

《体育赛事信息化 网络安全规范 第1部分：通用网络安全架构（征求意见稿）》

行业标准编制说明

一、工作简况

（一）任务来源

根据国家体育总局下发的《2021 年体育标准化工作要点》有关内容，提出“组织开展 2021 年体育国家、行业标准立项申报和重点标准制修订工作。完成全民健身、冰雪运动、体育场地设施等国家标准制修订工作。推进体育彩票、绿色体育场馆、赛事信息化、运动营养品等行业标准制定工作”。网络安全是赛事信息化的重要组成部分，2021 年国家体育总局体育信息中心向全国体育标准化技术委员会提交了《体育赛事信息化 网络安全规范 第1部分：通用网络安全架构》行业标准制定立项申请。2022 年 3 月，体育总局发布了《关于下达 2022 年第一批行业标准制定项目计划的通知》（体经字〔2022〕78 号），批准了行业标准《体育赛事信息化 网络安全规范 第1部分：通用网络安全架构》（计划号：202229）的制定立项。

（二）起草人员及其所在单位

本标准起草单位为：

本标准主要起草人为：

（三）主要起草过程

1. 建组与调研阶段

成立标准工作组，在标准编制前期，拟定工作计划，充分重视调查研究工作，广泛收集各项体育赛事网络安全相关的资料性文件，查阅相关资料，对国际标准进行了翻译校对，形成调研成果，为标准的编制提供依据，完成标准草案稿。

（本阶段工作成果：标准工作组讨论稿和编制说明）

2. 起草阶段

开展内部研讨会，在调研基础上完善初稿，并就完善后的初稿向工作组成员单位做说明，组织起草单位有关人员及相关专家开展标准研讨会，对标准具体条款进行讨论、征求意见，根据会议意见修改后，组织召开第二轮标准研讨会，并根据“体育赛事信息化 网络安全规范”的中英文对应、规范范围建议、规范性引用文件排序等意见进行修改，请标准化专家对讨论稿进行标准技术审核。期间，工作组与有关部门做了经常性沟通汇报。（本阶段工作成果：标准征求意见稿和编制说明）

3. 征求意见阶段

2022年9月30日，国家体育总局体育器材装备中心印发了关于对《体育赛事信息化 网络安全规范 第1部分：通用网络安全架构》等5项行业标准公开征求意见的通知，信息中心、标准编制工作组向体育场馆、高校及信息技术企业

发放征求意见函件。随后国家体育总局办公厅向各省、自治区、直辖市、计划单列市、新疆生产建设兵团和有关司发放征求意见函件。共收到 24 份回函，其中有修改建议的函 5 份。包括社会各相关单位意见，共收集意见 28 条，采纳的条数 27 条，未采纳的条数 1 条。工作组依据征求意见情况，逐条分析、整理。意见采纳的已依据意见情况修改标准文本；不采纳的逐条回复不采纳理由。

4. 送审阶段

2023 年 7 月 14 日，工作组组织召开《体育赛事信息化 网络安全规范 第 1 部分：通用网络安全架构》行业标准预审会，邀请来自网络安全、软件测试、通信网络等领域的 15 位专家，对标准文件及配套材料进行逐条审阅。会后工作组根据会议纪要逐条修改标准文本，并将本次会议意见合并至征求意见汇总表。

由于预审会标准稿件修改内容较大，为保障标准的广泛适用性，工作组讨论认为应再次开展公开征求意见工作，并将预审会后标准文本及编制说明提交国家体育总局体育器材装备中心。

（四）标准制定的必要性和意义

2021 年 10 月，国家体育总局印发《“十四五”体育发展规划》（以下简称《规划》），对体育信息化建设进行了部署，这是为满足人民期盼便捷智能体育需求、国家推动体育高质

量发展的要求而提出的任务和谋划的布局，体现了体育领域以信息化培育新动能的新理念，对助力实现体育强国建设目标具有重大意义。《规划》指出实施数字体育建设工程，弥补基础短板，建立系列信息技术标准规范，以标准助力增强体育政务运转效率、提高体育赛事规范化水平、提升便民服务能力。

近年来，随着我国信息技术水平不断提高，迈进“互联网+”时代，体育赛事的组织与管理走上了信息化发展道路，以计算机技术、精密传感技术、GPS定位技术、VR技术等为代表的各种技术手段逐渐应用于体育赛事的组织与开展，这对赛事的网络安全提出了更高的要求，只有守护好网络空间的安全与秩序，体育赛事信息化的价值才能得以实现。体育赛事信息化中的网络安全保障，尤其是大型体育赛事中的网络安全保障工作，既是对赛事主办方综合保障能力的考验，也是对举办地城市甚至国家信息技术水平和网络安全保障能力的考验。确保体育赛事信息化建设中的网络安全，构建完善的网络安全管理体系、检测体系和应急体系是基础。制定《体育赛事信息化 网络安全规范 第1部分：通用网络安全架构》行业标准，对确保体育赛事网络空间的安全与秩序、在赛事结束后为城市的网络安全防御赋能具有重要作用。

从政策支持、现实需求角度出发，本项目开展的必要性主要有以下2个方面：

第一是政策支持方面。2019 年 8 月，国务院办公厅印发颁布《体育强国建设纲要》，提出了落实全民健身国家战略，助力健康中国建设的战略任务，指出了运用物联网、云计算等新信息技术，促进赛事信息发布等整合应用，反映出当前落实体育赛事信息化、智慧化发展的迫切需求。2021 年国务院颁布实施《全民健身计划（2021-2025）》、国家体育总局颁布《“十四五”体育发展规划》将“推进体育产业数字化转型”“健全体育信息化标准体系”列为重要工作任务。2022 年 3 月，中共中央办公厅、国务院办公厅印发《关于构建更高水平的全民健身公共服务体系的意见》提出“加快运用 5G 等新一代信息技术改进场馆管理和赛事服务”。

第二是现实需求方面。信息技术作为现代科学技术的重要组成部分，对各个领域的发展产生着深刻影响。体育赛事随着全民健身运动的兴起快速发展，在体育赛事组织举办的过程中，引入现代化技术特别是信息技术能够有效减少工作负担、提高工作质量，同时减少体育赛事数据统计工作的人为因素、增强体育赛事统计工作的准确性和公正性。当前我国体育赛事信息传播工作对信息技术的需求是长远且巨大的，我国近年来举办的一系列大型运动会都彰显着计算机信息技术的重要作用，因此保障体育赛事信息化的网络安全是重中之重。2018 年平昌冬奥会开幕式当天奥组委服务器遭遇黑客攻击，官网宕机 12 小时，赛场附近网络瘫痪、观众无

法打印入场券、媒体中心无法直播开幕式，财务和其他敏感信息系统受到威胁。自 2000 年悉尼奥运会以来，历届奥运会期间的网络风波不断。安全专家预测，未来大型体育赛事期间将涌现更多针对性的黑客攻击事件。构建体育赛事信息化网络安全规范，对保障大型体育赛事整体安全至关重要。

二、编制原则、标准主要技术要求的依据

（一）编制原则

1. 业务优先原则

体育赛事通用网络安全架构是为体育赛事服务的，应符合体育赛事的特点，满足体育赛事需求，合理设计网络安全架构，保障业务连续稳定运行。

2. 开放性原则

能够保障和支持国内、国际主要体育赛事系统、应用、协议，在符合中华人民共和国相关法律法规的基础上，适度考虑国际体育赛事组织机构相关文化、习惯、技术要求（宗教除外）。

3. 网络安全合规原则

体育赛事网络安全架构的规划设计应符合我国法律法规要求，包括网络安全等级保护制度等。

（二）标准主要技术内容

1. 总体要求

本章节明确了网络安全架构的运行和技术角度的总体

要求。

2. 网络安全架构

本章节给出了通用网络安全架构图，并明确了三层内容和三个阶段的具体要求。

3. 赛前筹备阶段

本章节对统筹决策、网络安全规划、监督检查、网络安全建设和网络安全评估 5 方面内容作出了具体规定。

其中网络安全建设中的网络安全管理体系和网络安全技术体系符合国家标准《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）的要求。

网络安全运行体系根据体育赛事特点，明确了资产管理、配置管理、脆弱性管理、设备运维、网络安全监测、事件处置、应急响应、威胁情报 8 项内容。

4. 赛时运行阶段

本章节对统筹调度、应急指挥、安全值守保障、场馆安全检查、网络安全监测、事件处置、应急响应、威胁情报研判 8 方面内容作出了具体规定。

根据赛前筹备阶段的网络安全建设情况，赛时运行期间网络安全保障层的 6 项重点工作任务与赛前筹备阶段的网络安全运行体系具有对应关系。

5. 赛后总结阶段

本章节对总结复盘、项目验收、项目审计、数据归档、

数据清退、设备处置 6 方面内容作出了具体规定。

（三）本标准制定参考的主要依据

中华人民共和国网络安全法

中华人民共和国密码法

中华人民共和国数据安全法

GB 17859-1999 计算机信息系统安全保护等级划分准则

GB/T 37024-2018 物联网感知层网关安全技术要求

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 37988-2019 数据安全能力成熟度模型

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 25069-2022 信息安全技术 术语

三、与相关法律、行政法规和强制性标准的关系，相关推荐性标准的制定情况

本标准的制定过程中比对了网络安全法律法规中的内容。本标准内容符合国家现行法律、法规要求，并与参考的相关标准有一定的对应关系，确保与国家现行法律与部门规章相协调。

相关推荐性标准的制定情况如下：

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

YD/T 4237-2023 基于公众电信网的体育赛事网络安全

总体要求

四、与国际标准化组织、其他国家或者地区相关法律法规和标准的比对分析

网络安全是体育赛事信息化的基础和保障。然而，由于目前体育赛事网络安全架构缺乏统一的标准，安全技术漏洞、管理缺失、运行缺陷等问题日益凸显，不同建设、承建、运行保障主体的信息系统、网络等网络安全技术设备、访问策略、管理制度、运行办法难以形成横向到边、纵向到底、全面覆盖的网络安全防护体系。同时，国外的体育赛事网络安全防护措施与国内法律法规标准难以匹配，难以直接应用于在国内举办的体育赛事。因此，本标准为首自主制定，不涉及国际国外标准采标情况。

五、重大分歧意见的处理过程、处理意见及其依据

本标准的制定过程中未出现重大的分歧意见。

六、对强制性国家标准自发布日期至实施日期之间的过渡期

本标准作为行业标准，建议作为推荐性标准发布实施。标准过渡期拟定为 6 个月，用于开展标准宣贯工作，并拟于 2024 年 7 月正式实施。

七、与实施标准相关的政策措施

（一）组织措施：在国家体育总局体育信息中心的组织协调下，以标准起草组成员为主，成立标准宣贯小组，组织

撰写标准宣贯材料，2024 年拟召开标准宣贯会 1 次。

（二）技术措施：国家体育总局体育信息中心组织开展体育赛事网络安全规范化试点建设，首先要求体育总局系统内赛事执行本标准，并逐步推行至其他具有网络安全需求的赛事。计划将体育赛事网络安全架构的规划设计建设符合本标准纳入到体育总局系统赛事的招投标约束性条款中。

八、是否需要对外通报的建议及理由

本标准作为行业标准，建议作为推荐性标准发布实施。

九、废止现行相关标准的建议

不存在可废除的对应标准。

十、涉及专利的相关说明

本标准不涉及专利。

十一、标准所涉及的产品、过程或者服务目录

无。

十二、其他应予以说明的事项

无。