ICS 91.010.30
P 00

团　　体　　标　　准

T/GDCSA 003—2021

信息技术应用创新项目网络安全方案编制指南

Guidelines for network security programming of innovation projects in information technology applications

2021－**－**发布　　2021－**－**实施

广东省网络空间安全协会
信息技术创新联盟　　发布

目　　次

前　言

本标准按照 GB/T 1.1—2020 给出的规则起草。

本标准由***提出。

本标准由广东省网络空间安全协会和信息技术创新联盟归口。

本标准起草单位：　。

本标准主要起草人：　。

本标准是首次发布。

信息技术应用创新项目网络安全方案编制指南

1 范围

本标准规定了信息技术应用创新项目环境下网络安全方案编制应包括的主要内容。

本标准适用于组织对信息技术应用创新项目环境下网络安全系统建设使用单位（主持建设、信创环境下网络安全信息系统的单位）和集成资质单位对信创环境下网络安全系统等级保护方案的设计，也适用于公安工作部门对信创环境下网络安全信息系统的审批管理。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 2505.19-2010 信息安全技术 术语

GB/T 22239-2019 信息安全技术网络安全等级保护基本要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

自主可控 independently controllable

依靠自身研发设计，全面掌握产品核心技术，实现信息系统从硬件到软件的自主研发、生产、升级、维护的全程可控。

3.2

通信安全 communication security

保护网络中所传输信息的完整性、保密性、可用性等。

3.3

入侵防护 intrusion prevention

是一种可识别潜在的威胁并迅速地做出应对的网络安全行为。

3.4

网络安全 cyber security

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

3.5

身份鉴别 identification

通过相关技术，将实体标识和实体联系在一起，为其他安全服务提供支撑。

3.6

脆弱性 vulnerability

脆弱性是指信息资产或资产组中能被威胁利用的弱点，一般采用难易程度和严重性来衡量。

3.7

经济效益 economic benefit

从信息化项目产生的直接、间接经济效益出发，表征信息化项目在资金占用、成本支出与有用成果之间的比较。

4 项目概述

4.1 项目名称

项目的全称及简称。

4.2 项目单位概况

4.2.1 项目单位及负责人

1.项目建设单位：

2.项目建设单位负责人：

3.项目使用单位：

4.项目使用单位负责人：

4.2.2 项目建设及使用单位

1.应对方案设计、系统集成、软件开发、工程监理等任务承担单位的基本情况进行说明，至少包括以下内容：

1)单位资质情况及相关证书；

2)单位规模和技术实力；

3)近两年完成同类项目成功案例情况。

2.单位简介：根据三定职能，介绍单位情况及主要职责。

3.组织机构简介：画出组织机构图，展现本单位组织机构情况，包括本单位的内设机构、分支机构、直属单位、挂靠单位等。

4.3 项目编制依据

4.3.1 政策法规

《文件名称》（文号）：列举编制方案所依据的相关法律法规、经批准或审查的信息化建设规划、相关规划或主管部门的相关文件等，包括文件名称、文号。

4.3.2 标准与规范

1.（标准号）《标准规范名称》

2.《规范文件名称》（文号）（发布日期）

4.3.3 其它编制依据

列举所依据的项目审批部门的批复、项目需求分析报告及项目申报部门组织专家评议意见（如有）等，并将其中必要的部分全文附后，作为方案的附件。

4.4 项目背景

本标准针对有信息技术应用创新项目需求的客户，说明项目(系统)建设使用单位的基本情况和项目本身的建设背景（包括：国家政策背景等、行业政策背景等）等。

4.5 项目目的

结合实际情况，简要描述本次项目建设所用达到的目的。

4.6 建设内容

信创环境下建设相关的应用实施及新技术探索，包括终端、应用系统、基础设施、安全设备、运维平台及相关配套服务等，建设单位根据实际应用需求确定建设内容。

4.6.1 总体目标与分期目标

1.总体目标

项目总体目标主要表达实现业务需求后解决的社会和业务部门的实际问题、能力的提升、工作效率的提高。

2.分期目标

项目分期目标主要表达实现XXXX年至XXXX年每年度业务需求后解决的社会和业务部门的实际问题、能力的提升、工作效率的提高。

4.6.2 总体任务与分期内容

1.总体任务

描述项目总体任务，与建设单位总体信创环境下网络安全目标相匹配，根据建设单位实际情况选择重点任务简要描述即可。

2.分期内容

按项目时间段划分，若项目分多期实现，应根据项目规模及时间要求划分各期目标；也可根据建设单位实际情况选择重点任务简要描述分期内容等。若无分期，不用填写此项。

4.6.3 信创环境下网络安全应用总体设计

描述本项目在信创环境下网络安全应用方面的总体设计方案。结合项目建设方案要求，重点说明与传统建设项目不同之处，可包括如下内容：

1.说明项目中信创环境下网络安全建设的可量化的应用成效，可参考如下指标：

1） 本项目涉及信创环境下网络安全应用实施地点、应用网络、终端应用情况，包括采购数量、替换数量、建成后终端单轨率、建成后终端替换率等；

2） 信创环境下网络安全应用系统情况，包括新建应用系统数量、终端，适配改造应用系统数量、建成后应用替换率、适配率等；

3） 信创环境下网络安全产品应用种类等其他可量化的指标。

2.总结提炼项目的难点、亮点和创新点，突出项目特点。

3.若项目建设中采用了新技术、新产品、新应用，如基于信创环境下网络安全的云计算、大数据等，说明创新应用与已有软硬件产品、技术架构等的兼容设计和采用方法。

4.系统整合设计方案和网络迁移设计方案。对照台账中的已有系统功能和所支撑的业务，说明系统整合设计方案。

5.说明项目中在机制建立、安全保障、运行维护、问题管理、质量控制等方面的考虑。

5 方案设计

5.1 现状分析

5.1.1 系统建设使用单位情况

描述系统建设使用单位的情况，包括但不限于单位性质、单位组织机构、安全领导小组成员、工作职能等。对于涉及多个部门和单位参与建设的项目，按照牵头单位和参加单位的顺序分别描述。

5.1.2 网络安全技术体系分析

5.1.2.1 物理环境分析

描述使用单位现有的物理基础设施情况，包括但不限于物理位置、物理环境访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、温湿度控制、电力供应、电磁防护等情况。

5.1.2.2 网络系统分析

描述使用单位现有的网络系统情况，包括但不限于网络设备类型、数量、使用年限、网络覆盖范围、网络拓扑结构等。

5.1.2.3 网络安全分析

描述使用单位现有网络安全措施，包括但不限于网络安全设备类型、数量、使用年限、部署位置，以及系统的脆弱性、安全风险等。

5.1.2.4 软硬件资源分析

描述使用单位现有的软硬件资源情况，包括但不限于服务器设备、存储设备、网络设备、安全设备以及系统软件等的数量、型号、配置、建设年份、使用情况等。

5.1.2.5 应用系统分析

描述使用单位现有的应用系统使用情况，包括但不限于应用系统的主要功能、使用对象、数据库结构、数据内容、数据量、技术特征以及数据库软件情况等。

5.1.3 网络安全管理体系分析

描述系统配套的安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运营管理等。

5.1.4 信创覆盖率分析

描述使用单位现有信创软硬件资源现状，以及所占信息化建设比例。

5.2 需求分析

5.2.1 安全技术体系需求分析

5.2.1.1 安全物理环境

描述物理环境安全需求，应包括但不限于：机房位置、电力供应、门禁、视频监控、防雷、防火、电磁防护、温湿度等。

5.2.1.2 安全通信网络

描述安全通信网络需求分析时，应包括但不限于：网络架构、安全域划分、链路加密、加密算法、链路冗余、设备冗余、性能冗余等。

5.2.1.3 安全区域边界

描述安全区域边界需求分析时，应包括但不限于：区域边界访问权限控制、恶意代码防范、网络入侵防护、网络行为审计等。

5.2.1.4 安全计算环境

描述安全计算环境需求分析时，应包括但不限于：用户和设备身份鉴别、账号安全防护、访问权限控制、主机防病毒、应用安全防护、应用访问审计、应用系统水印、敏感数据脱敏、数据防泄露、数据备份等。

5.2.1.5 安全管理中心

描述安全管理中心需求分析，应包括但不限于：网络设备、网络链路、主机、应用系统等资源的运行状态监测和管理，对各类网络安全事件进行集中监测、采集、分析、存储和预警。

5.2.2 安全管理体系需求分析

5.2.2.1 安全管理制度

安全管理制度是一套体系，需编制安全方针、总体安全策略、安全管理制度等。安全管理制度需考虑以下方面：制定信息安全工作的总体方针、建立安全管理制度、对安全管理制度进行评审和修订、建立相应的审批部门、建立协调机制、建立审核和检查部门、建立恰当的联络渠道、建立审核和检查的制度、建立产品采购，系统测试和验收制度等内容。

5.2.2.2 安全管理机构

安全管理机构包括安全部门设置、人员岗位设置、人员安全管理等内容。安全管理机构需求分析时，应考虑以下因素：建立专门安全职能部门，对人员的录用、离岗、工作考核、安全意识的教育和培训等环节进行严格的管理，对第三方人员进行严格控制等。

5.2.2.3 安全人员管理

安全人员管理需求，包括人员的岗位设置、职责分工、人员管理等方面，安全人员管理需求分析时，应考虑以下因素：如何实现对人员的录用、离岗、考核进行严格的管理，如何对人员进行安全意识教育培训，以及如何对外部人员进行严格控制等。

5.2.2.4 安全建设管理

安全建设管理涉及定级备案管理、安全方案设计、产品采购和使用、软件开发管理、安全集成建设、测试验收交付、等级测评以及服务商选择等方面。安全建设管理需求分析时，应考虑以下因素：建立系统定级备案管理制度、定期等保测评和整改、具备技术方案设计评审和管理能力、产品采购符合国家标准、工程实施管理及监理过程控制、制定软件开发管理制度确保软件编写规范及源代码安全审计等。

5.2.2.5 安全运维管理

安全运维管理涉及机房运行管理、资产管理、系统安全运行维护管理等方面。安全运维管理需求分析时，应考虑以下因素：具备良好运行环境、资产标识及分类、及时对资产运行维护确保稳定运行、对资产的安全管理、运维工具管理以及应急响应等。

5.3 安全体系总设计

总设计目标应满足国家信创建设要求，满足具体项目总建设目标，如建立安全管理体系、建立业务连续性保障、构建安全技术体系等，应做到宏观且全面。

5.3.1 设计目标

列举项目详细要实现的目标，与总设计目标存在逻辑关联性。

5.3.2 设计原则和依据

5.3.2.1 设计原则

描述方案设计的原则，包括但不限于：合规性、先进性、针对性、可靠性、可扩展性等。

5.3.2.2 设计依据

描述方案设计的依据，包括但不限于：相关法律法规、国家标准、行业标准、行业规范等。

5.3.3 安全体系框架

描述方案设计的安全体系框架，可依据等级保护安全体系框架，结合信创建设要求，合理设计方

案的安全体系架构，建议使用架构图结合文字方式表述。

5.3.4 安全域划分

描述安全域划分的原则、思想和划分情况，以图表结合文字方式描述安全域构成情况。

5.3.5 产品选型

描述产品选型依据，包括但不限于：产品的性能、品牌、符合性等。

6 安全体系详细设计

6.1 安全技术体系详细设计

6.1.1 安全物理环境

本章节应包括机房物理位置选择、物理访问控制、防盗防破坏、防雷、防火、防水和防潮、温湿度控制、电力供应和电磁防护等方面的设计内容。

6.1.2 安全通信网络

本章节应包括网络架构、安全域划分、链路加密、加密算法、链路冗余、设备冗余、性能冗余等方面的设计内容。

6.1.3 安全区域边界

本章节应包括区域边界访问权限控制、恶意代码防范、网络入侵防护、网络行为审计等方面的设计内容。

6.1.4 安全计算环境

本章节应包括用户和设备身份鉴别、账号安全防护、访问权限控制、主机防病毒、应用安全防护、应用访问审计、应用系统水印、敏感数据脱敏、数据防泄露、数据备份恢复等方面的设计内容。

6.1.5 云计算平台

本章节属于可选内容，适用于使用云平台的项目场景。应包括云计算物理环境，云计算外部边界以及内部的访问控制、入侵防范、恶意代码防范、安全审计、加密认证和重要数据备份恢复等方面的设计内容。

6.1.6 安全管理中心

本章节应包括网络系统及云计算平台统一的系统管理、安全管理、安全审计、安全预警与通告等方面的设计内容。

6.2 安全管理体系详细设计

6.2.1 安全管理制度

本章节应包括安全策略、管理制度及其制定发布、评审修订等方面的设计内容。

6.2.2 安全管理人员

本章节应包括人员录用、人员离岗、安全意识教育培训、外部人员管理等方面的设计内容。

6.2.3 安全管理机构

本章节应包括岗位设置、人员配备、授权与审批、沟通和合作、审核和检查等方面的设计内容。

6.2.4 安全建设管理

本章节应包括系统定级备案、产品采购使用、软件自行开发和外部开发管理、工程实施与测试验收、等级测评和服务供应商选择等方面的设计内容。

6.2.5 安全运维管理（根据单位具体需求选择）

本章节应包括环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理、外包运维管理等方面的设计内容。

7 安全运营中心建设（根据单位具体需求选择）

描述安全运营中心框架建设、环境建设、团队建设、运营能力建设、运营机制建设等。

8 残留风险分析

8.1 残留风险

描述项目建设仍存在的安全风险，包括但不限于：运行安全残留风险、安全防护残留风险、安全管理残留风险、其他残留风险等。

8.2 风险规避措施

采用综合分析方法，对方案实施后的残留风险点提出规避措施建议，包括但不限于：组织保障、技术保障、管理保障、经费保障。

9 项目预算

9.1 总经费

应进行总经费说明，对于跨年度的建设项目，还应提供各年度的经费概算。

9.2 分项经费

应对各分项经费进行分析说明，至少包括经费支出内容和主要用途等；

1) 方案设计费；

2) 软件开发费；

3) 设备费（应列出产品名称、生产单位、用途、性能指标、数量、单价、总价等）；

4) 工程监理费；

5) 网络安全系统集成费；

6) 系统测评费；

7) 运行维护费。

9.3 经费来源和落实情况

经费来源：XXX

落实情况：本项目总投资估算以及计划。

10 实施计划

10.1 工程组织

应明确组织实施信创项目信创环境下网络安全信息系统等级保护方案的机构及其职责，至少包括：

1) 领导小组：由单位主管领导任责任人，信息化等相关部门参与，负责决策和总体协调；

2) 实施组：由信息化等相关部门人员组成，负责工程实施、监督、检查和指导；

3) 专家组：由信息安全技术领域的专家组成，在技术上提供咨询和指导。

10.2 任务分工

应根据信创环境下网络安全信息系统等级保护方案的具体内容，从以下方面对工程实施进行任务分工，并明确各承担单位的任务：

1） 系统集成；

2） 软件开发；

3） 综合布线；

4） 屏蔽室建设；

5） 安防监控；

6） 工程监理。

10.3 实施工期

应明确项目工期、阶段目标与任务。

10.4 进度安排

应明确工程实施各阶段的进度安排，以及系统测评和系统申请审批的时间。

序号	名称	备注
1	基础设施	
2	软件开发	
2.1	定制软件开发	
2.2	成品软件许可	
3	运行维护	
4	系统业务运营服务	
4.1	管理运营服务	
4.2	数据处理服务	
4.3	安全运营服务	
4.4	其他运营服务	
5	第三方服务	
5.2	咨询服务	
5.2	监理服务	
5.3	安全测评服务	
5.4	验收测评服务	

11 附件

11.1 软硬件配置清单

应提供方案中系统所用信创软硬件产品的配置清单。

11.2 项目预算清单

预算清单由基础设施、软件开发、运行维护、系统业务运营服务、第三方服务等组成。

序号	名称	备注
1	基础设施	
2	软件开发	
2.1	定制软件开发	
2.2	成品软件许可	
3	运行维护	
4	系统业务运营服务	
4.1	管理运营服务	
4.2	数据处理服务	
4.3	安全运营服务	
4.4	其他运营服务	
5	第三方服务	
5.1	咨询服务	
5.2	监理服务	
5.3	安全测评服务	
5.4	验收测评服务	

11.3 其他证明材料

应提供系统承建单位的法人营业执照复印件、部分合同复印件等其他证明材料。