ICS 35.020
CCS L 80

DB23

黑 龙 江 省 地 方 标 准

DB 23/T XXXX—2024

重大活动网络安全保障指南

（征求意见稿）

起草单位：中共黑龙江省委网信办网络安全处等

联系人：于佳华

联系电话：13845064502

联系邮箱：flameyu@aliyun.com

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

2024－XX－XX 发布　　2024－XX－XX 实施

黑龙江省市场监督管理局　发 布

目　　次

前　言

本文件依据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规则》的规定起草。

请注意本文件的某些内容可能涉及专利，本文件的发布机构不承担识别专利的责任。

本文件由中共黑龙江省委网信办提出并归口管理。

本文件起草单位：中共黑龙江省委网信办网络安全处、黑龙江省公安厅网络安全保卫总队、黑龙江省通信管理局网络安全管理处、哈尔滨工业大学、黑龙江大学、国家计算机网络应急技术处理协调中心黑龙江分中心、安天科技集团股份有限公司、杭州安恒信息技术股份有限公司。

本文件主要起草人：于佳华、伍一、于洪君、孙艳丰、夏楠、赵洋、余翔湛、李柏松、王拓、李晗、曹晓光、李思元、叶麟、林峰、孙树鹏、尹尚书、朱成林。

重大活动网络安全保障指南

1 范围

本文件规定了重大活动网络安全保障的术语和定义、总体原则、工作流程、保障启动、保障准备、保障实施、保障总结等。

本文件适用于各市（地）、省直各部门开展重大活动网络安全保障时的工作。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069 信息安全技术 术语

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 43269 信息安全技术 网络安全应急能力评估准则

3 术语和定义

GB/T 25069、GB/T 22239、GB/T 43269界定的以及下列术语和定义适用于本文件。

3.1

重大活动

党政机关或社会组织举行的具有特定规模和影响的政治、经济、文化、体育及其他重大社会活动，比如国家举行的重大会议、招生考试、庆祝活动等，我省主办重大赛事、展会等。

3.2

安全

对某一系统，据以获得保密性、完整性、可用性、可核查性、真实性以及可靠性的性质。

3.3

网络安全保障

通过一系列的管理和技术手段，确保网络和信息系统的硬件、软件及系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠正常运行，网络服务不中断。

3.4

网络安全应急演练

通过模拟网络和信息系统遭受网络攻击，检验网络和信息系统应对网络安全突发事件的能力。

3.5

网络资产

网络资产是指网络空间中对组织有价值的信息和资源，是安全策略保护的对象。比如服务器、路由器、交换机等物理设备，以及信息系统、数据库等应用软件。

3.6

安全控制基线

安全控制选择过程的起始点和选择基点。

3.7

组织

具有自身的职责、权威和关系已实现其目标的个人或集体。

4 总体原则

4.1 坚持统一领导、分级负责、密切协同。

4.2 坚持底线思维、突出重点、预防为主。

4.3 坚持属地管理、谁主管谁负责、谁运行谁负责。

5 工作流程

一般重大活动及主场活动的网络安全保障流程按附录A进行，重大活动网络安全保障流程图见A.1。

6 保障启动

6.1 一般要求

6.1.1 启动条件

各市（地）、省直各部门应根据网络安全主管部门或主场活动组委会的通知要求，及时启动本地区、本部门相关重大活动网络安全保障工作。

6.1.2 明确组织结构

本项要求包括：

a) 应明确网络安全保障工作领导小组，明确组长、成员；
b) 应明确网络安全保障工作领导小组办公室及具体承接部门；
c) 应明确网络安全保障工作领导小组各组成部门工作职责；
d) 应明确保障工作联系人、工作电话、工作邮箱等。

6.1.3 制定保障方案

本项要求包括：

a) 应根据相关部门通知要求，结合相关重大活动特点以及本地区、本部门工作实际，制定《重大活动网络安全保障工作方案》，重大活动网络安全保障工作方案（模板）见附录 B；
b) 方案应满足国家、行业或地方相关标准要求；
c) 方案应经本地区、本部门网络安全保障工作领导小组审议通过。

6.2 主场活动要求

主场活动按6.1执行，还应满足如下要求：
a) 活动组委会应成立网络安全工作组，负责制定和执行主场活动网络安全保障方案；
b) 方案应对重点保障的网络、信息系统等形成细化和可操作执行的工作项；
c) 方案应经专家组论证通过；
d) 方案应经活动组委会审议通过。

7 保障准备

7.1 一般要求

7.1.1 网络资产梳理

7.1.1.1 一般资产梳理

本项要求包括：
a) 应梳理本地区、本部门所有的互联网可访问信息系统、设备的资产清单；
b) 清单应包括域名、IP 地址、端口号、用途、维护单位、维护人员等；
c) 清单应包括设备的型号、操作系统版本等；
d) 清单应包括信息系统的软件物料清单等。

7.1.1.2 高风险资产梳理

本项要求包括：
a) 应梳理本地区、本部门可能在重大活动期间如被攻击破坏，造成严重影响的资产清单；
b) 清单应包括党政机关门户网站、重点新闻网站；
c) 清单应包括面向公众服务且能够大面积影响人民群众工作、生活的业务系统；
d) 清单应包括面向公众展示的 LED 大屏；
e) 清单应包括电子邮件服务和提供公共服务的短、彩信系统平台。

7.1.2 风险排查及修复

7.1.2.1 工作组织

各市（地）、省直各部门应以自行开展或委托专业技术机构开展的方式，对本地区本部门重要网络资产进行风险排查。

7.1.2.2 一般排查

7.1.2.2.1 基线安全检查

本项要求包括：
a) 应对所梳理出资产的操作系统、数据库、中间件等安全配置进行核查；

b） 应核查账号配置、口令配置、授权配置、日志配置、通信配置等方面内容。

7.1.2.2.2 网络安全检查

本项要求包括：

a） 应对物理环境安全、设备安全、网络线路安全等物理安全项进行检查；
b） 应对账号安全、文件系统安全、服务安全、补丁管理、恶意代码防护等主机安全项进行检查；
c） 应对身份鉴别、访问控制、安全审计、跨站脚本等应用安全项进行检查；
d） 应对组织和人员安全、第三方及外包安全、日常操作与维护管理等管理制度安全项进行检查。

7.1.2.3 重点排查

本项要求包括：

a） 应对门户网站、LED 屏幕的防篡改措施进行检查；
b） 应对暴露在互联网提供服务的设备物理端（接）口进行检查；
c） 应对重要数据的防窃取措施进行检查；
a） 应对勒索病毒的防范措施进行检查；
b） 应对面向公众服务的系统平台进行压力测试。

7.1.2.4 风险修复

本项要求包括：

a） 应对基线检查发现的重要问题进行安全配置加固；
b） 应对网络安全检查发现的重要问题进行整改修复；
c） 应对重点排查发现的问题进行整改清零；
d） 应进行补丁更新，不限于设备、操作系统、应用组件等。

7.1.3 应急演练

7.1.3.1 制定应急预案

本项要求包括：

a） 应制定网络安全应急预案；
b） 应急预案应结合实际情况，确保预案具有针对性和可操作性；
c） 应急预案应根据组织调整和安全形势的变化及时更新，确保预案具有时效性和有效性；
d） 应急预案应遵从相关法律法规和标准要求。

7.1.3.2 开展应急演练

本项要求包括：

a） 应制定应急演练方案，演练方案应包括演练的规模、方式、范围、内容、组织、评估、总结、演练脚本、所需资源等内容；
b） 应按应急演练方案组织开展应急演练；
c） 应参与网络安全主管部门组织的跨地区、跨行业网络安全应急演练。

7.1.4 安全培训

本项要求包括：

a) 应定制培训课程，从个人电脑安全、邮件安全、移动安全、日常工作生活等维度进行培训，强化工作人员安全意识；
b) 应对运维人员、安全管理员进行安全技能培训，了解网络安全攻防知识，可以应对网络攻击。

7.2 主场活动要求

主场活动按7.1执行，还应满足如下要求：
a) 应分业务、分场馆梳理与活动相关的设备、信息系统、网络（含无线网路）等详细资产清单；
b) 主场活动相关网络和信息系统应按照等保三级进行安全建设；
c) 应委托多个专业技术队伍对主场活动相关网络和信息系统进行多轮次交叉式网络安全检查；
d) 应确保网络安全检查发现的问题整改清零；
e) 应急预案应针对不同等级、不同类别的网络安全事件制定相应的专项处置措施，明确启动预案的条件、处置流程、资源保障等；
f) 应急预案应包括业务中断、系统宕机、网络瘫痪等极端情况下快速有效恢复主场活动业务系统运行的有效措施；
g) 应急预案应包括突发 0 day 漏洞的应急处置措施；
h) 应采取红蓝对抗的演练方式，实战化检验网络安全防护能力和应急处置能力；
i) 应对所有工作人员进行网络安全意识培训；
j) 应建立网络安全指挥中心，在活动组委会网络安全工作组的指导下，具体统一指挥调度主场活动举行期间的网络安全监测预警和应急处置工作。

8 保障实施

8.1 一般要求

8.1.1 封网管理

本项要求包括：
a) 保障实施期间机房（IDC）应进行封网管理；
b) 应不再进行诸如服务器上下架、设备及零配件更换、路由策略、带宽调配、业务割接等涉及电路、数据调整等操作；
c) 应仅提供重启系统等基本维护操作，禁止参观机房，且不办理任何人员、设备机房出入手续。

8.1.2 驻场值守

本项要求包括：
a) 应根据网络安全主管部门、主场活动组委会以及本地区本部门保障方案要求，在重大活动举行期间或重要时间节点进行驻场值守；
b) 应制定值班表，并按照值班表安排驻场人员；
c) 值班人员中应至少包含一名部门级领导、一名具体工作人员；
d) 值班表中应包括值班电话，及具体值班人员手机号码；
e) 值班表中应包括网络、软件、中间件、数据库、服务器、网络设备等软硬件第三方开发或维护人员的联系方式。

8.1.3 监测预警

本项要求包括：

a) 应对资产变更、网络流量、日志信息、运行状态、性能状况等进行监测；
b) 应对资产脆弱性、异常行为、安全事件等进行监测和告警；
c) 应对高风险资产的安全状态设置专岗进行监测；
d) 重要监测数据留存时间应不少于 6 个月；
e) 对于监测发现的安全隐患和可疑事件，应及时进行处理，留存处理记录，如研判可能发生安全事件应及时报告；
f) 应实施零报告制度，每日撰写保障日报报送保障工作领导小组办公室。

8.1.4 事件处置

本项要求包括：
a) 应按照应急预案处置流程，对安全事件采取相应的应急处置措施；
b) 现场处置人员应及时进行先期处置，防止危害扩大；
c) 在事件处置过程中，应校验处置结果，处置不当时应采取回退措施；
d) 在恢复系统后，应对系统恢复情况开展再评估，防止系统遭受二次破坏、危害或故障；
e) 应监测网络安全事件相关舆情信息，必要时以适当方式公开通告相关情况。

8.2 主场活动要求

主场活动按8.1执行，还应满足如下要求：
a) 应同专业技术队伍共同组建值守团队，开展保障值守；
b) 应配备必要的保障值守备份人员；
c) 应开展 7×24 小时安全监测；
d) 应具备态势感知能力，及时发现阻断网络攻击行为；
e) 应按照应急预案，对不同等级、不同类别安全事件采取相应的应急处置措施，对业务中断、系统宕机、网络瘫痪等极端情况进行快速有效恢复，对突发 0 day 漏洞迅速采取应急处置措施；
f) 应实施零报告制度，定期向活动组委会报告值守情况；
g) 紧急情况应及时向活动组委会报告；
h) 应监测网络安全事件相关舆情信息，根据活动组委会有关规定，经批准后及时向新闻媒体、社会公众通告相关情况。

9 保障总结

9.1 一般要求

9.1.1 复盘总结

本项要求包括：
a) 保障工作领导小组办公室应组织专项会议对保障工作进行复盘总结，撰写《重大活动网络安全保障总结报告》，重大活动网络安全保障总结报告（模板）见附录 C；
b) 应梳理整个保障的组织和实施过程，包括组织架构、工作计划、人员配备、技术方案、安全措施等，对保障方案进行优化完善；
c) 应总结提炼保障工作的经验和教训，为今后的重大活动网络安全保障工作提供参考和借鉴；
d) 应按照要求撰写重大活动网络安全保障工作总结，并经保障工作领导小组审议后进行报送。

9.1.2 实施奖励

本项要求包括：

a） 应对保障期间表现突出的先进集体及个人进行表彰；

b） 应对保障期间出现失误造成一定损失的集体和个人进行惩戒。

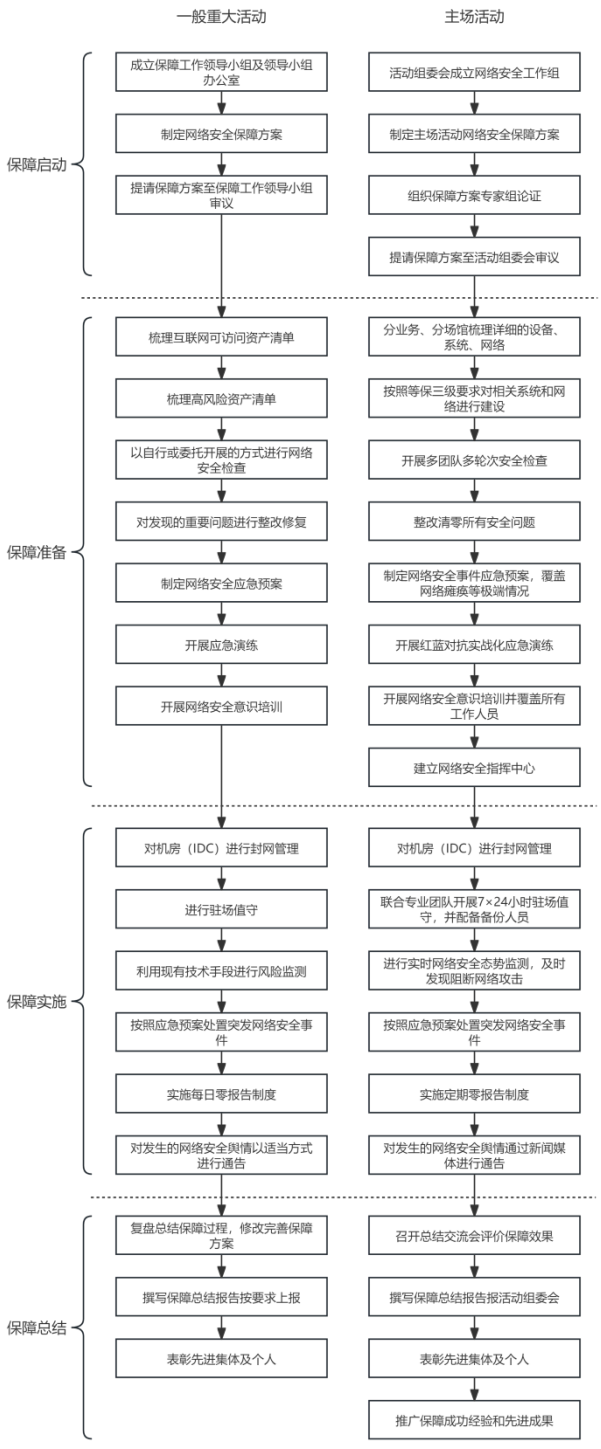
9.2 主场活动要求

主场活动按9.1执行，还应满足如下要求：

a） 活动组委会应组织网络安全保障工作总结交流会，邀请保障工作团队、主管部门、安全领域专家学者等参会，研判保障效果、总结实战经验、分享保障体会；

b） 应总结保障工作的成功经验和先进成果，探索在保障数字经济发展等领域进行推广应用。

附 录 A
（资料性）
重大活动网络安全保障流程图



图A.1 重大活动网络安全保障流程图

附 录 B
（资料性）
重大活动网络安全保障工作方案（模板）

一、工作背景

简述活动背景及网络安全保障工作背景。

二、保障目标

简述保障的工作目标及达到预期效果。

三、保障范围

描述纳入保障范围的系统及网络的名称、功能、部署位置等。

四、保障方案

描述网络安全保障前、中、后各阶段的工作部署。

附 录 C
（资料性）
重大活动网络安全保障总结报告（模板）

一、工作背景

简述网络安全保障工作开展的背景。

二、组织情况

描述开展网络安全保障的工作组织情况。

三、保障过程

描述保障前、中、后各阶段的具体工作措施及实施效果。

四、保障结果

描述保障方案中的保障目标的完成情况。

五、下步工作

简述后续工作的思路打算。

参 考 文 献

[1] 中华人民共和国网络安全法
[2] 黑龙江省网络安全事件应急预案（黑政办规〔2021〕5 号）