，着力营造市场化法治化国际化营商环境、激发市场活力，强化公平竞争政策基础地位、维护市场秩序，坚守安全底线、增强人民群众获得感幸福感安全感，完善质量政策和技术体系、全面提升质量水平，维护和优化高效、有序、统一、安全的超大规模市场，切实推动高质量发展，为全面建设社会主义现代化国家开好局、起好步提供有力支撑。

《规划》提出营商环境持续优化、市场运行更加规范、市场循环充分畅通、消费安全保障有力、质量水平显著提升、监管效能全面提高等目标，并提出六项重点任务：一是要持续优化营商环境，充分激发市场主体活力；二是要加强市场秩序综合治理，营造公平竞争市场环境；三是要维护和完善国内统一市场，促进市场循环充分畅通；四是要完善质量政策和技术体系，服务高质量发展；五是要坚守安全底线，强化消费者权益保护；六是要构建现代化市场监管体系，全面提高市场综合监管效能。

《规划》从五方面完善保障措施，包括强化组织领导、落实职责分工、鼓励探索创新、加强评估考核、引导社会参与。《规划》要求，要加强党对市场监管工作的全面领导，建立统一领导、部门协同、上下联动的工作体系，为市场监管工作创造良好的政策环境、体制环境和法治环境。各地区、各有关部门要研究制定配套政策和具体实施方案，明确工作重点，细化工作举措，推动规划有效落实。各地区要鼓励基层大胆探索，创新工作思路和方法，不断丰富完善有关政策措施；要将规划实施情况纳入政府综合评价和绩效考核，加强督查考核，强化评估结果运用，确保规划落地见效。

国务院：

加强重要行业领域关键信息基础设施网络安全防护能力

2021年12月12日，国务院发布“十四五”数字经济发展规划，强调加强重要行业领域关键信息基础设施网络安全防护能力，指出：要加快建设信息网络基础设施，建设高速泛在、天地一体、云网融合、智能敏捷、绿色低碳、安全可控的智能化综合性数字信息基础设施；要有序推进基础设施智能升级，建设可靠、灵活、安全的工业互联网基础设施，加快推进能源、交通运输、水利、物流、环保等领域基础设施数字化改造；要增强网络安全防护能力，加强网络安全基础设施建设，加强电信、金融、能源、交通运输、水利等重要行业领域关键信息基础设施网络安全防护能力，加强网络安全等级保护和密码应用安全性评估；支持网络安全保护技术和产品研发应用，推广使用安全可靠的信息产品、服务和解决方案。

发改委：

强化国家战略科技力量

2021年12月25日，国家发改委规划司在“十四五”规划《纲要》解读文章中指出，新时期、新形势对强化国家战略科技力量提出新要求。加快科技自立自强是应对新挑战、解决新问题的必然选择，是畅通国内大循环、塑造我国在国际大循环中主动地位的关键。要通过强化国家战略科技力量，更好地发挥新型举国体制优势，整合各方面力量开展协同攻关，加快提升自主创新能力，实现科技自立自强。

国家战略科技力量是国家创新体系的关键组成部分，在各类创新主体组成的“创新金字塔”中，处于塔尖位置，要通过强化国家战略科技力量引领国家创新体系整体效能提升。

网信办：

全面加强网络安全保障体系和能力建设

2021年12月27日，中共中央网络安全和信息化委员会在《“十四五”国家信息化规划》中指出，要全面加强网络安全保障体系和能力建设。加强网络安全核心技术联合攻关，开展高级威胁防护、态势感知、监测预警等关键技术研究，建立安全可控的网络安全软硬件防护体系。实施国家基础网络安全保障能力提升工程，加强关键信息基础设施安全防护体系建设，增强网络安全平台支撑能力。

国家互联网信息办公室等13部门修订《网络安全审查办法》保障关基网络安全和数据安全

2021年12月28日，国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、国家安全部、财政部、商务部、中国人民银行、国家市场监督管理总局、国家广播电视总局、中国证券监督管理委员会、国家保密局、国家密码管理局等十三部门联合修订了《网络安全审查办法》（以下简称《办法》），自2022年2月15日起施行。新《办法》将中国证券监督管理委员会纳入网络安全审查工作机制。

网络安全审查是网络安全领域的重要法律制度。原《办法》自2020年6月1日施行以来，通过对关键信息基础设施运营者采购活动进行审查和对部分重要产品等发起审查，对于保障关键信息基础设施供应链安全，维护国家安全发挥了重要作用。

2021年9月1日，《数据安全法》正式施行，明确规定国家建立数据安全审查制度。国家互联网信息办公室据此对《网络安全审查办法》进行了修订，将网络平台运营者开展数据处理活动影响或者可能影响国家安全等情形纳入网络安全审查范围，并明确要求掌握超过100万用户个人信息的网络平台运营者赴国外上市必须申报网络安全审查，主要目的是为了进一步保障网络安全和数据安全，维护国家安全。

值得关注的是：第一、新修订的《网络安全审查办法》对网络产品和服务进行了进一步的界定，需要注意哪些产品和服务属于网络安全审查的范畴。第二十一条 本办法所称网络产品和服务主要指核心网络设备、重要通信产品、高性能计算机和服务器、大容量存储设备、大型数据库和应用软件、网络安全设备、云计算服务，以及其他对关键信息基础设施安全、网络安全和数据安全有重要影响的网络产品和服务。第二、网络产品和服务提供者与“关基”运营者签署合同时需要注意网络安全审查的时限要求。通常情况下，网络安全审查需要30个工作日。情况复杂的，需要45个工作日。网络产品和服务提供者需要注意这个时限。因为通常情况下，关键信息基础设施运营者应当在与产品和服务提供方正式签署合同前申报网络安全审查。如果在签署合同后申报网络安全审查，建议在合同中注明此合同须在产品和服务采购通过网络安全审查后方可生效，以避免因为没有通过网络安全审查而造成损失。

工信部联合11部门启动网络安全技术应用试点示范工作启动

2022年1月10日，工信部联合11部门发布《关于开展网络安全技术应用试点示范工作的通知》，提出将遴选一批创新、先进、实用、可推广的网络安全技术平台或系统作为试点示范项目并推广落地。本次网络安全技术应用试点示范工作与工信部2021年7月12日《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）》中多项内容相呼应，即“涵盖的行业包括公共通信和信息服务、能源、交通、水利、应急管理面向5G、车联网、工业互联网、物联网等重点方向，开展优秀安全产品及解决方案遴选，促进试点示范项目在各重点行业领域应用推广，促进成果转化”，具体表现为：

1、试点工作涵盖几乎全部网络安全重点行业：此次通知为12部门联合发布，试点示范工作所、金融、医疗、广播电视等多个重要行业领域，与《关键信息基础设施安全保护条例》中关键信息基础设施所以涉及的重要行业领域基本重合，呼应《三年计划》中“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”。

2、9个重点方向全部涉及“新技术新业务新模式”：根据通知，此次试点示范项目涉及云安全、人工智能安全、大数据安全、车联网安全、物联网安全、智慧城市安全、网络安全共性技术、网络安全创新服务、网络安全“高精尖”技术创新平台9个重点方向，呼应《三年计划》中所提到的“新技术新业务新模式”，旨在加强“面向数字化新场景新业务的安全能力建设”。

此次网络安全技术应用试点示范工作可视作《三年计划》逐步落地的起点，主要影响包括：1、将加速“新安全”产品落地；2、表明了政府及行业监管部门对于网络安全预算分配的积极态度，有助于在夯实重点行业在网络安全领域的投入。

国密局等十部委：

为商用密码产业营造高质量发展环境

密码作为国家战略资源，是贯彻习近平总书记网络强国战略思想、落实《国家网络空间安全战略》、保障网络安全与数据安全的核心技术和基础支撑。密码是党和国家的一项特殊重要工作，直接关系到国家政治安全、经济安全、社会安全和人民利益。自2020年1月1日起正式施行的《密码法》，就是坚决贯彻党管密码的根本原则，落实习近平总书记关于密码工作的系列重要指示精神。日前国家密码管理局联合中央网信办、国家发改委、科技部、工信部、公安部、财政部、国资委、市场监管总局、证监会等十部委联合发布《促进商用密码产业高质量发展的若干措施》（以下简称“《若干措施》”），旨在为深入贯彻落实《密码法》，加快推进密码产业高质量发展，切实提升网络空间密码保障能力，制定了具体措施，提出了一系列扶持政策。

（一）强调要走持续深化需求牵引的发展路径。依法督促推进密码应用“三同步”，强化密码评估执法检查。“三同步”是指在网络和信息系统建设时，按照同步规划、同步建设、同步运行的方式建设密码保障系统，并定期评估。通过商用密码应用示范，促进网络身份互信互任和数据信息协同共享。

（二）强调要坚持创新驱动、提升产业链供应链安全稳定水平。要将新一代信息网络、量子信息、人工智能等新兴行业与密码技术深度融合创新，构建数据安全防护建设。要支持密码科技创新，鼓励商用密码单位、企业研发创新型商用密码产品，提升密码技术的高质量供给。

（三）强调要搭建产业发展平台。优化要素资源配置，集聚商用密码产业链、供应链、人才链等领域的优质资源，支持规范商用密码应用与创新发展基地建设，发挥产业链供应链的聚集效应。鼓励引导有关领军企业和大型综合性企业积极布局商用密码创新与产业发展，打造商用密码创新策源地、产业链生态链“链长”。鼓励运用市场规则设立密码基金和创新发展基金，综合运用股权投资、创业投资、风险投资等方式，从产业孵化角度赋能符合条件的商用密码企业，为商用密码企业发展打入“强心剂”。

（四）强调要持续优化完善商用密码产业发展环境。要完善商用密码国家标准和重点行业领域商用密码应用标准体系。要持续完善商用密码产品检测认证体系，强化商用密码应用安全性评估体系建设。通过优化融资担保业务政策，从金融角度赋能符合条件的商用密码企业，为中小微企业发展营造良好的融资环境。此外，还将从资本市场角度支持商用密码企业发展，强化企业兼并重组、融资、上市服务体系。从而建立起产融结合、相互促进的发展环境，有利于商用密码产业长期、快速、全面的高质量发展。

中央军委装备发展部：

优化完善快速支持机制，快速支持应用优质项目

2022年1月18日，中央军委装备部发布《关于优化完善装备预研共用技术领域基金类项目快速支持机制的公告》，优化调整了快速支持机制，最大限度实现开放宽进、流程优化和程序简化，进一步增强了预研共用技术领域基金类项目研究的创新性和灵活性，快速捕捉技术发展的最新动态，快速支持基础前沿、原始创新、潜在的应用优质项目。

（一）快速发现渠道。一是建立了现场征集渠道，现场受理征集项目的咨询、审核、提报等事宜；二是调整了实时平台征集渠道，在全军武器装备采购信息网“快速支持”项目征集专栏，面向军地各类研发力量，收集项目建议，北京中心同时提供征集项目的现场咨询、审核、提报等服务；三是领域专家推荐渠道，由专家组织优势力量有针对性的论证提报项目建议；四是单位择优推荐渠道，军兵种装备机关、相关军地研究院所，可组织优势力量有针对性的论证提报项目建议。五是建立了竞赛推荐优选渠道，由专业组在各类挑战赛、军地相关创新创意大赛和技术比测项目中，优选有特色的新技术，提出项目建议。

（二）快速筛选流程。设立了快速扶持项目和快速转化项目两种类别，由责任专家负责开展项目筛选，原则上，每年3-6月和8-10月，各开展一轮项目征集，7月和11月各办理一批。

（三）快速实施程序。快速扶持项目采取分类分阶段支持的方式，第一阶段，侧重新理论新概念研究，以及原创性强、研究风险大的项目，资助经费额度20-50万元，第二阶段，侧重技术路径相对明确、具备一定潜在应用基础的项目，资助经费额度100-200万元；快速转化项目，主要开展技术转化应用研究攻关，资助经费额度500-1000万元，研究周期1-2年。

技术创新联盟被列入新修订的《中华人民共和国科学技术进步法》

2021年12月24日，第十三届全国人民代表大会常务委员会第三十二次会议审议通过了新修订的《中华人民共和国科学技术进步法》，自2022年1月1日起施行。这是继《中华人民共和国科技成果转化法》之后，又一部国家层面的科技法，明确提出要鼓励技术创新联盟的组建、鼓励社会组织参与科学技术进步活动，将为产业联盟这类社会组织的健康发展提供法律保障。

与联盟等社会组织相关的法条包括：第十一条，国家营造有利于科技创新的社会环境，鼓励机关、群团组织、企业事业单位、社会组织和公民参与和支持科学技术进步活动。第三十一条，国家鼓励企业、科学技术研究开发机构、高等学校和其他组织建立优势互补、分工明确、成果共享、风险共担的合作机制，按照市场机制联合组建研究开发平台、技术创新联盟、创新联合体等，协同推进研究开发与科技成果转化，提高科技成果转移转化成效。第三十七条，引导科学技术研究开发机构、高等学校、企业和社会组织共同推进国家重大技术创新产品、服务标准的研究、制定和依法采用，参与国际标准制定。第八十一条，国家鼓励企业事业单位、社会组织通过多种途径建设国际科技创新合作平台，提供国际科技创新合作服务。鼓励企业事业单位、社会组织和科学技术人员参与和发起国际科学技术组织，增进国际科学技术合作与交流。

工信部、国标委：

支持社会团体参与工业互联网标准化工作

2021年12月24日，工信部、国标委在联合发布的《工业互联网综合标准化体系建设指南（2021版）》中指出，要进一步加快安全防护、安全管理、安全应用服务等标准研制；要加强可复制、可推广的应用模式和实施路径等标准的制定；要引导标准化技术组织、产业技术联盟等积极参与工业互联网标准化工作，鼓励社会团体围绕工业互联网的新技术新需求制定先进团体标准，支持产业技术联盟、标准化技术组织等开展工业互联网标准的宣传培训，引导和帮助企业执行标准。

工信部：

支持创建京津冀工业互联网协同发展示范区

近日，工业和信息化部办公厅在给北京市经济和信息化局、天津市工业和信息化局、河北省工业和信息化厅的复函中明确支持创建京津冀工业互联网协同发展示范区。工信部将加强对示范区创建工作的指导和协调，支持北京市、天津市和河北省，以示范区建设为重要抓手，立足自身实际，发挥三地优势，在基础设施联通、科技创新攻关、融合应用提升、产业生态营造等方面开展先行先试，加快形成可复制、可推广的发展经验，聚力打造工业互联网发展新高地，助力制造业高质量发展。

科技部：

营造更好环境，支持科技型中小企业研发

2022年1月13日，科技部在《关于营造更好环境支持科技型中小企业研发的通知》中提到，到“十四五”末，形成支持科技型中小企业研发的制度体系，营造全社会支持中小企业研发的环境氛围，科技型中小企业数量新增20万家。增强科技型中小企业研发能力，实现“四科”标准科技型中小企业新增5万家。“四科”标准科技型中小企业，指的是每个科技企业要拥有关键核心技术的科技产品、科技人员占比大于60%、以高价值知识产权为代表的科技成果超过5项、研发投入强度高于6%。

《通知》指出，要优化科技计划支持研发机制，在国家重点研发计划重点专项中，单列一定预算资助科技型中小企业研发活动，精准支持具备条件的科技型中小企业承担国家科技任务，加快培养一批研发能力强、技术水平高、科技人才密集、能够形成核心技术产品等“四科”特征明显的科技型中小企业。同时，优化国家科技成果转化引导基金绩效评价制度，将支持科技型中小企业突破关键核心技术作为重要绩效考核指标等。

围绕创造支持科技型中小企业研发的应用场景，夯实支持科技创新创业的基础条件。国家创新型城市、国家自主创新示范区等要向科技型中小企业开放智慧城市、重大工程等应用场景，发布场景清单，形成一批具有核心竞争力和商业价值的示范产品；支持探索科技型中小企业创新产品政府采购制度等。

中国人民银行等四部门印发《金融标准化”十四五”发展规划》

加强金融业网络安全防护能力

2月8日，中国人民银行、市场监管总局、银保监会、证监会四部门在联合印发的《金融标准化“十四五”发展规划》中指出，要健全金融业网络安全、数据安全和关键信息基础设施保护标准体系，支持提升安全防护能力。要加强金融网络安全能力评估、风险排查、安全防御、漏洞管理等标准建设，助力提升网络安全威胁发现、监测预警、应急处置、攻击溯源能力，推动商用密码应用等标准供给与实施。针对服务器端与终端有关技术，要制定具有安全可控能力的信息技术规范。要鼓励在金融信息安全等重点领域提供市场化检测认证服务，鼓励各类市场主体、社会组织和政府部门采信检测认证结果。

央行发布《金融科技发展规划（2022–2025年）》

明确数据安全

2021年12月31日，中国人民银行印发《金融科技发展规划（2022-2025年）》（以下简称《规划》）。《规划》提出新时期金融科技发展指导意见，明确金融数字化转型的总体思路、发展目标、重点任务和实施保障。

《规划》明确要求做好数据安全保护。严格落实数据安全保护法律法规、标准规范，明确数据安全负责人和管理机构，综合运用声明公示、用户明示等方式，明确原始数据和衍生数据收集目的、加工方式和使用范围，确保在用户充分知情、明确授权前提下规范开展数据收集使用，避免数据过度收集、误用、滥用。建立健全数据全生命周期安全管理长效机制和防护措施，运用匿踪查询、去标记化、可信执行环境等技术手段严防数据逆向追踪、隐私泄露、数据篡改与不当使用，依法依规保护数据主体隐私权不受侵害。建立历史数据安全清理机制，利用专业技术和工具对超出保存期限的用户数据进行及时删除和销毁，定期开展数据可恢复性验证确保数据无法还原。确需作为样本数据保存的，应经用户同意并进行去标识化处理，移入非生产数据库保存，确保用户隐私信息不被直接或间接识别，切实保障用户数据安全。

陈吉宁：

建设国际科技创新中心，构筑创新驱动发展新优势

2022年1月6日，北京市市长陈吉宁在北京市政府工作报告中指出，要紧扣国家重大战略需求，全面落实中关村新一轮先行先试改革若干措施，加快形成高效的新型举国创新体制机制，高水平建设“三城一区”主平台。聚力提升原始创新能力，抓住科学研究和创新范式变革机遇，整合科技资源，创新组织形式，全面建设国家实验室，加速建设综合性国家科学中心。加大基础研究投入力度，在未来科技前沿领域布局一批新型研发机构，力争取得更多基础原创成果和底层技术突破。深化科技成果转化和知识产权保护，加强国际科技交流与合作。进一步做强新一代信息技术、医药健康“双引擎”，推动集成电路、人工智能、通信等领域“卡脖子”技术实现新突破。

中国工程院：

电子信息工程科技面临十三大挑战，网络安全是重中之重

2022年2月15日，中国工程院信息与电子工程学部、中国信息与电子工程科技发展战略研究中心发布“电子信息工程科技发展十三大挑战（2022）”。分析研究了网络安全、网络与通信等十三大电子信息领域年度科技发展情况，综合阐述国内外年度本领域重要突破及标志性成果，为我国科技人员准确把握电子信息领域发展趋势提供了参考。

《报告》指出，新形势下的网络安全在于风险消减与赋能增值双轮驱动。包括：在网络系统的缺陷管控与纵深防御中，如何应对海量存量威胁治理及其有效防护不足、网络安全边界的削弱，如何构建威胁画像、威胁情报运营机制及安全知识体系；在运行任务的威胁管控与时机防御中，如何应对动态环境下“未知的未知”攻击，如何构建威胁感知的时机防御形态，如何打造计算和防护融合新模式、形成运行和防御并行双结构；如何实施风险管理与量化评估手段以支撑网络安全保险；如何破解数据安全和隐私保护与数据流动和开发利用相悖等等。

北京市科委、中关村管委会、市财政局：
启动科研项目经费“包干制”试点

2022年2月11日，北京市科委、中关村管委会、市财政局共同制定了《北京市财政科研项目经费“包干制”试点工作方案》。根据《方案》，2021年起，北京市自然科学基金专项、科技新星计划专项、独立法人研发机构科技专项三类项目将纳入“包干制”试点，试点期限为3年。其中：市自然基金专项包括自然科学基金研究项目、人才项目、合作项目以及环境促进项目等全部项目，较国家自然基金和部分省份仅将“杰青”等部分项目纳入“包干制”，我市试点范围更广、力度更大。独立法人机构科技专项是指在新一代信息技术、医药健康、新材料、人工智能等高精尖技术创新领域，遴选一批从事基础性、前沿性、公益性研究的独立法人研发机构纳入试点，在国内率先将“包干制”试点从项目支持经费扩展至机构支持经费。

其中，北京市自然科学基金项目和科技新星计划项目采取定额方式资助，项目申请人不再编制项目预算。重点研发机构专项由科研机构拟订预算、经费使用规则及设定可考核的绩效目标，不再编制项目预算，后续合同约定进行年度预算拨付及经费管理。所有纳入“包干制”试点项目将实行负面清单管理，明确经费不得用于捐赠、投资、赞助、罚款及支付在职人员学历性教育经费等支出，不得用于与试点项目研究无关的支出。

《方案》明确，项目负责人是项目经费使用的直接责任人，对项目经费使用的合规性、合理性、真实性和相关性承担法律责任。“包干制”项目对试点单位充分放权，作为经费管理的直接责任主体，试点单位应建立“包干制”项目内部经费管理办法，确保项目经费“放得开、管得住”。经费在不违反“负面清单”前提下，试点单位和项目负责人根据实际需要自主决定、统筹使用与科研项目相关支出。项目完成后，项目负责人根据实际使用情况编制项目经费决算，由试点单位自行开展财务审查后报市科委、中关村管委会备案。

“包干制”项目要求强化绩效目标管理，确保项目成果“看得见、摸得着”。《方案》提出建立结果导向评价机制，试点单位承担的项目实施期满后，由市科委、中关村管委会按照项目任务书/合同约定对其开展一次性综合绩效评价，评价结果提交市财政局备案，作为后续支持和考核奖惩的重要依据。评价突出代表性成果和项目实施效果，严格逐项考核结果指标完成情况，对绩效目标实现程度作出明确结论，不得“走过场”，严禁成果充抵等弄虚作假行为。

WAPI产业联盟参加
北京市中关村社团第二联合党委全体党员大会

WAPI产业联盟　周　园

2022年1月6日，WAPI产业联盟秘书长张璐璐、秘书长助理周园参加了在北京西郊宾馆举办的北京市中关村社团第二联合党委全体党员大会。

会上，北京市中关村社团第二联合党委（以下简称“第二联合党委”）书记梅萌向与会的全体党员作公开述职报告。梅萌书记在述职中介绍了联合党委的总体情况、2021年联合党委工作情况、存在问题及2022年工作计划。2021年联合党委着重围绕“班子队伍建设、建章立制工作、党员教育管理、规范组织生活、党建业务融合、党建保障支撑、重点特色工作”等七个方面扎实推进党建工作；从与所属联盟加强联系、党建引领业务发展模式创新等方面分析工作中存在问题。最后，梅萌书记将2022年党委的四项重点工作做了说明：一是强化主体责任，加强班子建设；二是规范社会组织基层党组织建设，抓好党员的教育管理；三是抓好党风廉洁建设，加强意识形态工作；四是不断探索党建和业务融合发展模式。

会后，周园向WAPI产业联盟秘书处宣贯了本次会议思想，明确了联盟2022年的党建工作重点。WAPI产业联盟将继续坚定践行习近平新时代中国特色社会主义思想并与自身业务紧密集合，在党的指引下推动无线网络和网络安全技术产业创新联合发展。

WAPI产业联盟参加中关村产业技术联盟联合会第二届第五次理事会及全体会员大会

WAPI产业联盟　刘剑昕

2021年12月29日和2022年1月6日，WAPI产业联盟积极履行理事单位职责，张璐璐秘书长及秘书处同事参加了中关村产业技术联盟联合会第二届第五次理事会和第二届第五次会员大会。

联盟联合会副理事长兼秘书长杜宏群汇报了2021年工作总结和2022年工作计划。汇报从深入推进联盟党建工作、持续加强联盟服务和产业服务工作、不断完善公共服务平台体系建设等方面总结了2021年度工作任务完成情况。2022年，联盟联合会将继续从党建工作、产业联盟规范建设、推动产业联盟协同创新发展、促进产业升级、提升信息平台功能和智库服务等方面开展相关工作。会员大会上，审议通过了《联盟联合会章程修正案（草案）》《增补中关村数字经济产业联盟、中关村数智人工智能产业联盟、北京第三代半导体产业技术创新战略联盟为联盟联合会理事单位》等事项。

北京市社会组织管理中心主任温育梁、综合处处长许泉，北京市科委、中关村管委会园区发展建设处副处长刘亚军，中关村产业技术联盟联合会理事长梅萌、执行理事长汪诚文等出席了会员大会。

温育梁主任在致辞中肯定了联盟作为科技创新型社会组织在服务科技创新、产业升级和社会发展中起到的积极作用。她表示，希望联盟继续坚持党的领导、提高政治站位、加强自身建设，进一步创新发展模式，为服务北京国际科技创新中心建设发挥更大作用。

刘亚军副处长在致辞中对大会的召开表示了热烈祝贺，并且结合当前形势，对联盟发展提出了几点要求：一是坚持规范化发展要求，强化诚信体系建设。二是持续增强联盟核心服务能力，支撑国际科技创新中心和世界领先的科技园区建设。三是依托“联盟园区行”行动，积极开展联盟与中关村分园“结对子”活动。

联盟联合会执行理事长汪诚文发布了“中关村产业技术联盟园区行”行动方案。园区行将构建分园与联盟“结对”合作机制，开展联盟资源开放服务、科创品牌活动、项目招引、优化营商环境等系列工作，为推进北京国际科技创新中心、中关村世界领先科技园区建设贡献力量。

中关村数智人工智能产业联盟秘书长贾昊、中关村氢能与燃料电池技术创新产业联盟秘书长卢琛钰，分享了联盟工作经验及成果。

联盟联合会梅萌理事长在总结发言中剖析了联盟的组织性质、核心作用和根本任务。他表示联盟要不忘成立初心，牢记发展使命，在当前严峻的社会经济环境下，始终秉持“服务产业、服务企业、服务民生、服务政府”的发展理念，跨界融合，协同创新，不断壮大联盟力量，努力提高联盟的影响力和竞争力。

华辰泰尔WAPI系列产品通过联盟测试

WAPI产业联盟　王立华

2022年1月24日，山东华辰泰尔信息科技股份有限公司（以下简称“华辰泰尔”）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。联盟为该系列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）、鉴别服务器（AS）、客户前置设备（CPE）以及球形WAPI摄像头设备。其中AP、CPE通信速率支持802.11ac协议，可满足行业应用中大宽带、移动性、大连接的无线局域网应用需求；AS设备具备漫游功能，实现了用户可以使用同一张证书在不同的地点接入WAPI网络，满足了行业市场应用中WAPI大规模部署对漫游的需求；球形WAPI摄像头设备内置了WAPI通信模块，相较于摄像头外接CPE方式在硬件成本上显著降低，易用性也得到了显著提升。

联盟测试实验室依据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，联盟测试实验室和设备厂商积极克服疫情困难，通过远程联调形成互动。对发现的未通过项，联盟测试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。

据华辰泰尔介绍，此次测试通过的产品，将用于国家电网基于WAPI的可信WLAN试点示范建设，后续还将开展WAPI终端模组研发，与电力行业专用终端设备匹配，进一步扩大WAPI的应用场景和覆盖范围。

WAPI产业联盟发布《无线局域网安全技术规范》团体标准

WAPI产业联盟　简　练

2021年12月28日，WAPI产业联盟发布团体标准T/WAPIA 046—2021《无线局域网安全技术规范》。这是联盟发布的第83项团体标准。

该团体标准的起草单位包括：无线网络安全技术国家工程研究中心、西电捷通公司、WAPI产业联盟(中关村无线网络安全产业联盟)、国家密码管理局商用密码检测中心、国家信息技术安全研究中心、国家无线电监测中心检测中心、中国移动通信集团有限公司、中能融合智慧科技有限公司、广西大学、广西诚新慧创科技有限公司、中国通用技术研究院、北京数字认证股份有限公司、北京计算机技术及应用研究所、广西通量能源技术有限公司、广州未来能源中心等。标准起草过程中，广泛征求了业界各方意见，为后续依据标准开展产业化工作达成了共识。

标准规定了无线局域网安全技术，包括端口控制、身份鉴别、密钥建立、保密通信以及无线局域网管理帧保护和快速切换等功能，规定了与多种模式无线局域网物理层技术协作时的工作方式。该标准扩展了无线局域网国家标准（GB 15629.11）中的无线局域网安全技术（WAPI），适配了国家密码管理局批准的国密算法（SM2和SM3），适用于无线局域网安全产品、系统的设计和实现，也适用于无线局域网产品、系统安全功能的研制、开发、测试检测等等。

当前，全球网络安全面临“量子计算攻击威胁、字典攻击”等新的安全风险和挑战。我国《密码法》《数据安全法》《个人信息保护法》等法律法规，对加强用户身份保护提出了明确的要求。结合产业市场的需求，WAPI产业联盟迅速组织产学研用开展了《无线局域网安全技术规范》的创新工作，本团体标准使用了安全性更高的原子密钥建立与实体鉴别（AKEA）机制，适配了国密算法SM2和SM3，增强了主动身份保护、抗字典攻击和缓解量子计算暴力攻击等安全性，将更好地服务市场和产业发展需要。

16年来，WAPI产业联盟以无线网络安全技术国家工程研究中心、联盟测试实验室、精准服务平台为抓手，围绕无线网络和网络安全的技术研发、标准化、产业化、市场化、国际化，组织协同创新工作。产业链上下游可自愿加入联盟无线网络安全标准化委员会或参与相关WG工作组，提出标准项目立项申请、牵头开展新标准项目或参加已立项项目。联盟通过平台化的服务，有效地协助产学研用各环节提升标准能力、满足市场需求。通过加入联盟，产业链上下游厂商可以更准确地把握技术和市场演进方向，引领（及早发现）市场机会，掌控投资重点；可以将本单位创新技术通过标准提案的方式推进采纳，掌握市场先机；可以在标准化过程中增强与产业链上下游的协作机会，促进标准化所辐射的技术、产品、市场获得综合能力提升；可以更加有效地参与团体标准“走出去”，参与标准国际化活动。

山东华辰泰尔信息科技股份有限公司加入WAPI产业联盟

WAPI产业联盟　周　园

日前经联盟理事会批准，山东华辰泰尔信息科技股份有限公司正式加入WAPI产业联盟，联盟会员单位增至109家。

山东华辰泰尔信息科技股份有限公司（以下简称“华辰泰尔”）成立于2002年，注册资本6200万元，是山东省为数不多的电信级通信设备研发制造商，业务领域涉及政企单位通信专线互联、企业入云、边缘计算、融合通信、物联网等，是中国联通和中国电信认定的一类供应商。

据华辰泰尔介绍，目前已支持国网山东电力公司、东营供电公司、烟台供电公司、济南供电公司部署了基于WAPI的可信WLAN试点。加入联盟后，公司关注并计划开展WAPI终端和模组研发，与本行业专用终端设备匹配，扩大WAPI的应用场景和覆盖范围。

华辰泰尔下设山东通信接入网工程技术研究中心、山东省集成电路设计中心、济南市企业技术中心等研发机构，目前拥有6项发明专利、3项实用新型专利和56项软件著作权。目前与国内外多家知名公司达成了良好的合作关系，是中国联通、英特尔的全球战略合作伙伴，是阿里云整体解决方案的接入部分提供商。公司产品已广泛应用于电信运营商及电力、公安、石油、军队等专业通信网，产品遍布全国以及亚洲、非洲、欧洲等国外电信运营商。

华辰泰尔拥有完善的法人治理结构和高效稳定的经营团队，公司已取得ISO9001：2015质量管理体系认证、ISO14001：2015环境管理体系认证及ISO18001：2007职业健康安全管理体系认证、GB/T29490−2013知识产权管理体系认证证书，被认定为高新技术企业、“双软”企业、济南市创新型企业、软件创新型企业、山东省电子信息行业优秀企业。

中国联通科技助力北京冬奥会

中国联通

在为期17天的北京2022年冬奥会期间，中国联通的大联接、大数据、大应用、大安全，为科技冬奥、智慧冬奥提供了有力支撑，实现了系统0故障、0掉网。

期间，中国联通借助高速率、广覆盖的网络为冬奥每一个单元的连接搭建起沟通的桥梁。覆盖北京、延庆、张家口两个城市三个赛区所有竞赛场馆和非竞赛场馆的一张大网，规模庞大，系统复杂，这对网络的安全保密、可用性、稳定性、可管理性和数据传输完整性等要求极高。

绿色冬奥、节能环保是本次冬奥会的重要主题，场馆制冰、设备运行、灯光照明等能源耗费较多。传统的能源管理模式，不可避免造成浪费。

中国联通打造的可视化综合指挥平台，实现了对场馆内各类设备能耗数据的数字化采集、存储、统计分析、节能诊断、优化控制和综合管理，能实时查看相关故障和报警，对故障设备实现空间定位，方便维修人员第一时间解决相关问题。可视化运营平台的应用，在各系统安全稳定运行的前提下，减少了能源消耗，提高了能源利用率，可为场馆节能20%，为能源管控提供科学性依据，助力场馆实现节能降碳绿色运营。

在北京冬奥所有重要场馆的安检工作中，安检机器会实时把他们的证件等数据传送到数据中心进行校验，校验无误再放行，这需要超低的网络延迟和对安检机器安全入网的保障。

由中国联通提供的冬奥赛事网络，支撑了整个赛事的平稳运行，互联了北京冬奥会的所有竞赛和非竞赛场馆，服务了所有场馆的竞赛服务和北京冬奥组委的办公服务。这套网络里有着许多复杂的IT系统，这些IT系统各司其职，共同保障了冬奥会各项赛事的顺利运行。其中一套最重要的系统，能确保未经认证的接入及没有授权的设备，诸如办公人员、记者、媒体工作人员的个人终端设备，或非法用户将带有巨大安全威胁的终端接入进冬奥赛事网络中实行攻击、散播病毒等。

中国移动A股上市

中国移动

2022年1月5日，中国移动有限公司（证券简称“中国移动”，证券代码：600941）成功登陆上交所主板。

中国移动是全球领先的通信及信息服务企业，也是全球网络和客户规模最大、盈利能力领先的世界级电信运营商。中国移动用户规模位居全球之首。中国移动拥有基站总数达528 万个、覆盖全国超99.5%的人口，其中4G基站约占全球三成、5G基站约占全球35%，均位居全球第一。

中国电信政企部门开展机构改革

运营商财经网

近期，中国电信为加快提升产业数字化核心能力，促进DICT业务高速发展，决定聚焦重点行业设立产业研究院，同时将中国电信集团系统集成有限责任公司更名为“中电信数智科技有限公司”，对此进行管理。

中电信数智科技有限公司旗下设立卫健、应急、政法公安、农业农网等12个产业研究院，名称统一为中国电信XX产业研究院，工商注册为“中电信数智科技有限公司XX分公司”。此外，中国电信数智科技公司还将设立政务、商客等2个产业创新中心，即中国电信政务行业创新中心和中国电信商业与服务业产业创新中心。中国电信强调数智科技公司要加大投入，提升产业创新中心的行业研究及平台研发能力，逐步向产业研究院过渡。

华大电子发布三款智能安防安全“芯”品

全球TMT

2021年12月26日，北京中电华大电子设计有限责任公司（简称“华大电子”）在第十八届中国国际社会公共安全博览会上发布三款智能安防安全芯片产品及其解决方案。

华大电子智能安防安全SE芯片产品、智能安防安全TF卡产品、智能安防安全USB模组，能满足安防旧设备升级改造也能支持新设备产品研发，可用于安防前端设备以及后台监控中心等。三款产品使用了SM1/SM2/SM3/SM4算法，通过了国密二级/EAL4+安全认证，产品均符合GB35114-2017《公共安全视频监控联网信息安全技术要求》A/B/C 级要求和GMT0054-2018《信息系统密码应用基本要求》等智能安防安全产品准入标准。

国家无线电监测中心助力智能网联汽车创新发展

中国无线电管理

2021年12月13日，国家无线电监测中心副主任曾开祥在2021国际智能网联汽车测试示范发展论坛作《智能网联汽车无线电频率管理政策与规划》演讲中，讲述了无线电频率在智能网联汽车领域的政策、规划和意义，并对C-V2X和车载雷达相关的政策和规划进行了详细分析。

会上，国家无线电监测中心检测中心（SRTC）主任王俊峰与国家智能网联汽车创新中心（CICV）总经理助理兼整车事业部总经理刘卫国签署了合作框架协议，携手助力智能网联汽车创新发展。

根据合作协议，SRTC与CICV两家单位将充分发挥各自的专业能力与资源优势，在国内车载无线设备检测、自愿性认证机制构建、实验室资源共享、科研项目标准研究、产品研发及推广等方面开展合作，共同服务于智能网联汽车产业的创新与发展。

展锐智能连接技术Perfelink助力万物互联

ToP思维

随着智能设备的增加，解决设备间的连接和交互需求不断升级，展锐智能连接技术Perfelink正在万物互联中发挥重要作用。

万物互联时代，“随时随地”在线,是用户对连接技术的基本需求，技术层面，当前WLAN、蓝牙、UWB等各类中短距连接技术与5G齐头并进。在不同的应用场景下，如何获得始终如一的连接体验，就需要连接技术能够智能感知使用场景，并根据场景智能调整技术配置。

展锐是少数全面掌握2G/3G/4G/5G、WLAN、蓝牙、电视调频、卫星通信等全场景通信技术的企业之一，其Perfelink技术解决方案，可同时启动WLAN和移动通信的多链路并发，以提高传输速率，亦可实时感知用户所处场景，对WLAN、4G、5G三个网络的信号与链路质量进行动态检测，在“用户无感”的情况下，把终端接入到质量最佳的网络上，为用户提供的高速连接的使用体验。

数字认证入选北京市国资委举办“十三五”重大创新成果

数字认证

2022年1月，北京数字认证股份有限公司（以下简称“数字认证”）的面向互联网开放环境的重要信息系统安全保障关键技术研究及应用项目在北京市国资委系统“十三五”创新成果发布会上，荣获国家科技进步二等奖。会上，该项目和来自全系统38个获得国家、北京市科技奖励或解决行业“卡脖子”技术的重大创新成果集中进行了展示。

通过该获奖项目，数字认证助力实现了数字经济发展的信息安全保障，推动密码技术与数字经济融合发展，力争实现可信身份、可信行为、可信电文和数据安全四位一体的“大安全体系”。北京市国资委党委书记、主任张贵林对此表示认可，并鼓励数字认证继续创新，助力国家安全。

面向互联网开放环境的重要信息系统安全保障关键技术研究及应用项目，瞄准了国家重要信息系统网络安全保障重大战略需求，以自主密码技术为基础，突破开放环境下动态安全防护、数字信任体系构建等关键核心技术，实现了密码技术与产业数字化全方位应用场景融合发展。据介绍，未来该成果还将全面推动密码技术与数字经济的融合发展，打造“大安全体系”，为网络空间秩序维护和数字经济发展赋予强大动能。

锐捷荣获2021博鳌企业论坛年度十大创新企业

锐捷网络

2022年1月，锐捷荣获由环球时报、中国企业网联合主办的2021博鳌企业论坛“年度十大创新企业奖”。

根据IDC数据，锐捷在中国以太网交换机市场占有率排名第三，WLAN产品出货率连续2年排名第一，在中国企业级终端VDI市场占有率连续6年排名第一。

在无线产品领域，锐捷网络针对不同行业的不同场景，通过对物理环境的洞察及客户需求细节的把握，进行无线信号以及无线网络性能和功能的优化设计。在天线、射频及无线报文底层转发算法方面进行了大量创新性设计，开发出多个场景化创新无线网络解决方案，为用户提供良好的信号覆盖、流畅的无线接入和使用体验。

在交换机领域，针对大型数据中心场景，锐捷自主研发开放化软硬件架构，实现软硬件解耦的创新，并取得一定的先发优势。

新华三荣获通信领域三奖项

紫光股份

近期，新华三分别荣获第18届ICT产业龙虎榜 “2021年度ICT综合实力企业奖”以及2021通信产业大会“2021年度推动产业进步企业”、“2021年度优秀产品技术方案”通信产业金紫竹奖。

2021年，新华三助力运营商加速数字化变革，为运营商提供5G、IP承载以及云网融合等诸多领域的整体产品及解决方案，在电信级运营商市场表现突出。在运营商大网方面，新华三核心集群路由器CR19000实现了三大运营商集采持续中标，在IP城域网、IDC出口和骨干网等关键节点平稳运行。同时，新华三集团的高端路由器也是中国移动云专网、中国联通智能城域网、中国电信新型城域网的主要在网设备，落地规模和应用范围不断扩大。

鼎桥荣登AIoT行业先锋榜

鼎桥通信

2021年12月9日，鼎桥在物联网智库联合挚物AIoT产业研究院举办的2021中国 AIoT产业年终盛典中，荣登AIoT行业先锋榜。其中，鼎桥的5G物联网系列化模组入选《2022年5G产业全景图谱报告》和《2022年中国AIoT产业全景图谱报告》。

数字化转型的深入推进和行业客户需求的多元化发展，要求信息通信企业具有深厚的产品研发能力和行业理解能力，能够不断提供适应需求的产品和解决方案。鼎桥在5G技术的应用上持续创新，5G和AI的结合，5G和边缘计算的结合，5G和区块链的结合鼎桥都逐步的产品化，为行业客户提供更好的解决方案。

中兴通讯在武汉建立全国研发中心 聚焦三大方向

科技日报

2022年1月，武汉东湖高新区与中兴通讯股份有限公司签署中兴通讯武汉研发中心项目合作协议。

根据协议，中兴通讯拟在光谷打造其通信设备软件、通信电源解决方案、数据中心设备软件三条产品线的全国研发中心，为该集团5G通信相关研发业务提供重要支撑，进一步巩固其在5G通信领域中的优势地位。

磁域网（MFAN）标准体系分析

西电捷通公司，无线网络安全技术国家工程研究中心

杜志强，王月辉，李琴

1.磁域网技术概述

1.1 磁域网的概念

磁域网（MFAN）是可以在一个低频段的磁场上传输和接收数据的无线通信网络。磁场内的无线通信可以实现可靠的通信，并扩展了通信系统对金属、土壤和水的覆盖范围。这种无线通信网络是根据磁场通信的特点而设计的。在恶劣环境下，采用低载频可靠通信和大磁场区域，采用BPSK等简单鲁棒调制，以降低实现成本和错误概率；采用曼彻斯特编码或NRZ-L等动态编码技术，实现噪声鲁棒性。本质上，磁域网无线通信能够提供传输距离在几米之内的数千比特每秒（kbps）级的数据传输。

磁域网使用一种简单而高效的网络拓扑结构（如星型拓扑结构）以降低功耗。采用动态地址分配的方法实现了小数据包规模和高效率的地址管理，并考虑了可变数据传输速度和编码的自适应链路质量控制。磁域网中的设备根据角色被指定为两类元素：磁域网协调器（MFAN-C）和磁域网节点（MFAN-N）。在网络中，可以仅有一个协调器。当节点加入网络时，协调器根据节点的请求和协调器的决定为每个设备分配时隙。因此，考虑采用TDMA进行数据传输。

1.2 磁域网的应用场景

在恶劣的环境中的无线通信已成为各行各业的迫切需求。按现有的无线通信标准，传感器节点很难利用射频在金属、土壤和水周围传输数据。磁域网技术目前主要应用于满足地面状态管理、地下基础设施管理、建筑和桥梁的管理、灾难预防监控、污染管理等需求。全球的环保、建筑、农业、水利、交通运输等行业对磁域网有大量的需求，其中较为迫切的需求主要集中在水和含矿物质的土壤勘探、油藏漏油检测、土地运动滑坡监测和地震监测等方面，在当今物联网技术及应用飞速发展的大环境下具有较为广阔的应用前景和应用价值。

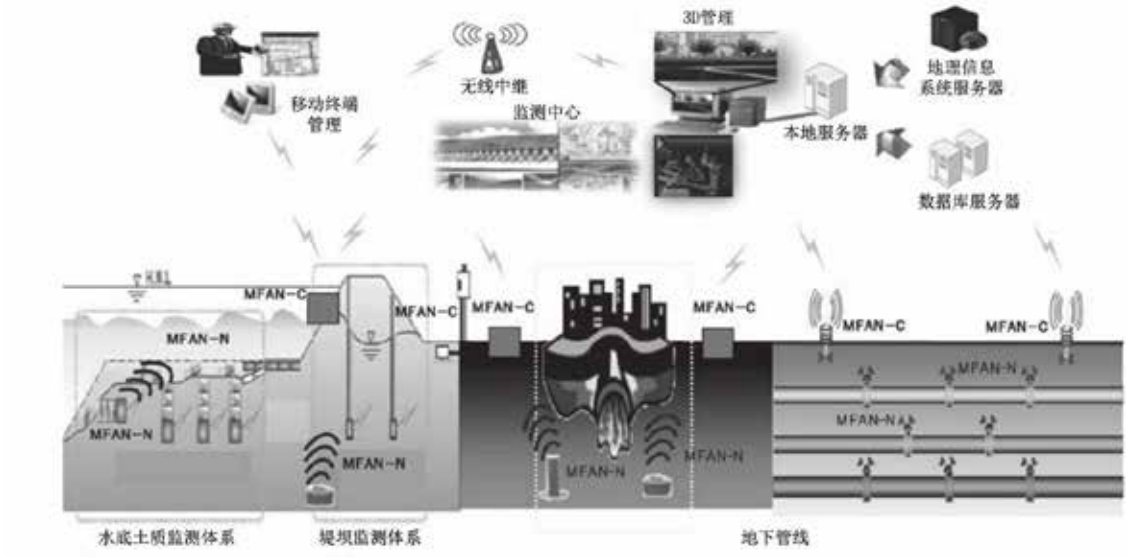


图1 地下状态监测系统

图1所示为基于磁域网的地下状态监测系统。该系统中，MFAN-N埋在地下，MFAN-C置于地上。如果MFAN-N从传感器接收到传感数据，则MFAN-N通过磁场将接收到的数据发送给MFAN-C。MFAN-C通过远距离无线或有线方式将接收到的MFAN-N数据发送到监控中心。

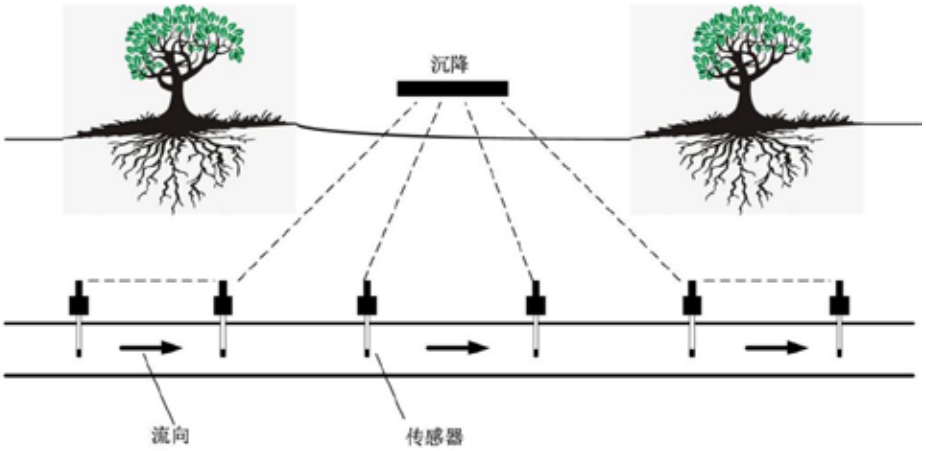


图2 地表状态监测

图2所示为基于磁域网的地表状态监测系统。该系统中，传感器节点可以埋在地下，用于探测地面塌陷、沉降、滑坡等。

2.磁域网相关国际标准和国家标准

2.1 磁域网国际标准

磁域网国际标准ISO/IEC 15149“Information technology — Telecommunications and information exchange between systems — Magnetic field area network (MFAN)”系列对磁域网技术进行了规范，共包括4个部分：

ISO/IEC 15149-1:2014 Information technology — Telecommunications and information exchange between systems — Magnetic field area network (MFAN) — Part 1: Air interface（信息技术 系统间远程通信和信息交换 磁域网 第1部分：空中接口），该标准规范了适用于低载频磁场环境中物理层及媒体访问控制层协议的空中接口。

ISO/IEC 15149-2:2015 Information technology — Telecommunications and information exchange between systems — Magnetic field area network (MFAN) — Part 2: In-band Control Protocol for Wireless Power Transfer（信息技术 系统间远程通信和信息交换 磁域网 第2部分：带内无线充电控制协议），该标准规范了在同一频段内同时进行无线电能传输和数据传输的带内网络系统的具体要求。

ISO/IEC 15149-3:2016 Information technology — Telecommunications and information exchange between systems — Magnetic field area network (MFAN) — Part 3: Relay Protocol for Extended Range（信息技术 系统间远程通信和信息交换 磁域网 第3部分：扩展范围的中继协议），该标准规范了适用于扩展范围内中继协议的寻址、请求、响应代码相关规则。

ISO/IEC 15149-4:2016 Information technology — Telecommunications and information exchange between systems — Magnetic field area network (MFAN) — Part 4: Security Protocol for Authentication（信息技术 系统间远程通信和信息交换 磁域网 第4部分：安全鉴别协议），该标准规范了磁域网安全鉴别协议及要求。西电捷通公司承担了ISO/IEC 15149-4:2016的项目编辑，磁域网安全关键技术——磁域网安全协议（MFSec）由西电捷通公司提出并被国际标准采纳，这是我国在磁域网领域第一项成为国际标准的安全协议技术，填补了磁域网安全技术的空白。

2.2 磁域网国家标准

磁域网国家标准GB/T 40783“信息技术 系统间远程通信和信息交换 磁域网”以采用国际标准ISO/IEC 15149的方式制定，拟包括四部分：空中接口协议、带内控制协议、中继协议和安全协议。目前，我国正在开展GB/T 40783第1部分和第2部分的制定工作，进展情况如下：

GB/T 40783.1-2021《信息技术 系统间远程通信和信息交换 磁域网 第1部分:空中接口》已发布，该标准提供了磁域网（MFAN）内信息通信协议，在吸纳了国际标准ISO/IEC 15149-1:2014技术优点的基础上，对磁域网间信息通信空中接口的协议规定进一步完善。为了保证信息传感设备在特殊环境中能够有效通信，结合国内磁域网通信技术的应用需求，改进了其安全机制，进而提出符合国内行业发展的磁域网间信息通信空中接口规范。MFAN支持基于无线通信以及复杂环境下的无线电能传输等服务。

GB/T 40783.2《信息技术 系统间远程通信和信息交换 磁域网 第2部分: 带内无线充电控制协议》，处在国家标准报批阶段，以等同采用ISO/IEC 15149-2:2015的方式，规定了一种可以在同一频带内同时进行无线能量传输和数据传输的带内网络系统，为稳定的网络以及远程和持续的能量供应提供了技术解决方案。该网络的设计基于在ISO/IEC 15149-2中给出的磁域网原理，以此方式实现在设备控制方面优先的同时，对请求中的多个设备进行无线能量传输管理。本文件注重于PHY层和MAC层协议，不涉及有关上层协议的事项。PHY层和MAC层应能够共同执行以下任务：数据传输、信号控制、无线能量传输。

3.磁域网团体标准

3.1 T/WAPIA 042.3–2021

3.1.1 标准简况

T/WAPIA 042.3-2021《信息技术 系统间远程通信和信息交换 磁域网 第3部分：扩展范围的中继协议》，该标准由WAPI产业联盟（中关村无线网络安全产业联盟）与工业和信息化部宽带无线IP标准工作组共同提出，由无线网络安全标准化委员会归口，具体由西电捷通公司牵头起草，无线网络安全技术国家工程实验室、中关村无线网络安全产业联盟、中国南方电网电力调度控制中心、广西电网公司电力科学研究院、中国南方电网超高压输电公司广州局、重庆邮电大学、国家无线电监测中心检测中心等参与。

3.1.2 标准主要技术内容

该标准以等同采用国际标准ISO/IEC 15149-3:2016的方式制定，主要规定了用于扩展磁域网的有效覆盖范围的中继协议，定义了寻址、请求和响应代码等内容。该标准的主要内容如下：

1 范围	2 规范性引用文件	3 术语和定义	4 缩略语	5 综述
6 网络元素	7 网络功能	8 网络状态	9 MAC层帧格式式	10 MAC层功能

MFAN中继网络超帧包括请求周期，响应周期和自发周期。

在请求周期，MFAN-R将响应请求数据包广播至所有设备。MFAN-N收到后，决定是否将响应数据包返回给MFAN-R。MFAN-R可以将设备分组来选择性接收目标设备的响应。

在响应周期，由MFAN-R分组的MFAN-N选择性将响应数据包返回给MFAN-R。一旦MFAN-R接收到来自MFAN-N的响应数据包，MFAN-R就发送确认数据包以确认接收。如果MFAN-N没有收到来自MFAN-R的确认数据包，则MFAN-N会在响应期间持续发送响应数据包，直到它们能接收确认数据包为止。

当一段时间内没有MFAN-N发送响应数据包时，自发周期开始。该时间段一直持续到直到MFAN-R请求响应请求数据包为止，这是新超帧的开始。例外地，MFAN-N能够在自发周期内传输数据，而无需MFAN-C或MFAN-R的请求。

中继器设置过程如图3所示，在请求周期，当MFAN-C向具有中继器功能的MFAN-N发送RSRq数据包时，MFAN-N在响应周期发送RSRs数据包。MFAN-C探测MFAN-N的中继器设置状态，然后发送RSRA数据包。如果中继器的设置过程完成，则MFAN-N成为MFAN-R，然后MFAN-R在MFAN中继网络中扮演MFAN-C的角色。

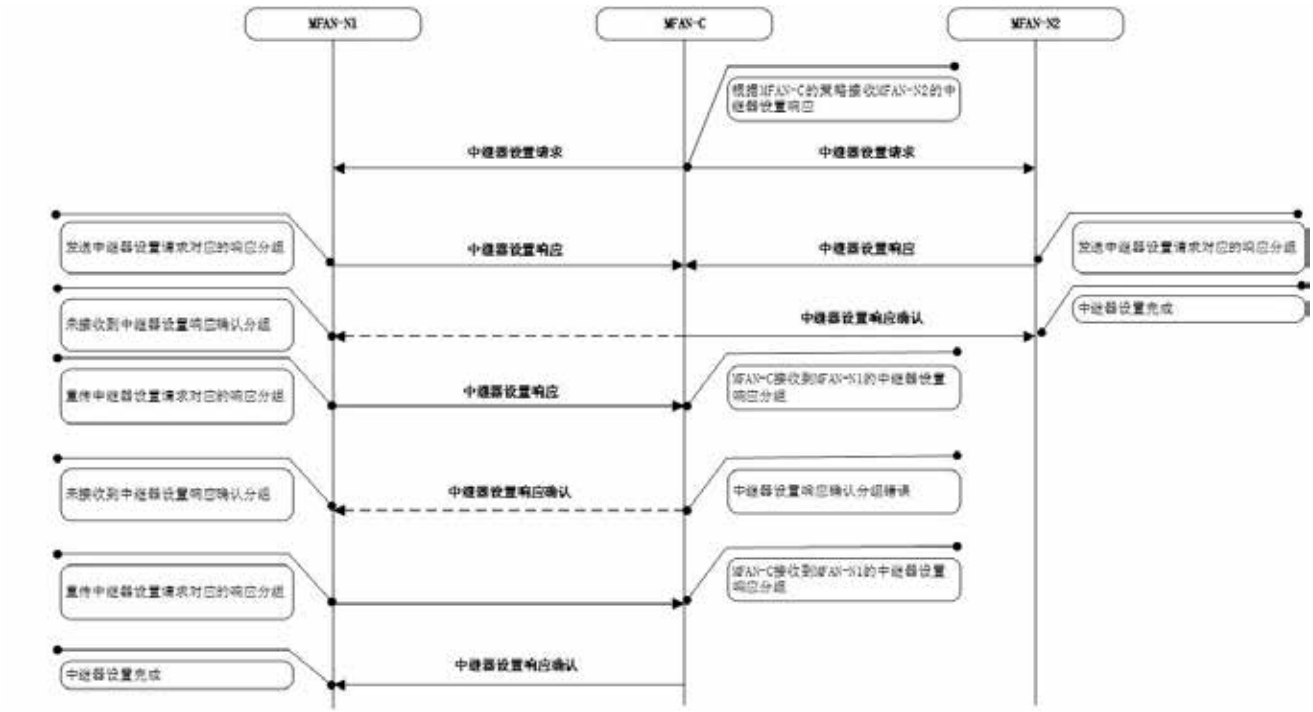


图3 中继器设置过程

该标准规范的扩展范围的中继协议已在多个场景下进行了工程化实现和验证，验证结果表明该标准所规范的协议能够适用于磁域网环境下的短距离信息通信。

3.2 T/WAPIA 042.4–2021

3.2.1 标准简况

T/WAPIA 042.4-2021《信息技术系统间远程通信和信息交换磁域网第4部分：安全鉴别协议》，该标准由WAPI产业联盟（中关村无线网络安全产业联盟）与工业和信息化部宽带无线IP标准工作组共同提出，由无线网络安全标准化委员会归口，具体由西电捷通公司牵头起草，无线网络安全技术国家工程实验室、中关村无线网络安全产业联盟、中国南方电网电力调度控制中心、广西电网公司电力科学研究院、中国南方电网超高压输电公司广州局、重庆邮电大学、国家无线电监测中心检测中心等参与。

3.2.2 标准主要技术内容

该标准以等同采用国际标准ISO/IEC 15149-4:2016的方式制定，主要规定了磁域网安全鉴别协议，该技术为资源受限但又有特定安全需求的磁域网设备提供安全防护能力。该标准定义了寻址，请求和响应代码等内容。该标准的主要内容如下：

1 范围	2 规范性引用文件	3 术语和定义	4 符号和缩略语	5 综述	6 网络元素
7 网络功能	8 网络状态	9 物理层帧格式	10 MAC层功能	附录A安全考虑	

磁域网与其他网络（如无线传感器网络）相似，受到许多网络安全威胁。为了对抗这些威胁，在上述网络里应采取必要的安全措施。

ITU-T X.800和ITU-T X.805里规定的下列网络安全威胁适用于磁域网：信息和/或其他资源的破坏；信息的错误或修改；信息的泄露。

此外，针对节点的特定威胁，例如传感器节点被捕获、侦听、敏感数据泄露、拒绝服务攻击（DoS攻击）和网络的恶意使用等也同样出现在磁域网里。

ITU-T X.805里规定的下列安全要求适用于磁域网：数据保密性；数据鉴别/身份；数据完整性。

该标准规定了磁域网安全协议（MFSec）。MFSec使用异或运算实现了MFAN-C和MFAN-N之间的双向鉴别。

鉴别过程如图4所示，在请求周期，MFAN-C发送AuRq分组给未鉴别的MFAN-N。在响应周期MFAN-N发送AuRs分组给MFAN-C。MFAN-C识别此MFAN-N是否合法，并通过AuRC分组通知结果。当鉴别过程成功完成时，相关的身份标识符应包括在ASA分组里，当鉴别不成功，MFAN-C必须记录相关MFAN-N的身份。如果MFAN-C未接收到AURs分组，或者MFAN-N由于分组错误未接收到AuRC分组，MFAN-C连续发送AuRq分组的每个超帧，直到接收到正确的AuRC分组为止。当从MFAN-C接收到AuRC时，MFAN-N的鉴别过程完成。

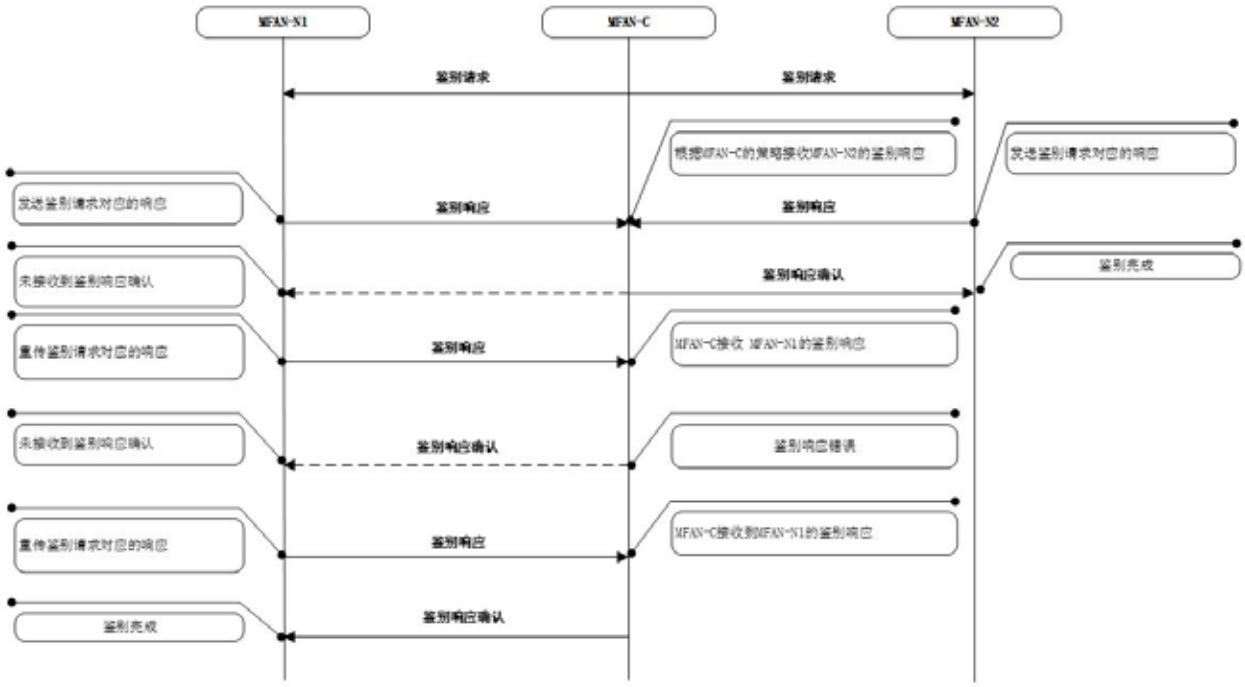


图4 鉴别过程

本文件规范的安全鉴别协议已在多个场景下进行了工程化实现和验证，验证结果表明本文件所规范的协议能够适用于磁域网环境下的短距离信息通信。

3.3 标准应用前景

磁域网是一种使用磁场作为通信介质，能够在恶劣环境下进行可靠通信的无线网络。磁域网是一种近场磁感应系统，在传统的无线网络中，数据通过无线电波进行交换；而在磁域网中，数据和能量是通过磁场中的粒子进行交换的。传统的无线电波在水、土壤甚至金属中传播信号会极大衰减，损耗严重，传输数据较为困难；而磁域网技术是利用低频段使用磁场技术发送和接收数据的一种新型的无线通信网络技术，它利用磁场的特性，可以突破恶劣环境下数据难以传输这一瓶颈，利用金属、土壤和水内部的多个传感器节点将数据传输至外部协调器中。

磁域网是近距离感知和通信网络的一种新兴形式，是形成物联网的新型连接网络。磁域网技术目前主要的典型应用是满足地面状态管理、地下基础设施管理、建筑和桥的管理、灾难预防监控、污染管理等需求。当前，全球的环保、建筑、农业、水利、交通运输等行业对磁域网的需求正在急速提升，其中较为迫切的需求主要集中在水和含矿物质的土壤勘探、油藏漏油检测、土地运动滑坡监测和地震监测等方面，在当今物联网技术及应用飞速发展的大环境下具有较为广阔的应用前景和应用价值。

WAPI产业联盟作为在全球研究磁域网技术和开发标准最早的标准组织之一，将持续践行网络强国战略，组织成员单位进一步完善磁域网标准体系，并引领磁域网产业发展。

WAPI 产业联盟成员单位名录

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

【注：截至2022年2月，联盟正式成员已达109家，以加入联盟的时间先后排序。】

WAPI Alliance

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