

DB4403

深 圳 市 地 方 标 准

DB4403/T XXX—XXXX

数字政府信息技术服务供应链安全要求

Security requirements for supply chain of digital government information
technology service

(送审稿)

XXXX-XX-XX 发布

XXXX-XX-XX 实施

深圳市市场监督管理局 发 布

目 次

前言 II

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 要求概述 2

 4.1 信息技术服务类型 2

 4.2 信息技术服务供应链安全目标 3

 4.3 信息技术服务供应链安全管理基本原则 3

 4.4 信息技术服务供应链安全要求框架 3

5 需方安全要求 4

 5.1 通用安全要求 5

 5.2 开发与集成服务供应链扩展安全要求 13

 5.3 运营与维护服务供应链扩展安全要求 15

 5.4 基础设施服务供应链扩展安全要求 177

 5.5 生成式人工智能服务供应链扩展安全要求 18

 5.6 其他服务供应链扩展安全要求 19

6 供方安全要求 19

 6.1 通用安全要求 19

 6.2 开发与集成服务供应链扩展安全要求 25

 6.3 运营与维护服务供应链扩展安全要求 29

 6.4 基础设施服务供应链扩展安全要求 31

 6.5 生成式人工智能服务供应链扩展安全要求 34

 6.6 其他服务供应链扩展安全要求 36

附录 A（资料性） 安全要求与其他法律法规技术标准的对应关系 37

附录 B（资料性） 通用要求对应安全风险 38

附录 C（资料性） 扩展要求对应安全风险 41

附录 D（规范性） 安全评估评分方法 47

附录 E（规范性） 增强安全要求 48

参考文献 49

前 言

本文件按照 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。

本文件由深圳市政务服务和数据管理局提出并归口。

本文件起草单位：深圳市信息安全管理中心、国家信息中心、深圳市南山区智慧城市运营中心、深圳市盐田区网络安全和信息化中心、深圳市盐田区政务服务中心、深圳市宝安区信息中心、深圳海云安网络安全技术有限公司、深圳市智慧城市科技发展集团有限公司、杭州默安科技有限公司、金砖国家未来网络研究院中国分院。

本文件主要起草人：张军、董安波、罗菁春、林宇群、穆端端、赵剑、轩豪男、潘志斌、童子琦、彭磊磊、张灏、赵睿斌、方景鑫、王佳颖、姚俊华、林军、廖英豪、颜军、郭志远、谢朝海、彭波、蔡宏安、雷德诚、蒋亚伟、黄焱、王志、吴飞、程进、张桐桐、周罗红、林桢、李小叶、王佳。

数字政府信息技术服务供应链安全要求

1 范围

本文件确立了数字政府信息技术服务供应链安全要求目标，规定了信息技术服务供应链供需双方的基本安全要求、服务规划安全要求、服务入场安全要求、服务实施安全要求和服务结束安全要求。

本文件适用于指导数字政府范围内非涉密信息技术服务供应链中的供需双方开展供应链安全管理，为第三方机构开展信息技术服务供应链安全检测和评估提供依据，供主管监管部门参考使用。

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 2887—2011 计算机场地通用规范
- GB/T 9361—2011 计算机场地安全要求
- GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
- GB/T 28458—2020 信息安全技术 网络安全漏洞标识与描述规范
- GB/T 30276—2020 信息安全技术 网络安全漏洞管理规范
- GB/T 30279—2020 信息安全技术 网络安全漏洞分类分级指南
- GB/T 31168—2023 信息安全技术 云计算服务安全能力要求
- GB/T 32400—2015 信息技术 云计算 概览与词汇
- GB/T 34943—2017 C/C++语言源代码漏洞测试规范
- GB/T 34944—2017 Java语言源代码漏洞测试规范
- GB/T 36637—2018 信息安全技术 ICT供应链安全风险管理体系指南
- GB/T 39412—2020 信息安全技术 代码安全审计规范
- GB/T 39770—2021 信息技术服务 服务安全要求

3 术语和定义

GB/T 36637—2018、GB/T 39770—2021界定的以及下列术语和定义适用于本标准。

3.1

需方 acquirer

从其他组织获取服务或产品的政府部门或政府组织。

[来源：GB/T 36637—2018，3.1，有修改]

3.2

供方 supplier

提供服务或产品的组织。

注：供方也可称供应商、供应方。

[来源：GB/T 36637—2018，3.2，有修改]

3.3

信息技术服务 information technology service

供方（3.2）为需方（3.1）提供开发、应用信息技术的服务或产品，以及供方以信息技术手段提供支持需方业务活动的服务。

注：常见的数字政府信息技术服务类型包括软件开发服务、系统集成服务、安全服务和运行运维服务、业务运营服务、基础设施服务及第三方服务等。

[来源：GB/T 39770—2021，3.1]

3.4

服务供应链 supply chain of digital government service

为满足信息技术服务（3.3）供应关系通过资源和过程将需方（3.1）、供方（3.2）相互连接的网链结构，可用于将服务或产品提供给需方。

[来源：GB/T 36637—2018，3.4，有修改]

3.5

供应链安全风险 supply chain security risk

供应链安全威胁利用供应链管理中存在的脆弱性导致供应链安全事件的可能性，及其由此对组织造成的影响。

[来源：GB/T 36637—2018，3.5]

3.6

次级供应商 sub-suppliers

向供方（3.2）提供服务或产品的组织或个人。

注：次级供应商也可称多级供应商。

[来源：GB/T 36637—2018，3.2，有修改]

3.7

数字政府 digital government

以新一代信息技术为支撑，重塑政务信息化管理架构、业务架构、技术架构，通过构建大数据驱动的政务新机制、新平台、新渠道，进一步优化调整政府内部的组织架构、运作程序和管理服务，全面提升政府在经济调节、市场监管、社会治理、公共服务、生态环境等领域的履职能力，形成“用数据对话、用数据决策、用数据服务、用数据创新”的现代化治理模式。

[来源：《广东省人民政府关于印发广东省“数字政府”建设总体规划（2018-2020年）的通知》，引言，有修改]

4 要求概述

4.1 信息技术服务类型

数字政府信息技术服务供应链包括服务类型如下。

- a) 开发与集成服务主要包含软件设计与开发、系统集成、硬件集成、安全集成等类型的信息技术服务。
- b) 运营与维护服务主要包含基础设施运维、软件运维、硬件运维、安全运维、综合运维管理、呼叫中心、数据加工处理、存储服务等类型的信息技术服务；

- c) 基础设施服务主要包含物理机房、5G专网、通信网络、云计算基础平台、区块链等信息技术基础设施服务；
- d) 生成式人工智能服务主要包含生成式人工智能服务算法、算力、数据和应用等服务；
- e) 其他服务主要包含咨询规划、测试评估、渗透测试、等级测评、密码测评等第三方服务和其他信息技术服务。

4.2 信息技术服务供应链安全目标

数字政府信息技术服务需方和供方应采取合理和适当的管理与技术保障措施，以达到目标如下。

- a) 防范数字政府信息技术服务供应关系建立及供应过程的相关安全风险，确保服务供应商可信、供应过程可靠、供应物可控和供应服务可持续。
- b) 保障数字政府信息技术服务供应链的韧性，持续增强服务供需双方安全合规和保障能力。
- c) 确保数字政府信息技术服务供应链安全满足数字政府业务发展的需要。

4.3 信息技术服务供应链安全管理基本原则

政府部门在实施数字政府信息技术服务供应链安全管理时应遵循基本原则如下。

- a) 安全合规原则：数字政府信息技术服务供应链安全管理应以符合网络安全有关的法律法规和标准规范为原则。附录A给出了本文件与法律规范和标准规范对应关系。
- b) 责任不变原则：政府部门委托第三方提供数字政府信息技术服务的，各单位的网络安全与数据安全主体责任不变，安全管理标准不变。
- c) 体系化安全原则：数字政府信息技术服务供应链安全管理应对服务全生命周期、全过程进行安全管控，形成安全管理和技术措施相结合的纵深防御体系。附录B和附录C给出了供应链常见安全风险。
- d) 动态调整原则：应根据数字政府信息技术服务供应链的运行机制、运行环境等方面的变化，及时调整安全保护措施，确保数字政府信息技术服务供应链的安全。在更高安全需求场景下，应遵循附录E增强安全要求。

4.4 信息技术服务供应链安全要求框架

4.4.1 框架内容

数字政府信息技术服务供应链安全要求框架由通用安全要求和扩展安全要求两部分构成，其中通用安全要求包括基本安全要求和过程通用安全要求两部分，扩展安全要求覆盖开发与集成服务、运营与维护服务、基础设施服务、生成式人工智能服务、其他服务等信息技术服务的过程扩展安全要求。供应链中各服务类型的整体安全框架如图1所示，框架内容对需方和供方规定了服务供应链通用安全要求和服务供应链过程扩展安全要求。过程扩展安全要求是在过程通用安全要求的基础上，针对开发与集成服务、运营与维护服务、基础设施服务、生成式人工智能服务、其他服务在服务供应过程中的差异化提出的安全要求，如图1所示。

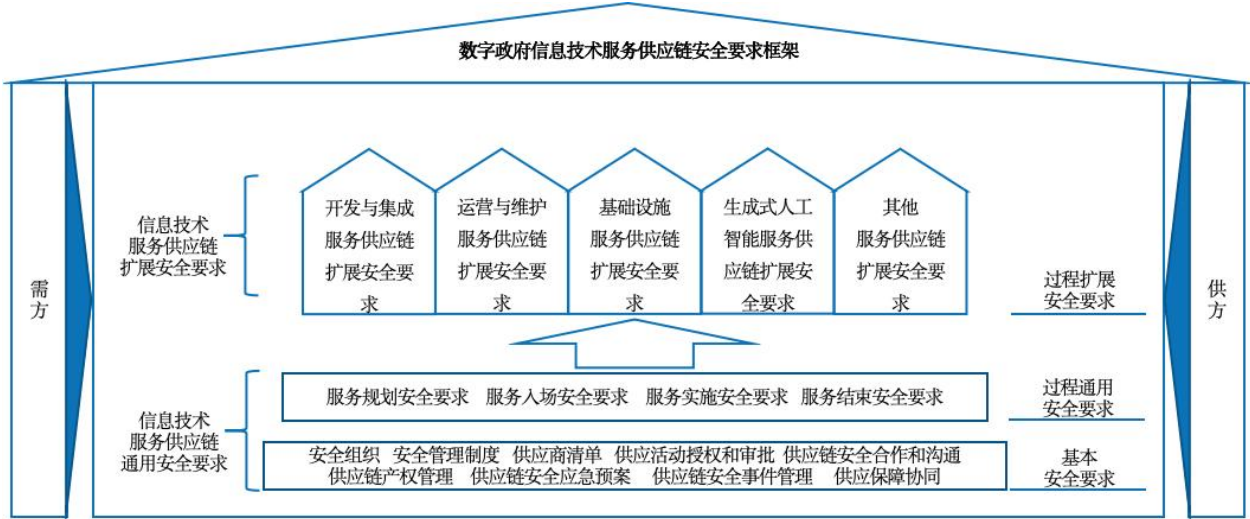


图1 信息技术服务供应链安全要求框架

4.4.2 框架适用服务

数字政府信息技术服务供应链通用安全要求适用于所有信息技术服务。服务供应链过程扩展安全要求分别适用于不同类型的信息技术服务项目。表1列出各种类型的信息技术服务项目应该满足的服务供应链过程扩展安全要求。当一个信息技术服务项目含有多种服务类型的信息技术服务时，该项目应该同时满足这些服务类型对应的服务供应链过程扩展安全要求。信息技术服务项目应满足安全要求见表1。

表1 信息技术服务项目应满足的服务供应链过程扩展安全要求一览表

数字政府信息技术服务 供应链安全要求	开发与集成服务	运营与维护服务	基础设施服务	生成式人工 智能服务	其他服务
信息技术服务通用安全要求	√	√	√	√	√
开发与集成扩展安全要求	√	×	×	×	×
运营与维护服务扩展安全要求	×	√	×	×	×
基础设施服务扩展安全要求	×	×	√	×	×
生成式人工智能服务扩展安全要求	×	×	×	√	×
其他服务扩展安全要求	×	×	×	×	√
注：√表示应该满足，×表示可以不要求。					

5 需方安全要求

5.1 通用安全要求

5.1.1 基本安全要求

5.1.1.1 组织机构

组织机构对需方要求如下：

- a) 应明确指定由内部网信安全管理部门或者专门部门负责数字政府信息技术服务供应链安全统筹管理工作，并制度化；
- b) 应明确数字政府信息技术服务供应链安全管理责任部门的相关工作职责，相关工作职责内容包括服务供应链安全管理制度的制定和维护、服务供应链安全技术防护措施的计划与落实、服务供应链资源的提供和管理及服务供应链相关人员的安全教育培训等。

5.1.1.2 安全管理制度

安全管理制度对需方要求如下：

- a) 应制定数字政府信息技术服务供应链安全管理制度或者在相关网络安全管理制度中明确信息技术服务供应链安全管理相关内容，内容包括信息技术服务供应链安全总体方针、供应商安全管理、服务供应活动安全管理、服务供应参与人员安全管理及知识产权管理等；
- b) 应每年组织不少于1次对数字政府信息技术服务供应链管理制度相关内容进行评审，并依据评审结果进行必要的更新；
- c) 应每年组织不少于1次对数字政府信息技术服务供应链安全管理制度相关内容进行宣贯培训。

5.1.1.3 供应商清单

供应商清单对需方要求如下：

- a) 应基于现有项目整理服务供应商清单，清单内容应包括企业名称、统一社会信用代码、注册所在地、联系人、联系方式、服务类型、专业资质、关联项目等信息；
- b) 应每年对数字政府信息技术服务供应商开展不少于1次的安全评审，对供应商安全资质以及关联项目安全评价等信息进行审查，更新供应商管理清单信息；
- c) 应持续对数字政府信息技术服务供应商威胁情报进行监测，对可能影响服务供应的事件进行评估和处置，并更新供应商管理清单相关信息，监测内容包括：供应商负面舆情、股权结构变化、网络安全事件、业务经营风险、资质存续情况、交付产品的安全漏洞等信息。

注：供应商安全事件监测应关注执法部门披露信息、信息安全通报、应急响应机构的风险提示、国家网络安全审查结果等。

5.1.1.4 供应活动授权和审批

供应活动授权和审批对需方要求如下：

- a) 应明确数字政府信息技术服务供应链安全管理工作的授权审批事项、审批部门和批准人等；
- b) 应针对数字政府信息技术服务供应过程中的重要操作、物理访问和系统接入等重要事项建立审批程序，按照审批程序执行审批过程，对重要事项建立服务项目组内的逐级审批流程；
- c) 应每年组织不少于1次数字政府信息技术服务供应链授权审批事项及审批流程审查，并依据评审结果进行必要的更新；
- d) 数字政府信息技术服务供应链授权审批事项、审批部门和审批人等信息发生变更后应及时更新相关流程。

5.1.1.5 供应链安全合作和沟通

供应链安全合作和沟通对需方要求如下：

- a) 应加强与供应商之间的合作与沟通，每半年组织不少于1次协调会议，共同协作处理数字政府信息技术服务供应链安全相关问题；
- b) 应建立项目应急处置机制，处理数字政府信息技术服务供应过程中产生的投诉、争议和突发事件等，并形成处置结论或解决方案；
- c) 应加强与信息技术服务供应链业界专家及安全组织的合作与沟通；
- d) 应建立信息技术服务供应链业界专家及安全组织联系列表，包括单位名称、合作内容、联系人和联系方式等信息。

5.1.1.6 供应链产权管理

供应链产权管理对需方要求如下：

- a) 数字政府信息技术服务供应链安全管理内容应包含明确的知识产权管理要求，应明确要求管控信息技术服务供应链知识产权风险，避免或降低信息技术服务中所涉及的设备、工具、代码和产品因侵权、授权等知识产权问题导致的法律纠纷及合规风险；
- b) 信息安全风险评估应纳入数字政府信息技术服务供应链知识产权和数据产权风险内容，分析其可能发生的纠纷及损失，提出防范与应对预案。并对剩余风险进行评估，应确保剩余风险符合单位风险接受准则。

5.1.1.7 供应链安全应急预案

供应链安全应急预案对需方要求如下：

- a) 应制定数字政府信息技术服务供应链安全事件应急预案，包括启动预案的条件、应急组织构成、应急资源保障、应急处理流程、供应链恢复流程、事后教育和培训等内容；
- b) 应每年组织不少于1次数字政府信息技术服务供应链相关人员进行应急预案培训和演练；
- c) 应每年组织不少于1次对原有的应急预案进行重新评估，修订完善。

5.1.1.8 供应链安全事件管理

供应链安全事件管理对需方要求如下：

- a) 应制定数字政府信息技术服务供应链安全事件处置和报告管理流程，明确不同安全事件的处置和报告等响应流程，规定安全事件的现场处理、后期恢复和事件报告的管理职责等；
- b) 应在数字政府信息技术服务活动中发生以下重大风险事件时，及时向市数字政府主管部门和网信主管部门报告，需要报告的事件包括但不限于：
 - 1) 需方重要数据或个人信息泄露；
 - 2) 需方数据损毁或者重要业务运营中断；
 - 3) 因供方不当行为或其服务的信息系统遭受网络攻击或其他原因，造成需方重大损失；
 - 4) 发现重大的供方违法违规事件；
 - 5) 重要供应服务非正常中断、终止或供方非正常退出；
 - 6) 其他规定需要报告的重大安全事件。

- c) 在数字政府信息技术服务供应过程中发生重大安全事件时，应及时开展事件调查和处置。应开展相关信息安全风险评估，分析风险原因及可能造成的损失，总结经验改进重大安全事件的应急预案。

5.1.1.9 供应链安全检查评估

供应链安全检查评估对需方要求如下：

- a) 应每年组织不少于1次数字政府信息技术服务供应链安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；
- b) 应对数字政府信息技术服务供应链安全检查结果进行通报，督促供方对安全检查结果中不合规内容进行整改，无法整改的应记录在案并注明原因。

5.1.2 服务规划安全要求

5.1.2.1 服务供应商选择

服务供应商选择对需方要求如下：

- a) 数字政府信息技术服务应避免过度依赖单一供应商，防止发生供应商依赖和服务中断风险；
- b) 应根据供应商清单、信息技术服务类型、业务重要性以及服务对象的安全等级，进行数字政府信息技术服务供应商选择，应优先选择满足下列条件数量最多的供应商：
 - 1) 有相关类型项目经验，具备成熟的项目安全管理方案和服务安全技术实施能力；
 - 2) 对次级供应商实施了安全管理；
 - 3) 对服务项目全生命期制定了安全管理计划，措施符合法律法规安全要求；
 - 4) 不存在服务中断风险；
 - 5) 不存在影响或可能影响国家安全的风险；
 - 6) 在历史合同履行中未发生过重大安全事件；
 - 7) 在中华人民共和国境内注册的供应商。

5.1.2.2 安全合规审查

安全合规审查对需方要求如下：

- a) 拟采购的数字政府信息技术服务或产品影响或可能影响国家安全的，应按有关规定对服务或产品开展网络安全审查。不应选择未通过网络安全审查的服务或产品；
- b) 拟采购的数字政府信息技术服务或产品涉及密码应用的，应按有关规定制定密码应用方案、组织方案安全性评估、规划及建设密码保障系统，并每年组织不少于1次密码应用安全性评估。

5.1.2.3 采购合同或协议

采购合同或协议对需方要求如下：

- a) 应在数字政府信息技术服务采购合同或协议中明确服务供方的网络安全相关责任和义务，包括但不限于：
 - 1) 明确约定服务的范围、工作内容；
 - 2) 明确服务的服务水平要求、功能要求、安全要求、培训要求等；
 - 3) 明确提出供应商应满足的安全管理要求和安全技术要求；
 - 4) 明确分包、转包的安全要求；

- 5) 明确对供方服务人员团队的能力要求及成员合规性、稳定性要求;
 - 6) 明确安全保密要求,明确保密内容、保密期限、保密范围;
 - 7) 明确数据安全及个人信息保护要求;
 - 8) 明确服务项目合同不生效、无效、被撤销或者终止的离场要求;
 - 9) 明确不履行网络安全和安全保密相关义务的违约责任。
- b) 应在数字政府信息技术服务采购合同或协议中明确对服务供方的知识产权要求,包括但不限于:
- 1) 明确服务项目产出物(如著作、专利、论文、数据等)的知识产权归属,涉及多个合作方的知识成果,划分确定产出物的知识产权归属;
 - 2) 供方承诺整个服务项目中不存在开源软件使用合规风险、商业授权法律风险、盗用冒用需方知识产权等行为;
 - 3) 明确处理知识产权纠纷的解决方式,包括协商、诉讼、仲裁、调解等。
- c) 应在数字政府信息技术服务采购合同或协议中明确对服务和产品的安全要求,包括但不限于:
- 1) 要求对第三方代码、开源组件及基础模型的使用进行安全管控;
 - 2) 要求提供关键软硬件、基础模型及服务的备选方案和供应商;
 - 3) 涉及个人信息数据处理的,明确个人信息数据确权授权要求。不得采取强制同意等方式过度收集个人信息,应按照个人信息主体授权范围依法依规采集、传输、存储和使用;
 - 4) 涉及采购现货软件和硬件产品的,明确产品的授权使用期限、维保期限、完整性和安全性要求;
 - 5) 涉及采购信息安全设备、核心网络设备、系统软件、基础软件和业务应用软件等关键产品的,明确采购产品的自主可控、信创、商业授权期限及维保期限等要求。
- d) 应在数字政府信息技术服务采购合同或协议中明确对服务安全能力的要求,包括但不限于:
- 1) 明确对可能涉及的敏感信息的访问、处理、存储要求;
 - 2) 明确对服务工具(包括设备、软件、模板和知识库等)的要求;
 - 3) 服务对象的安全保护等级为二级及以上的,应明确业务连续性保障要求。
- e) 在数字政府信息技术服务采购合同或协议中应要求供方做出必要的安全承诺,包括但不限于:
- 1) 承诺不非法获取用户数据、控制和操纵用户系统和设备;
 - 2) 承诺不利用需方对服务以及产品的依赖性谋取不正当利益或者迫使需方更新换代;
 - 3) 承诺不向未授权方提供需方的相关数据,或者将相关数据用于项目实施以外的目的。

5.1.3 服务入场安全要求

5.1.3.1 实施方案准备

实施方案准备对需方要求如下:

- a) 应为数字政府信息技术服务项目指定一名以上安全管理人员负责该项目的供应链日常安全管理工作,人员安全管理能力应符合本项目网络安全管理人员的水平要求;
- b) 应组织对数字政府信息技术服务项目供方提交的项目组人员资质、项目安全管理方案和项目安全管理计划进行评审;
- c) 应准备针对数字政府信息技术服务项目供方设备和工具入场安全检查的方案和计划;
- d) 应准备针对数字政府信息技术服务项目供方人员的安全培训方案和计划,方案和计划应与供方的培训方案和计划保持一致,包括入场安全培训和长期服务项目实施过程中定期安全培训。培训内容应包含需方网络安全规定、数据安全规定、保密要求、违规责任等,影响或可能影响国家安全的还应包含反间谍培训内容。

5.1.3.2 供应商人员安全

供应商人员安全对需方要求如下：

- a) 应组织审查数字政府信息技术服务项目供方提交的项目组人员背景资料；
- b) 数字政府信息技术服务对象的安全保护等级为二级及以上或者可能影响国家安全的，应开展供方项目参与人员国籍审查；
- c) 应与数字政府信息技术服务项目供方参与人员签订安全承诺书和保密协议，协议内容应包括服务项目安全实施要求、安全保密要求及违约责任等内容；
- d) 应要求数字政府信息技术服务项目供方参与人员在服务供应过程中及服务结束离场后不得将需方数据泄露给他人，或者利用需方数据实施不利于需方的行为。

5.1.3.3 人员入场控制

人员入场控制对需方要求如下：

- a) 应为数字政府信息技术服务项目供方参与人员分配物理身份标识，包括供应商专用的工卡或铭牌等，并将访问授权控制其在工作中所需的最小物理区域；
- b) 应对数字政府信息技术服务项目供方参与人员提出的接入需方网络系统书面申请进行内部流程审批；
- c) 应由专人为通过审批的数字政府信息技术服务项目供方参与人员开设网络系统账户，授予工作所需的最小权限，并按需开启网络系统账号多因子认证；
- d) 不应共享需方人员账号给数字政府信息技术服务项目供方参与人员；
- e) 应依据入场安全培训方案和计划对数字政府信息技术服务项目供方参与人员开展入场安全培训。

5.1.3.4 设备入场控制

设备入场控制对需方要求如下：

- a) 应依据入场安全检查方案和计划对数字政府信息技术服务项目拟接入需方网络的供方设备和工具进行安全检测、病毒查杀和商业授权确认，通过安全检查、商业授权确认和安装准入客户端后方可接入使用；
- b) 应为数字政府信息技术服务项目供方设备和工具分配物理和网络身份标识，包括供应商专用的设备SN、设备铭牌和网络标识等，并采取措施对供应商设备和工具进行身份鉴别；
- c) 应为数字政府信息技术服务项目供方设备和工具分配工作所需的最小网络、系统和数据访问权限，并配置相关的访问策略。

5.1.4 服务实施安全要求

5.1.4.1 供应过程访问控制

供应过程访问控制对需方要求如下：

- a) 应在数字政府信息技术服务项目供方人员访问物理受控区域前先提出书面申请，批准后安排专人全程陪同；
- b) 数字政府信息技术服务项目应限制通过互联网等公共网络进行电子政务内网的远程访问实施，如需远程访问实施的，应采取零信任访问控制、限时开通和空闲关闭等措施保证远程实施接入的安全性，并记录、审计远程访问行为；

- c) 数字政府信息技术服务项目实施过程中涉及供方设备无线接入网络的,应对无线接入网络进行安全管控,安全管控措施包括但不限于:
 - 1) 开启接入认证功能,并支持采用认证服务器认证或国家密码管理机构批准的密码模块进行认证;
 - 2) 保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备。
- d) 数字政府信息技术服务项目实施过程中涉及使用移动终端设备的,应对移动终端设备进行安全管控,安全管控措施包括但不限于:
 - 1) 确保移动工作终端安装、注册并运行终端管理客户端软件;
 - 2) 确保移动工作终端具有移动应用管控功能,具备选择应用软件安装、运行的黑白名单功能,能够允许指定证书签名的应用软件安装和运行,能根据黑白名单控制应用软件安装、运行;
 - 3) 确保移动工作终端接受移动终端管理服务端的设备生命周期管理、设备远程控制,如远程锁定、远程擦除等。
- e) 数字政府信息技术服务项目应限制授予供方人员需方业务系统和设备的特权账户,因工作确实需要授予业务系统和设备特权账户时,应采取必要的控制措施,包括但不限于:
 - 1) 仅授予供方负责人或特定操作人员使用;
 - 2) 通过多因子认证、时间限定、设备限定等技术措施管控特权账户的登录和使用;
 - 3) 记录、审计特权账户授予期间的所有操作行为。

5.1.4.2 供应过程数据安全

供应过程数据安全对需方要求如下:

- a) 应对供方在数字政府信息技术服务过程中访问到的敏感信息和重要数据采取如下措施,确保数据不被非授权访问和泄露:
 - 1) 应进行加密存储,部署必要的数据脱敏、数据水印、加密传输等技术措施;
 - 2) 应采用虚拟桌面访问、多因子认证等方式控制数据访问、操作等行为,重要操作应需要二次身份鉴别;
 - 3) 应利用技术措施管控数据的非授权打印、下载、拷贝等操作。
- b) 数字政府信息技术服务项目实施授权供方下载、导出敏感信息、重要数据的,应对数据进行脱敏处理、添加数据水印,以及指定数据导出方式和工具,并记录、审计数据导出行为;
- c) 涉及重要数据和个人信息处理或者关系国家安全、政府声誉的数字政府信息技术服务,服务全过程数据不得跨境。

5.1.4.3 供应过程安全监测

供应过程安全监测对需方要求如下:

- a) 应当对数字政府信息技术服务供应过程的网络安全、数据安全进行监测和记录,主动识别、处置和通报服务供应过程中的物理损毁、网络攻击、数据破坏、信息泄露、配置篡改、非法利用等安全风险;
- b) 应对数字政府信息技术服务供方参与人员及自带设备的物理和网络访问行为进行安全监测,及时发现非法访问、未授权访问等违规行为,防范其导致的安全风险,监测的内容包括但不限于:
 - 1) 对服务项目供方参与人员访问需方办公、计算、网络、存储、安全资源的行为进行安全监测,及时发现非法访问、违规数据传输和危险操作等安全风险;

- 2) 对服务项目供方参与人员物理和网络身份标识的使用进行安全监测，及时发现身份标识冒用、转借等违规行为；
 - 3) 对服务项目供方参与人员授权账号的使用进行安全监测，及时发现账号异地登录、非工作时间登录、非常用客户端登录、疑似批量数据查询导出、未授权访问尝试等异常行为；
 - 4) 对服务项目供方人员的高风险操作行为进行监测，及时发现非授权数据增删改、批量数据查询导出、数据文件下载/拷贝、数据库拖库等安全风险；
 - 5) 对服务项目的特权账户行为进行监测，及时发现异常登录行为、异常操作行为等安全风险；
 - 6) 对服务项目中供方自带设备和工具的运行使用进行安全监测，及时发现设备和工具的非法连接、恶意代码和非授权程序等安全风险。
- c) 应持续对数字政府信息技术服务供方的股权结构变化、业务经营风险、资质存续情况进行监测，对监测发现的可能导致服务供应中断的情况采取措施进行防范和应对。

5.1.4.4 供应过程检查评估

供应过程检查评估对需方要求如下：

- a) 应每季度组织不少于1次对数字政府信息技术服务供应过程供方设备和工具的安全性进行检查，包括扫描设备和工具是否存在恶意程序，分析其网络流量是否异常等；
- b) 应每年组织不少于1次对数字政府信息技术服务供应过程需方提供的办公、计算、网络、存储、安全等资源的安全性进行检查，确保相关资源未被挪用、不安全使用；
- c) 应每季度组织不少于1次对数字政府信息技术服务供应过程供方服务质量进行检查，检查内容包括安全管理落实情况、项目实施进度、服务供应质量等，确保服务供应质量可控、安全可靠。

5.1.4.5 供应过程变更安全

供应过程变更安全对需方要求如下：

- a) 数字政府信息技术服务项目实施过程发生供应物、服务人员、软硬件升级及参数配置改动等变更时，变更方应提出变更申请，变更申请应包括变更内容、变更时间、变更风险分析及应对措施等内容；
- b) 数字政府信息技术服务项目需方应组织对变更申请进行评审，变更经过审批后方可实施；
- c) 因供应物替换导致的数字政府信息技术服务项目变更，需方应：
 - 1) 审阅相关的安全性、完整性检测报告，评估替换供应物的功能及安全性；
 - 2) 及时更新供应物资产管理信息；
 - 3) 及时更新访问控制等相关安全配置策略。
- d) 因数字政府信息技术服务项目供方参与人员替换导致的信息技术服务变更，需方应：
 - 1) 评估供方替换人员的能力与资质；
 - 2) 与供方待离场人员签署服务终止确认协议，回收相应的账户权限等资源；
 - 3) 与供方替换人员签订服务安全或保密协议，提供工作所需最小权限账户等相应资源。
- e) 数字政府信息技术服务项目应限制供方对生产环境的信息系统、软件、硬件及其固件进行升级、卸载、变更等操作，如需操作应取得需方授权后方可执行，并记录、审计相关操作。

5.1.5 服务结束安全要求

5.1.5.1 服务结束方案

服务结束方案对需方要求如下：

- a) 应制定数字政府信息技术服务供应商离场管理方案，管理供应商离场安全风险，确保现有业务正常运行；
- b) 数字政府信息技术服务供应商离场管理方案应包括服务完整移交确认、供方设备和人员授权撤销、供方设备数据清除、服务供应链安全评价和服务中断安全风险评估等内容。

5.1.5.2 服务资料移交

服务资料移交对需方要求如下：

- a) 应对数字政府信息技术服务项目供方移交的完整性进行确认，包括文档资料、知识产权成果、知识培训以及关联次级供应商信息等；
- b) 应对数字政府信息技术服务项目供方提交材料的真实性进行验证，包括安全漏洞验证、引用数据来源和真实性核验等。

5.1.5.3 离场资源回收

离场资源回收对需方要求如下：

- a) 应回收分配给数字政府信息技术服务项目的办公、计算、网络、存储、安全等资源；
- b) 应回收分配给数字政府信息技术服务项目的网络、系统、设备等用户账号及权限。

5.1.5.4 人员离场管理

人员离场管理对需方要求如下：

- a) 应回收分配给数字政府信息技术服务项目相关离场人员的物理身份标识，包括供应商专用的工卡或铭牌等；
- b) 应撤销数字政府信息技术服务项目相关离场人员的系统账号和权限；
- c) 应要求数字政府信息技术服务项目相关离场人员不得私自预留用户账号、预留程序后门、植入恶意代码等。

5.1.5.5 设备离场管理

设备离场管理对需方要求如下：

- a) 应回收数字政府信息技术服务项目供方离场设备进场所分配的设备SN、设备铭牌、网络IP和标识等；
- b) 应将数字政府信息技术服务项目供方测试设备、试用设备下线，清除或迁移需方相关数据；
- c) 应对数字政府信息技术服务项目供方离场设备和工具进行离场安全检查，确认已迁移、清除需方相关数据。

5.1.5.6 服务结束评估

服务结束评估要求如下。

- a) 应对数字政府信息技术服务项目离场供应商进行服务供应链安全评估，评估内容须包含次级供应商安全管理、项目安全管理、服务安全技术符合性等内容；
- b) 数字政府信息技术服务供应链安全评估结果应记录在案，并作为下次数字政府信息技术服务供应商选择采购的参考。供应链安全评估应按照附录D进行评估评分。

5.2 开发与集成服务供应链扩展安全要求

5.2.1 服务规划安全要求

5.2.1.1 项目安全需求

项目安全需求对需方要求如下：

- a) 应在项目规划阶段对数字政府开发与集成服务项目进行安全定级，在需方内部初步确定安全保护等级；
- b) 涉及软件开发的数字政府开发与集成服务项目，应组织开展项目需求分析及软件安全需求文档评审：
 - 1) 应根据国家标准以及自身业务要求制定软件的安全需求基线，确保软件产品安全并保护个人敏感信息、重要数据等不被泄露；
 - 2) 应要求供方开展安全需求分析，提出安全需求，并在软件需求规格说明等需求文档中明确记录或者单独编制形成软件安全需求文档。

5.2.2 服务实施安全要求

5.2.2.1 开发集成测试环境

开发集成测试环境对需方要求如下：

- a) 数字政府宜建立统一的开发集成测试环境，并确保开发集成测试环境与生产环境的物理隔离，无法物理隔离的应采取可信访问控制，相关环境仅提供给授权的开发集成服务团队使用；
- b) 涉及非驻场软件开发的数字政府软件开发与集成服务项目，应要求供方加强软件开发集成测试环境的安全管控，确认供方采取访问控制、安全扫描、配置核查、安全加固、安全审计等措施保证开发与测试环境的安全性；
- c) 涉及软件开发的数字政府开发与集成服务项目，应对供方提出安全开发管理要求，包括但不限于：
 - 1) 应要求供方在开发过程采取代码版本控制、安全开发流程管理、安全检测等措施保证软件源代码和制品的安全性；
 - 2) 宜要求供方对其研发、测试工具提供可操作性的安全替代方案，在断供、停服等情况下不影响开发、测试工作。

5.2.2.2 开源组件安全

开源组件安全对需方要求如下：

- a) 数字政府宜建立统一的可信开源组件库，并要求供方通过统一可信开源组件库下载开源组件；
- b) 应要求供方承诺所使用的开源软件和第三方组件不存在已公开的中高危漏洞，或者对于存在已公开中高危漏洞未修复的情况，但经过评估后存在补救措施的，提供相应的安全分析报告。

5.2.2.3 开发集成过程监理

涉及软件开发的数字政府开发与集成服务项目，应聘请第三方监理对软件开发过程文档、测试文档等进行定期安全监督检查。

5.2.3 服务结束安全要求

5.2.3.1 系统安全交付

系统安全交付对需方要求如下：

- a) 涉及软件开发的数字政府开发与集成服务项目，应建立安全的通道和机制接收供方提交的制品、源代码、软件物料清单、密钥、许可证等；
- b) 涉及软件开发的数字政府开发与集成服务项目，在软件开发阶段和软件开发完成后，需方应组织开展安全测试验证或者要求供方提供安全测试报告，安全测试验证内容应覆盖安全需求，对软件的代码、开源组件、API接口、业务逻辑等进行安全性测试，采用白盒测试、灰盒测试、黑盒测试等方法进行测试；
- c) 试运行阶段不接入生产环境实际使用的数字政府开发与集成服务项目，测试及试运行数据使用真实敏感信息、重要数据时，应进行必要的脱敏处理；
- d) 在数字政府开发与集成服务项目结束离场时，应确保已获得完整的软硬件资产及运行文档，包括但不限于：
 - 1) 合同约定的软硬件资产、软件开发生命期工程文档、集成配置清单、集成环境文档和相关系统与设备的账号权限；
 - 2) 软件安全基线、培训资料、运维手册和安全事件响应手册等；
 - 3) 硬件产品说明文档等相关文档资料；
 - 4) 产品安全测试报告、查验报告等相关文档资料。
- e) 应确认数字政府开发与集成服务项目交付软硬件的商业授权、开源许可符合采购合同或协议约定。

5.2.3.2 软件资产管理

涉及软件开发的数字政府开发与集成服务项目，应对软件资产及版本发布环境进行安全管控，软件资产管理对需方要求如下：

- a) 应建立成品软件资产库以接受供方提交的各种软件资产，软件资产库至少包括源代码库、开源组件库、软件制品库；
- b) 应对软件制品进行恶意代码、脚本、病毒蠕虫木马等扫描，对软件制品进行完整性检查，防止被植入恶意代码或者恶意篡改；
- c) 应对软件的发布环境进行安全管控和安全加固，防止软件发布环境被攻击而导致发布的软件被植入恶意代码或者恶意篡改。

5.2.3.3 程序代码安全

涉及软件开发的数字政府开发与集成服务项目，应采取措施确保程序代码的安全，程序代码安全对需方要求如下：

- a) 应组织开展代码评审、代码检测、代码自查等审计工作或者要求供方提供代码安全审计报告，识别并修复源代码安全漏洞；
- b) 应保护程序代码自身的安全性，采用多因子认证、密码技术、数字水印、虚拟桌面等方式保护被访问的程序代码，对访问者进行身份鉴权、权限设定等技术措施进行管控，并记录、审计所有的访问行为；
- c) 应确保不将软件产品的全部或部分代码泄露到授权以外的范围，并在互联网持续监测软件代码的泄露情况。

5.2.3.4 软件成分分析

涉及软件开发的数字政府开发与集成服务项目，应组织开展软件成分分析，管理构建软件构成图谱，软件成分分析对需方要求如下：

- a) 应组织开展软件成分分析或者要求供方提供软件成分分析报告，形成符合相关国家标准要求的软件物料清单；
- b) 应要求供方构建软件构成图谱，充分掌握软件中包含的开源组件和开源代码，以及它们之间的依赖关系，软件构成图谱至少能追溯至其第一级供应商，对于重要组织或场景，例如关键信息基础设施运营者等，需方可根据需求要求软件构成图谱追溯的供应商层级，且关键信息基础设施运营者需符合《中华人民共和国网络安全法》等法律法规对关键信息基础设施运营者的要求。

5.2.3.5 软件安全发布

涉及软件开发的数字政府开发与集成服务项目，应采取措施对软件发布进行安全管控，软件安全发布对需方要求如下：

- a) 应按照最小化原则进行软件的安装部署，只开放软件运行所必需的端口和服务；
- b) 应通过受控的安全渠道发布软件；
- c) 应对重要或核心业务场景的软件进行安全加固，宜配置应用安全自我防护技术手段。

5.2.3.6 离场资源回收

离场资源回收对需方要求如下：

- a) 涉及驻场开发和集成的数字政府开发与集成服务项目，应回收测试资源（包括接口测试文档、测试数据、测试设备等）、测试环境访问权限、网络访问权限及其他权限等；
- b) 涉及软件开发的数字政府开发与集成服务项目，应建立软件产品废止处理规范流程，包括软件停用、卸载和数据清除或迁移等内容，并依据废止处理规范流程对停止使用的软件进行废止处理。

5.3 运营与维护服务供应链扩展安全要求

5.3.1 服务入场安全要求

5.3.1.1 业务连续性保障

应依据数字政府运营与维护服务项目的业务对象重要程度，制定业务连续性保障计划，业务连续性保障对需方要求如下：

- a) 内容包含恢复点目标（RPO）、恢复时间目标（RTO）和最小恢复资源配置等；
- b) 规定应急执行团队的职责与人员；
- c) 确定数据的冗余防护级别，在业务连续保障性计划制定数据安全保障相关内容；
- d) 考虑供需双方的人力、设备、技术和财务等方面，确保服务连续性保障计划的执行有足够的资源；
- e) 明确应急联络渠道，确保在事件发生时能及时通报情况和获得支持。

5.3.2 服务实施安全要求

5.3.2.1 服务实施环境安全

服务实施环境安全对需方要求如下：

- a) 数字政府运营与维护服务项目的关键运维终端应关闭或拆除软盘驱动、光盘驱动、多余网口等非必需接口，确需保留的应通过相关的技术措施实施严格的安全控制和管理；
- b) 涉及驻场业务运营服务工作的数字政府运营与维护服务项目，应加强对业务运营工作环境及访问控制的安全管控：
 - 1) 应提供独立、安全的运营工作环境和网络环境；
 - 2) 应根据业务需求进行最小访问控制权限分配，保障工作环境的安全性；
 - 3) 应在工作终端安装网络版杀毒软件进行恶意代码防护；
 - 4) 应在工作终端安装访问控制系统、终端安全管理软件，关闭或拆除软盘驱动、光盘驱动、多余网口等非必需接口，管理 USB 外设和网络使用安全；
 - 5) 应每季度至少进行一次工作终端安全检查，并记录检查结果。
- c) 涉及非驻场业务运营服务工作的数字政府运营与维护服务项目，应要求供方加强对业务运营工作环境及访问控制的安全管控：
 - 1) 应指定业务运营服务首选的信息系统、设备、网络环境和工作地点等；
 - 2) 应对供方运营服务工作环境、网络环境和工作终端进行实地检查，以确保满足服务基本安全要求和过程安全要求；
 - 3) 对具有运营服务集中度的供方，可采取联合、委托等形式进行检查。
- d) 涉及硬件设备运维的数字政府运营与维护服务项目，应建立硬件组件、设备的备件库，指定专门的部门或人员对备件库的状态、出入库进行管理和定期维护，确保备件供应的可持续性和安全性。

5.3.2.2 业务数据安全

业务数据安全对需方要求如下：

- a) 应依据数字政府运营与维护服务项目的业务连续性保障计划保障业务和数据的可用性；
- b) 涉及数据增删改等高风险操作实施的数字政府数据运营与维护服务项目，应组织对供方提交的操作申请进行评审，并出具实施授权书；
- c) 涉及数据分析（日志分析）的数字政府数据运营服务项目，应配置日志采集安全策略，对日志中的敏感信息通过混淆、替换等措施进行脱敏处理；
- d) 涉及硬件设备运维的数字政府运营与维护服务项目，含有存储介质的设备带出工作环境时，应对其中存储的敏感信息和重要数据加密，并经过审批才能带离；
- e) 授权数字政府业务运营服务项目供方进行数据发布的，应在发布前核查数据中是否含有非公开信息；
- f) 涉及数据库运维及数据治理的数字政府运营与维护服务项目，应制定数据的备份和恢复策略，并定期验证备份策略的有效性和备份数据的完整性。

5.3.2.3 应用程序接口安全运维

涉及应用程序安全运维的数字政府运营与维护服务项目，应构建应用程序接口以提供跨部门的政务数据共享交换服务，并对应用程序接口进行安全管控，应用程序接口安全运维对需方要求如下：

- a) 应采取身份认证、访问授权、流量控制和监控分析等技术措施管控应用程序接口的安全；
- b) 应建立应用程序接口运维监测平台，或将应用程序接口运维监测纳入统一监测平台并重点监测；

- c) 应定期对应用程序接口进行安全巡检，安全巡检内容既包括应对应用程序接口进行源代码安全审计、渗透测试等技术检查还包括对使用方应用程序接口安全集成情况进行检查。

5.3.2.4 桌面及外围设备安全运维

涉及桌面及外围设备安全运维的数字政府运营与维护服务项目，应采取措施对桌面及外围设备运行维护过程中可能产生的安全风险进行预防控制，桌面及外围设备安全运维对需方要求如下：

- a) 应构建可靠的运维机制和使用安全可控的工具，保障运营与维护服务的设备安全、信息数据安全和人身安全等；
- b) 应建立桌面及外围设备维护场所准入制度、维护工具使用要求以及拆卸和携带设备进出维护场所的有关规定。

5.3.2.5 业务连续性评估

业务连续性评估对需方要求如下：

- a) 应依据数字政府运营与维护服务项目的业务连续性保障计划，定期组织验证测试业务的可用性，保障重要业务的连续性；
- b) 应根据验证测试记录和报告，进一步完善数字政府运营与维护服务项目的业务连续性保障计划。

5.4 基础设施服务供应链扩展安全要求

5.4.1 服务规划安全要求

5.4.1.1 服务供应商选择

涉及云计算的数字政府基础设施服务项目，应确保服务供应商的能力满足相关要求，并履行自身的安全管理责任，服务供应商选择对需方要求如下：

- a) 服务对象的安全保护等级为二级及以上的，应选择至少达到GB/T 31168—2023中所规定的增强安全能力的云计算服务；
- b) 采用云计算服务期间，数字政府的安全管理责任不变。安全管理责任不宜随服务外包而转移，无论数据和业务是位于单位内部信息系统还是云服务商的云计算平台上，数字政府都是安全的最终责任人。

5.4.1.2 迁移容灾安全

迁移容灾安全对需方要求如下：

- a) 应制定迁移规范和预案，包括迁移计划、数据备份方案、业务割接方案、主备切换方案等，明确相关方的安全责任和义务，对迁移过程的安全风险进行持续监控，确保在安全的前提下进行迁移；
- b) 应制定灾难恢复计划，明确处理安全事件、重大灾难事件等的流程、措施、人员等。

5.4.2 服务实施安全要求

5.4.2.1 基础环境安全

基础环境安全对需方要求如下：

- a) 涉及物理机房建设的数字政府基础设施服务项目，应按约定要求提供安全的物理环境，确保物理位置、访问控制、电力供应、电磁防护、防火防雷等安全要求符合GB/T 22239—2019相关规定；
- b) 涉及云计算、区块链等提供数据存储的数字政府基础设施服务项目，计算资源池及数据存储资源池应位于本市党政机关及其直属单位自有数据中心、专门租赁数据中心等场所。

5.4.2.2 云服务安全能力

云服务安全能力对需方要求如下：

- a) 涉及云计算的数字政府基础设施服务项目，应采取措施保障云计算平台及应用能力的安全性，包括但不限于：
 - 1) 应根据 GB/T 32400—2015 中所定义的应用能力类型、平台能力类型和基础设施能力类型等三类不同的云能力类型来确定云服务商与数字政府对云计算平台的安全控制范围；
 - 2) 宜根据 GB/T 32400—2015 中所规定的要求，在应用能力类型下，应用软件层的安全措施宜由数字政府和云服务商分担，其他安全措施宜由云服务商实施；在平台能力类型下，软件平台层的安全措施宜由数字政府和云服务商分担，数字政府宜负责自己开发和部署的应用及其运行环境的安全，其他安全措施宜由云服务商实施；在基础设施能力类型下，虚拟化计算资源层的安全措施宜由客户和云服务商分担，客户宜负责自己部署的操作系统、运行环境和应用的安全，云服务商宜负责虚拟机监视器及底层资源的安全；
 - 3) 在所有云能力类型下，数字政府均不应要求所有安全措施全部由云服务商实施。
- b) 应建立基础软件供应链安全风险评估机制，并定期开展风险评估，及时发现潜在安全风险，包括安全漏洞、数据泄露、服务中断、恶意软件植入等，降低软件遭受攻击的可能性；
- c) 应建立云服务数据出境安全审核机制，对出境数据进行事前评估和持续监督，防范数据出境安全风险，保障数据依法有序自由流动。

5.5 生成式人工智能服务供应链扩展安全要求

5.5.1 服务入场安全要求

5.5.1.1 生成式人工智能服务供应商选择

生成式人工智能服务供应商选择对需方要求如下：

- a) 如数字政府提供的生成式人工智能服务具有舆论属性或者社会动员能力，应按照《生成式人工智能服务管理暂行办法》等国家有关规定选择经过备案的算法；
- b) 数字政府生成式人工智能服务项目应在相应程序中向主管部门如实上报生成式人工智能服务数据应用合规的制度建设、落实情况与自评估结果。

5.5.2 服务实施安全要求

5.5.2.1 使用者尽责义务的告知

使用者尽责义务的告知对需方要求如下：

- a) 应对注册使用数字政府生成式人工智能服务的使用者明确告知如下事项：
 - 1) 生成式人工智能服务的基本特点与可能风险；

- 2) 使用者使用生成式人工智能服务的基本规范,包括不得利用生成式人工智能服务特性,有意识地获取违反法律法规、违反社会公德或伦理道德的内容;
 - 3) 使用者负有审慎、尽责使用生成式人工智能服务的义务,在生成内容含有违反法律法规、违反社会公德或伦理道德的内容时,不应将此生成内容对外传播。
- b) 对于生成内容在特定行业的应用,尤其是对内容准确性有较高要求的如法律、医疗等领域,应向数字政府生成式人工智能服务使用者重点提示风险。

5.5.2.2 生成内容安全

生成内容安全对需方要求如下:

- a) 数字政府生成式人工智能服务提供者应建立生成内容审核机制,通过技术手段或人工审核的方式,对生成式人工智能生成的内容在对外提供前进行检测,识别并过滤其中的个人隐私信息、虚假有害信息、违法违规信息等不宜对外提供的内容;
- b) 应建立使用者对生成内容提出异议的投诉和举报机制,及时处理数字政府生成式人工智能服务使用者对生成内容合法合规性的异议。

5.5.2.3 第三方模型安全

应每年组织不少于1次或者出现重大变更时对数字政府生成式人工智能服务第三方组件、基础模型、基础硬件、算力及服务供应商的安全风险评估,并采取措施控制发现的风险。

5.6 其他服务供应链扩展安全要求

5.6.1 服务入场安全要求

5.6.1.1 供应商资质

涉及第三方测评服务的数字政府信息技术服务项目,应选择具备相关资质的供应商。

5.6.2 服务实施安全要求

5.6.2.1 业务风险控制

业务风险控制对需方要求如下:

- a) 涉及等保测评、密码测评的数字政府信息技术服务项目,应在测评前与测评机构进行充分沟通,再次确定测评范围并出具授权书;
- b) 涉及安全漏洞扫描、渗透测试和攻防演练等可能对需方业务和数据造成影响的数字政府信息技术服务项目,应要求供方提交实施方案和风险控制措施,并组织评审、出具实施授权书;
- c) 涉及安全漏洞扫描、渗透测试和攻防演练等的数字政府信息技术服务,应实时监测实施范围内的安全预警信息。

6 供方安全要求

6.1 通用安全要求

6.1.1 基本安全要求

6.1.1.1 组织机构

组织机构对供方要求如下：

- a) 应明确指定项目组负责数字政府信息技术服务项目和次级供应链的安全管理工作，并制度化；
- b) 应明确数字政府信息技术服务项目和次级供应链安全管理责任部门的相关工作职责，相关工作职责内容包括服务项目和次级供应链安全管理要求的制定和维护、服务项目和次级供应链安全技术防护措施的计划与落实、服务项目和次级供应链资源的提供和管理、服务项目和次级供应链相关人员的组织和安全教育培训等。

6.1.1.2 安全管理制度

安全管理制度对供方要求如下：

- a) 应制定文档化的数字政府信息技术服务项目和次级供应链安全管理相关内容，内容包括次级供应商安全管理、服务供应活动安全管理、服务供应参与人员安全管理及知识产权管理等内容；
- b) 应每年组织不少于1次对数字政府信息技术服务项目和次级供应链安全管理相关内容进行评审，并依据评审结果进行必要的更新；
- c) 应每年组织不少于1次对数字政府信息技术和次级供应链安全管理相关内容进行宣贯和培训。

6.1.1.3 次级供应商清单

次级供应商清单对供方要求如下：

- a) 应建立次级供应商管理清单，清单记录内容应包括次级供应商基本信息、联系人、联系方式、专业资质、关联需方项目等信息；
- b) 应每年对数字政府信息技术服务次级供应商开展不少于1次的安全评审，对次级供应商安全资质存续、股权结构变化、业务经营状况等信息进行审查，更新次级供应商管理清单信息；
- c) 应选择符合以下条件的组织作为次级供应商：
 - 1) 不存在较大的业务经营风险，保证服务持续不会中断；
 - 2) 在历史合同履行中未发生过较大的安全事件。
- d) 应将需方的安全要求准确传递给项目涉及的次级供应商，应与次级供应商通过签订安全保密协议和安全责任书等方式明确安全和保密义务与责任。

6.1.1.4 供应链安全合作和沟通

应加强与数字政府信息技术服务需方、其他供应商及次级供应商之间的合作与沟通，共同协作处理数字政府信息技术服务供应链安全相关问题。

6.1.1.5 供应链产权管理

供应链产权管理对供方要求如下：

- a) 应承诺不侵犯数字政府信息技术服务需方的知识产权和不引入第三方知识产权纠纷；
- b) 数字政府信息技术服务项目中使用的设备和工具等商业产品应拥有合法使用授权，并充分考虑其安全性；
- c) 应明确了解数字政府信息技术服务项目涉及开源组件的开源许可协议并遵守使用，保证服务项目中不存在开源许可合规风险。

6.1.1.6 供应链安全应急预案

数字政府信息技术服务供应中应根据需方要求积极配合参与安全应急预案培训和演练。

6.1.1.7 供应链安全事件管理

供应链安全事件管理对供方要求如下：

- a) 应制定数字政府信息技术服务项目及次级供应链安全事件处置和报告管理流程，及时向需方通报交付产品的安全漏洞及可能影响需方的网络安全事件，并提供相应的解决方案；
- b) 数字政府信息技术服务供应中应根据需方要求积极配合参与安全事件应急处置。

6.1.1.8 供应保障协同

供应保障协同对供方要求如下：

- a) 数字政府信息技术服务供应中涉及重大活动保障时，应根据需方要求设立专门的安全保障小组，协助开展安全保障工作；
- b) 应积极配合需方开展数字政府信息技术服务供应链安全检查，并根据安全检查结果进行安全整改，确实无法整改的应记录在案并采取其他弥补措施。

6.1.2 服务规划安全要求

6.1.2.1 安全合规审查

安全合规审查对供方要求如下：

- a) 对拟参与的数字政府信息技术服务或产品影响或可能影响国家安全的，应按有关规定配合需方对服务或产品开展网络安全审查；
- b) 对拟参与的数字政府信息技术服务或产品涉及密码应用的，应按有关规定配合需方制定密码应用方案、方案安全性评估等工作。

6.1.3 服务入场安全要求

6.1.3.1 实施方案准备

实施方案准备对供方要求如下：

- a) 应向需方提交数字政府信息技术服务项目安全管理员信息、项目安全管理方案和项目安全管理计划，内容应包括切实可行的服务项目实施安全、数据安全保密、个人信息保护、内部人员安全培训计划等；
- b) 存在次级供应商的数字政府信息技术服务项目，应开展次级供应商报备及安全管理，安全管理内容包括但不限于：
 - 1) 安全管理方案和安全管理计划应包含对次级供应商的安全管理内容；
 - 2) 应向需方报备相关联的次级供应商清单信息。

6.1.3.2 供应商人员安全

供应商人员安全对供方要求如下：

- a) 应为数字政府信息技术服务项目指派至少1名安全管理人员，具体负责该项目的日常安全管理工作，指派的安全管理人员应达到GB/T 42446—2023中所规定的网络安全管理类人员相应能力水平要求；
- b) 参与数字政府信息技术服务项目的安全架构师、安全工程师等人员的能力应达到GB/T 42446—2023中所规定的与服务类型相适应的网络安全建设、网络安全运营、网络安全审计和评估等人员的能力水平要求；
- c) 应向需方提供数字政府信息技术服务项目参与人员、角色清单及个人简历，个人简历信息应包含学历、项目经验、资质证书等内容，如有需要还应提供国籍证明文件。

6.1.3.3 设备入场控制

设备入场控制对供方要求如下：

- a) 应向需方提交数字政府信息技术服务项目实施所需且属于供方所有的设备和工具清单，内容应包括设备工具名称、软硬件类型、商业授权许可、具体用途和安全可靠性证明等；
- b) 数字政府信息技术服务项目实施所需且属于供方所有的设备和工具应具备安全日志记录和审计功能；
- c) 数字政府信息技术服务项目实施所需且属于供方所有的设备和工具操作结束后应能自动或手动删除工具缓存的敏感信息、个人信息和重要数据。

6.1.4 服务实施安全要求

6.1.4.1 供应过程访问控制

供应过程访问控制对供方要求如下：

- a) 应使用安全可控的设备和工具开展数字政府信息技术服务项目实施活动。服务项目实施确需备案之外的设备工具时，应向需方申请备案，经安全检查和授权许可后方可入场使用；
- b) 应开展数字政府信息技术服务项目实施工具使用培训，避免操作不当对需求方系统、业务和数据造成影响；
- c) 应确保数字政府信息技术服务项目实施对象和范围仅为合同约定或需方再次授权的对象和范围；
- d) 因数字政府信息技术服务项目实施需要访问物理受控区域的，应事先向需方提出书面申请，获得批准后由专人陪同访问；
- e) 应在数字政府信息技术服务项目实施过程中仅使用需方提供或许可的方式连接和访问需方内部网络资源，不应私建手机热点和移动WIFI等网络接入点接入需方内部网络。

6.1.4.2 供应过程数据安全

供应过程数据安全对供方要求如下：

- a) 应确保需方数据和个人隐私信息在数字政府信息技术服务项目实施全过程不被泄露；
- b) 应采用密码技术保证数字政府信息技术服务项目实施非需方网络环境数据传输、非需方设备和介质数据存储过程中需方敏感信息、重要数据的保密性和安全性；
- c) 应通过加密存储、访问控制等技术措施保护数字政府信息技术服务项目实施过程中产生的临时数据备份文件和数据缓存文件，并在相关实施完成后及时清除临时数据备份文件和数据缓存文件；

- d) 应采用多因子认证、密码技术等技术措施，保障数字政府信息技术服务项目所使用密钥和证书的安全；
- e) 应定期检查数字政府信息技术服务项目实施相关的数据备份和恢复策略，并验证备份数据的有效性和完整性；
- f) 不应将数字政府信息技术服务项目实施中涉及的需方数据（包括系统源代码、配置信息、网络拓扑等），上传至供方组织、第三方组织和个人的外部存储等；
- g) 未经授权许可不应下载数字政府信息技术服务需方敏感信息和重要数据至工作终端本地存储；
- h) 未经授权许可不应访问和使用数字政府信息技术服务项目实施以外的需方相关数据；
- i) 未经授权许可不应向第三方提供数字政府信息技术服务需方相关数据，或将需方相关数据用于服务项目实施以外的目的；
- j) 未经授权许可不应将数字政府信息技术服务项目的测试、仿真等环境部署在本市党政机关及其直属单位自有数据中心、专门租赁数据中心以外的场所；
- k) 应仅通过数字政府信息技术服务需方提供或许可的方式（如内部邮件系统、文件摆渡系统等）进行文件发送，不应使用未经授权许可的移动存储介质（如U盘、移动硬盘、手机、光盘等）进行文件拷贝；
- l) 未经授权许可不应将数字政府信息技术服务项目实施使用的存储介质及具有数据存储功能的设备带出服务项目实施环境；
- m) 数字政府信息技术服务供应过程涉及的存储介质和存储设备应建立目录清单，对各类存储介质和存储设备的存放和使用进行管控。实行存储环境专人管理，并根据存储介质和存储设备的目录清单定期盘点；
- n) 应对数字政府信息技术服务供应过程涉及的存储介质和存储设备的领取、使用和归还等进行登记，确保存储介质和存储设备的状态可追踪；
- o) 涉及存储介质二次分配使用的数字政府信息技术服务项目，存储介质分配前应进行完全清除或被安全覆盖，确保该介质上的敏感信息、重要数据和授权软件无法被恢复重用。

6.1.4.3 供应过程安全监测

供应过程安全监测对供方要求如下：

- a) 在数字政府信息技术服务项目实施过程中发现与服务相关的网络安全风险或事件时，应及时向需方报告并积极配合进行风险控制和应急响应；
- b) 应向数字政府信息技术服务项目需方报告的风险或事件，应报告的风险或事件包括但不限于：
 - 1) 供方自身或次级供应商发生影响服务连续性的网络安全风险或事件；
 - 2) 发现服务对象存在安全漏洞、违反开源协议、违反数据隐私规定等；
 - 3) 发现服务对象在运行中的网络安全风险或事件。
- c) 应对数字政府信息技术服务项目实施所使用设备、工具及其组件的安全漏洞和其他可能存在的已知安全漏洞进行监测。发现漏洞时，应进行充分测试评估，并及时修补漏洞。

6.1.4.4 供应过程检查评估

供应过程检查评估对供方要求如下：

- a) 应每季度组织不少于1次对数字政府信息技术服务项目实施工具、环境、网络和终端的安全自查工作，及时采取措施控制发现的安全风险；

- b) 应每季度组织不少于1次对数字政府信息技术服务项目实施过程的安全自查工作，安全自查内容应包括需方安全管理遵守、项目安全管理方案执行、项目安全风险控制、次级供应商安全管理等。

6.1.4.5 供应过程变更安全

供应过程变更安全对供方要求如下：

- a) 数字政府信息技术服务项目实施过程发生供应物、服务人员、软硬件升级及参数配置改动等变更时，变更方应提出变更申请，变更申请应包括变更内容、变更时间、变更风险分析及应对措施等内容；
- b) 应在变更申请获得数字政府信息技术服务项目需方审批授权后，方可执行变更实施；
- c) 数字政府信息技术服务项目供应物变更的，应保证替换供应物的功能和安全满足服务项目要求。应采用安全可控的渠道交付，并提交相关的安全性、完整性检测报告；
- d) 数字政府信息技术服务项目参与人员变更的，应保证替换人员的资质和能力符合服务项目需求；
- e) 数字政府信息技术服务项目配置变更、软件升级、固件升级、漏洞补丁安装的，应在测试环境进行测试确认无异常，取得需方授权后进行生产环境变更、升级、安装操作。

6.1.4.6 第三方软件安全

第三方软件安全对供方要求如下：

- a) 在数字政府信息技术服务项目实施中使用第三方软件时，如中间件、数据库、容器镜像、操作系统等，应主动管理第三方软件安全，保证不因使用有缺陷的软件而对需方的网络、系统或数据造成安全风险；
- b) 在数字政府信息技术服务项目实施中将第三方软件集成于服务对象时，应对软件进行安全测试，确保不存在恶意代码、后门和隐蔽信道；
- c) 数字政府信息技术服务项目实施不得使用包含中高危漏洞的软件，必须使用时应向需方提交报告说明使用必要性和漏洞解决方案，并应获得需方确认；
- d) 对已经集成于数字政府信息技术服务项目需方服务对象中的第三方软件，服务期和维保期内该软件出现安全漏洞等风险时，应及时通知需方，并采取措施控制风险；
- e) 应生成并定期维护数字政府信息技术服务项目中的第三方软件清单，清单内容包括软件名称、版本、制造商、IP地址、责任人等；
- f) 应通过自动化方式对数字政府信息技术服务项目中的第三方软件进行安装、更新和删除。

6.1.5 服务结束安全要求

6.1.5.1 服务结束方案

服务结束方案对供方要求如下：

- a) 应制定数字政府信息技术服务结束离场计划，在确保需方现有业务正常运行的前提下有序开展离场工作；
- b) 数字政府信息技术服务结束离场计划应包括服务完整移交、需方资源交回、供方人员保密和供方设备数据清除等内容。

6.1.5.2 服务资料移交

服务资料移交对供方要求如下：

- a) 应完整移交数字政府信息技术服务项目约定交付物，包括资产清单、文档资料、知识产权成果、知识培训以及关联次级供应商信息等；
- b) 应提供数字政府信息技术服务项目交付材料的真实性证明文件，包括安全漏洞验证截图及POC、引用数据来源出处等。

6.1.5.3 离场资源回收

应交回数字政府信息技术服务项目需方分配的网络、系统、设备等用户账号及对应密码。

6.1.5.4 人员离场管理

人员离场管理对供方要求如下：

- a) 应交回数字政府信息技术服务项目需方分配的人员物理身份标识，包括供应商专用的工卡或铭牌等；
- b) 应承诺不私自预留数字政府信息技术服务项目需方网络及系统用户账号、不预留程序后门、不植入恶意代码等。

6.1.5.5 设备离场管理

设备离场管理对供方要求如下：

- a) 应交回数字政府信息技术服务项目需方分配的设备SN、设备铭牌、网络IP和标识等；
- b) 应将数字政府信息技术服务项目供方测试设备和试用设备下线，并配合清除或迁移需方相关数据；
- c) 应配合需方清除数字政府信息技术服务项目所使用供方设备存储的需方相关数据。

6.2 开发与集成服务供应链扩展安全要求

6.2.1 服务规划安全要求

6.2.1.1 项目安全需求

涉及软件开发的数字政府开发与集成服务项目，应配合开展项目需求分析及软件安全需求文档评审，项目安全需求对供方要求如下：

- a) 应配合需方开展安全需求分析，在软件需求规格说明等需求文档中明确记录或者单独编制形成软件安全需求文档；
- b) 应组织专家进行安全需求评审，并持续维护安全需求，在需求变更等情况时重新评审安全需求。

6.2.2 服务实施安全要求

6.2.2.1 系统安全设计

涉及软件开发的数字政府开发与集成服务项目，应开展软件安全性设计和威胁建模，系统安全设计对供方要求如下：

- a) 应进行软件安全设计，选型和设计应符合安全需求的技术架构，形成安全设计文档并组织评审；
- b) 应开展威胁建模，在概要设计文档或者详细设计文档中明确记录有关安全的内容；
- c) 应组织安全设计评审，逐一确认软件设计是否符合安全需求；

- d) 应持续维护安全设计，在重构、更改业务逻辑等情况时重新开展安全设计威胁建模和评审。

6.2.2.2 开发集成测试环境

开发集成测试环境对供方要求如下：

- a) 数字政府开发与集成服务项目应保证开发集成测试环境的相对独立，与生产环境的物理隔离；
- b) 涉及软件开发的数字政府开发与集成服务项目，应采取措施对软件开发集成测试环境、开发过程进行安全管控，包括但不限于：
 - 1) 应加强软件开发集成测试环境的安全管控，采取访问控制、安全扫描、配置核查、安全加固、安全审计等措施保证数字政府开发与集成服务项目在开发编码、CI/CD 流水线、编译和测试环境的安全性，并定期检查和记录；
 - 2) 应在开发过程采取代码版本控制、安全开发流程管理、安全检测等措施保证软件源代码和制品的安全性；
 - 3) 应对研发、测试工具提供可操作性的安全替代方案，在断供、停服等情况下不影响开发、测试工作。

6.2.2.3 软件资产库

涉及软件开发的数字政府开发与集成服务项目，应对软件源代码、开源组件及软件制品进行安全管控，软件资产库对供方要求如下：

- a) 应在开发测试环境中建立软件资产库，软件资产库至少包括源代码库、开源组件库、软件制品库；
- b) 应对软件资产库采取严格的安全措施保护软件资产的安全，如具备防止捆绑恶意代码、下载劫持、网络劫持、升级劫持的能力。

6.2.2.4 开发集成数据安全

开发集成数据安全对供方要求如下：

- a) 涉及软件开发的数字政府开发与集成服务项目，应对源代码、证书及密钥安全进行管控，在开发者终端环境和代码仓库采取访问控制、权限控制、防泄露等技术措施，防止源代码、证书及密钥被非法访问和泄露；
- b) 因开发需要传入数字政府开发与集成服务项目的外部数据的，应当满足以下安全要求：
 - 1) 承担项目实施期内外部数据的安全管理责任；
 - 2) 只能存储于项目所属存储资源内；
 - 3) 与项目中的内部数据有明确的标识区别；
 - 4) 仅供本服务项目开发和测试使用。
- c) 数字政府开发与集成服务项目涉及生产环境业务系统集成的，应事先进行数据备份，并制定相关的应急预案；
- d) 涉及软件开发的数字政府开发与集成服务项目，应对互联网侧源代码及其相关文档泄露进行监测，防范源代码泄露导致的相关安全风险。

6.2.2.5 开源组件安全

开源组件安全对供方要求如下：

- a) 应从可信的开源组件库下载开源组件和开源代码并在项目组内部建立本地软件资产库，例如用Maven管理本地库，并记录数字政府开发与集成服务项目组件来源形成组件清单；
- b) 应主动管理第三方开源组件安全，建立开源及第三方组件的入库和使用审批机制，对数字政府开发与集成服务项目的组件进行安全测试，确保使用的开源软件和第三方组件不存在已公开漏洞未修复的情况，或者对于存在已公开漏洞未修复的情况，但经过评估后存在补救措施的，提供相应的安全分析报告；
- c) 不得使用包含中高危漏洞、违反许可证协议及超过5年无更新维护的第三方开源组件，必须使用时应向数字政府开发与集成服务项目需方提交报告说明使用必要性和漏洞解决方案，并获得需方同意；
- d) 数字政府开发与集成服务项目应制定组件使用管控机制，统一管理编码过程中使用的组件版本；
- e) 应以软件物料清单等形式说明数字政府开发与集成服务项目软件中所集成的第三方组件、调用外部的服务接口以及对外开放的服务接口等信息，信息内容包括组件名称、组件版本、接口名称、接口参数、功能描述等；
- f) 第三方组件发生安全漏洞或许可证变更等风险时，应及时通知数字政府开发与集成服务项目需方，并采取措施控制风险。

6.2.2.6 安全开发编码

安全开发编码对供方要求如下：

- a) 涉及软件开发的数字政府开发与集成服务项目，应进行软件安全自测，进行源代码审计和安全检测、组件安全检测、人工渗透测试、个人信息安全影响评估，深层次挖掘、发现、修复和记录安全缺陷和漏洞；
- b) 涉及软件开发的数字政府开发与集成服务项目，应建立安全编码规范，针对不同的编程语言，制定相对应的安全编码要求，软件安全编码要求和源代码安全检查应符合相关国家标准的要求，主要包括：
 - 1) C/C++语言代码审计应符合 GB/T 34943—2017 中所规定的相关要求；
 - 2) Java 语言代码审计应符合 GB/T 34944—2017 中所规定的相关要求；
 - 3) 其他语言代码审计应符合 GB/T 39412—2020 中所规定的相关要求。
- c) 涉及软件开发的数字政府开发与集成服务项目，应建立软件缺陷与漏洞修复闭环管理机制，对软件缺陷与漏洞修复进行管理，软件漏洞修复和管理应符合GB/T 28458—2020、GB/T 30276—2020、GB/T 30279—2020等相关要求；
- d) 涉及软件开发的数字政府开发与集成服务项目，宜采用生成式人工智能服务等先进技术提高安全开发编码能力，包括自动代码补齐、漏洞成因分析、代码漏洞修复等。

6.2.2.7 安全测试验证

涉及软件开发的数字政府开发与集成服务项目，应在软件开发阶段和软件开发完成后，开展安全测试验证，对发现的安全漏洞及时进行修复，安全测试验证对供方要求如下：

- a) 应对软件的代码、开源组件、API接口、业务逻辑等进行安全性测试，采用白盒测试、灰盒测试、黑盒测试等方法进行测试，安全测试验证应覆盖安全需求；
- b) 应开展代码评审、代码检测、代码走查，识别并修复源代码安全漏洞；
- c) 应开展开源组件安全合规检查，识别并修复开源组件的安全漏洞和开源许可证冲突问题；
- d) 应将发现的安全漏洞收录到内部漏洞库中，记录并跟踪软件安全测试出的问题和修复情况。

6.2.2.8 开发过程审计

涉及软件开发的数字政府开发与集成服务项目，应对开发人员的开发活动开展内部监测和审计。

6.2.3 服务结束安全要求

6.2.3.1 系统安全交付

系统安全交付对供方要求如下：

- a) 应保证交付的系统、设备不使用包含有害程序、安全缺陷或假冒的组件或者产品，符合国家法律法规及数字政府开发与集成服务项目需方提出的安全要求、功能要求及授权要求；
- b) 应承诺数字政府开发与集成服务项目不存在隐蔽接口、可绕过安全机制的功能模块、违规收集和使用需方数据、泄漏需方敏感数据等情况；
- c) 涉及软件开发的数字政府开发与集成服务项目，应保证开发、测试、运行等不同环境中代码的一致性；
- d) 涉及采购现货软件和硬件产品的数字政府开发与集成服务项目，应采取以下措施保证交付软硬件产品的安全性和完整性：
 - 1) 应对系统、系统组件及服务实施防篡改保护措施；
 - 2) 应检查集成产品的完整性和安全性；
 - 3) 应提交产品查验报告。
- e) 涉及移动应用软件采购的数字政府开发与集成服务项目，应采取以下措施保证交付移动应用软件的安全性和完整性：
 - 1) 应保证移动应用软件由指定开发商开发；
 - 2) 应通过可靠分发渠道、可信证书签名保证安全性和完整性。
- f) 应制定数字政府开发与集成服务项目整体运行所必要的培训计划，编制培训手册、运维手册和安全事件响应手册等，并培训需方相关人员；
- g) 数字政府开发与集成服务项目应建立安全可控的机制和渠道交付约定的软件产品、源代码及版本升级程序等；
- h) 数字政府开发与集成服务项目应制定服务交付清单，并根据清单完整交付软件、源代码、软件物料清单、配置文件、安全基线文件、集成产品、产品配置项列表和相关文档等；
- i) 不应交付数字政府开发与集成服务采购合同或协议约定以外的功能或服务。

6.2.3.2 程序代码安全

涉及软件开发的数字政府开发与集成服务项目，应采取措施确保程序代码的安全，程序代码安全对供方要求如下：

- a) 应确保不将软件产品的全部或部分代码泄露到授权以外的范围，如发现互联网等存在软件产品代码泄露情况应及时报告需方；
- b) 不应在软件产品中设置后门，或利用软件产品的便利条件非法获取用户数据、控制和操纵用户系统和设备；
- c) 不应利用软件产品的依赖性谋取不正当利益；
- d) 不应在未授权情况下对软件产品进行升级或更新换代。

6.2.3.3 软件成分分析

涉及软件开发的数字政府开发与集成服务项目，应开展软件成分分析，构建软件构成图谱，软件成分分析对供方要求如下：

- a) 应提供软件成分分析报告，提供符合相关国家标准要求的软件物料清单，并尽可能修复开源组件的安全漏洞和开源许可证冲突问题，宜选用不含中危以上级别安全漏洞的开源组件和开源代码；
- b) 应构建软件构成图谱，充分掌握软件中包含的开源组件和开源代码，以及它们之间的依赖关系，软件构成图谱至少能追溯至其第一级供应商，直至满足需方要求的软件构成图谱追溯的供应商层级。

6.3 运营与维护服务供应链扩展安全要求

6.3.1 服务入场安全要求

6.3.1.1 业务连续性保障

涉及业务运营的数字政府运营与维护服务项目，应依据运营业务重要程度，确定人员的冗余保障级别，应保证业务的连续性，业务连续性保障对供方要求如下：

- a) 重要程度高的业务运营服务，应确保驻场人员满足冗余保障要求；
- b) 重要程度高的业务运营服务，应确保储备人员满足冗余保障要求。

6.3.2 服务实施安全要求

6.3.2.1 服务实施环境安全

服务实施环境安全对供方要求如下：

- a) 涉及非驻场运营服务工作的数字政府运营与维护服务项目，应提供独立、满足需方要求的运营工作环境，并保障工作环境的安全性，具体措施包括但不限于：
 - 1) 应根据业务需求进行最小访问控制权限分配，保障工作环境的安全性；
 - 2) 应在工作终端安装网络版杀毒软件进行恶意代码防护；
 - 3) 应在工作终端安装访问控制系统、终端安全管理软件，关闭或拆除软盘驱动、光盘驱动、多余网口等非必需接口，管理 USB 外设和网络使用安全；
 - 4) 应限制接入和使用外部设备，因工作需要接入和使用的应进行安全检查；
 - 5) 无线接入网络应开启接入认证功能，并支持采用认证服务器认证或国家密码管理机构批准的密码模块进行认证；
 - 6) 应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备。
- b) 应对数字政府运营与维护服务项目供应过程中的外部设备使用、账号使用进行安全管控，防范违规使用带来的安全风险，具体措施包括但不限于：
 - 1) 未经授权许可不应擅自违规接入外部设备（如 U 盘、U 盾等），防范社会工程攻击和不安全外部设备带来的病毒入侵、木马植入等风险；
 - 2) 应按要求安全使用需方授权的业务平台及账号，防范账号风险误报、账号失窃、数据泄露等风险；
 - 3) 应妥善保管自己的授权账号，不应擅自违规外借、共享自己的账号给他人使用；
 - 4) 需方特权账号持有人应谨慎登录、使用特权账号，不应将特权账号私自转借、共享给他人。

- c) 涉及非驻场运维的数字政府运营与维护服务项目，应使用安全访问通道指导运维操作实施，具体措施包括但不限于：
 - 1) 应按照需方的远程访问要求建立访问通道、配置认证凭据；
 - 2) 不应直接远程访问、操作运维对象，应远程指导现场人员进行运维操作实施。

6.3.2.2 业务数据安全

业务数据安全对供方要求如下：

- a) 应对数字政府运营与维护服务项目实施敏感信息泄露进行监测，监测内容包括但不限于：
 - 1) 关键设施配置信息泄露；
 - 2) 特权账号、密钥和证书泄露；
 - 3) 关键资产及网络拓扑信息泄露。
- b) 涉及需方数据增删改等高风险操作的数字政府运营与维护服务项目，应向需方提交申请获取授权后实施，申请内容包括操作对象、范围、执行动作、操作人员、操作时间、风险及规避措施等。并在操作实施前进行数据备份，确保数据的完整性和可用性；
- c) 数字政府运营与维护服务项目实施过程中发现需方敏感信息、重要数据应脱敏但未被脱敏处理或者脱敏处理不完整的，应及时向需方报告并暂停相关数据处理，待需方数据脱敏处理正常后，再继续相关数据的服务实施；
- d) 涉及数据导出的数字政府运营与维护服务项目，应安全导出、使用需方数据，具体措施包括但不限于：
 - 1) 应告知需方导出数据的用途、使用时长等相关信息；
 - 2) 应仅使用需方许可的方式和设备进行授权数据的导出；
 - 3) 导出数据不应用于授权之外的用途，超过授权时长的数据应及时进行删除销毁；
 - 4) 不应有约定之外的数据共享、导出、委托、公开等行为。
- e) 涉及数据运营和业务运营的数字政府运营与维护服务项目，应采取必要的安全措施保证需方数据的真实性、准确性，具体措施包括但不限于：
 - 1) 对数据进行加密存储；
 - 2) 对数据进行完整性校验；
 - 3) 对数据进行备份；
 - 4) 未经授权许可不应更改、删除、销毁需方原始数据。
- f) 涉及数据治理服务的数字政府运营与维护服务项目，应对服务供应过程中的数据资产进行保护，具体措施包括但不限于：
 - 1) 应在数据分发和发布时对内容进行风险评估和敏感信息检查；
 - 2) 应确保需方数据在存储、传输、处理过程中不会被人为和程序进行篡改。

6.3.2.3 业务运行安全

数字政府运维服务项目应至少每季度进行一次超授权期限、超维保期限运行软件和业务应用排查，对其安全性进行评估分析，及时发现并控制业务运行安全风险。

6.3.2.4 应用系统运维安全

应用系统运维安全对供方要求如下：

- a) 涉及应用系统运维的数字政府运营与维护服务项目，应采取措施保障应用系统的维护安全性，包括但不限于：
 - 1) 应用系统维护应保持系统版本变更的一致性和适应性，建立完整的软件维护、变更记录文档，保存维护修改的历史信息。针对每次维护及故障处理过程，详细地记录维护开始和结束时间、维护操作人、维护的原因、过程和具体的解决方法；
 - 2) 应对安全保护等级三级及以上的应用系统安排专人维护，每个应用系统应至少安排两人共同维护，实现维护人员的备份制度，保障人员的后备保证。
- b) 应制定补丁管理策略，包括补丁的识别、评估、测试和部署流程，建立快速响应流程，确保在确认补丁适用性后，能够迅速部署。

6.3.2.5 桌面及外围设备运维安全

涉及桌面及外围设备运维的数字政府运营与维护服务项目，应采取措施保障服务的可用性与及时性，桌面及外围设备运维安全对供方要求如下：

- a) 供方在进行桌面及外围设备运维时，应充分考虑到用户的工作时间、使用水平和工作性质等因素。在服务交付过程中，供方应为用户提供灵活的服务形式和丰富的服务资讯，帮助用户方便快捷地获取服务或通过自助服务正确使用桌面及外围设备以及处理各类突发事件；
- b) 供方宜完善用户自助服务的机制和工具，供方宜为用户制定桌面及外围设备操作指引和常见故障快速恢复指引，并帮助用户方便地获得操作指引并理解其内容。

6.4 基础设施服务供应链扩展安全要求

6.4.1 服务规划安全要求

6.4.1.1 云服务供应商选择

涉及云计算的数字政府基础设施服务项目，对安全保护等级为二级及以下的信息系统，云服务运营的安全能力应达到GB/T 31168—2023中所规定的增强要求。对安全保护等级为三级及以上的信息系统，云服务运营的安全能力应达到GB/T 31168—2023中所规定的高级要求。

6.4.2 服务实施安全要求

6.4.2.1 基础环境安全

涉及数据中心租赁的数字政府基础设施服务项目，应确保数据中心物理位置、访问控制、电力供应、电磁防护、防火防雷等安全要求应符合GB/T 22239—2019相关规定。

6.4.2.2 第三方镜像安全

数字政府云计算基础设施服务应主动管理操作系统和容器镜像安全，第三方镜像安全对供方要求如下：

- a) 应通过可信渠道获取操作系统和容器镜像，并记录镜像来源形成镜像清单；
- b) 对操作系统和容器镜像进行安全测试；
- c) 应建立自有操作系统和容器镜像库。

6.4.2.3 云服务运营安全

云服务运营安全对供方要求如下：

- a) 数字政府云计算基础设施服务的云服务运营安全应遵循GB/T 31168—2014中的相关要求；
- b) 数字政府云计算基础设施服务的云服务提供者应对其云服务环境中的支撑环境资源进行有效管理，用于支撑云服务的机房基础设施应符合GB/T 2887—2011和GB/T 9361—2011的要求；
- c) 应具备系统负载的监测和控制能力，及时发现和处理潜在的系统过载风险；
- d) 应合理规划云计算基础设施的容量和性能，避免因系统过载导致服务中断或性能下降；
- e) 应具备容灾恢复能力，建立必要的备份设施，确保客户业务可持续；
- f) 应制定容灾恢复预案和应急响应计划，包括对事件的预防、检测、分析、控制、恢复等，确保在供应链中断时能快速恢复服务；
- g) 不宜依据其他国家的法律和司法要求将客户数据及相关信息提供给他国政府及组织，数据出境宜遵循国家相关法律法规的要求。

6.4.2.4 平台隔离安全

平台隔离安全对供方要求如下：

- a) 数字政府云计算基础设施服务应实现资源、网络、物理安全隔离：
 - 1) 不同用户虚拟网络之间的安全隔离；
 - 2) 不同虚拟机之间的资源安全隔离；
 - 3) 虚拟机与物理机之间的安全隔离。
- b) 应支持虚拟机安全隔离，在虚拟机监控器（Hypervisor）层提供虚拟机与物理机之间的安全隔离措施，控制虚拟机之间及虚拟机和物理机之间所有的数据通信；
- c) 应提供资源隔离失败后的告警措施。

6.4.2.5 平台数据安全

平台数据安全对供方要求如下：

- a) 数字政府云计算基础设施服务应采取措施保护云计算平台中数据传输、存储、使用、删除等阶段的安全：
 - 1) 应通过访问鉴权、密码技术等措施，保障云计算平台的数据存储、处理及传输安全；
 - 2) 数据删除操作应确保副本已被完全销毁，不会被恢复导致数据泄露；
 - 3) 应承诺不泄露云计算平台使用者的数据。
- b) 数字政府区块链基础设施服务应采取措施防范违法信息、不良信息上链，同时防范隐私数据泄露：
 - 1) 应使用符合国家标准或行业标准的数字签名算法和数据加密算法等密码技术，保证节点间通信过程中信息的机密性、完整性和真实性，确保信息在存储、传播过程中不被未授权用户读取或恶意修改；
 - 2) 应通过接口等方式规范交易发起账号、交易接收账号、交易杂凑值、数字签名、交易类型和交易时间戳等采集的交易信息；
 - 3) 应使用屏蔽查询等技术手段，对检测出的违法信息、不良信息进行处置，并对处置过程存证；
 - 4) 应通过关键词检测、图像识别、语音识别等技术手段对用户账号信息、上链信息内容进行审核，确保信息内容不包含违法信息、不良信息；
 - 5) 应对账号数据、区块数据、配置数据、证书等不同类型数据进行分类存储、分开管理；

- 6) 应采取技术手段，使链上待销毁用户信息保持不可被检索、访问的状态；
 - 7) 应对用户信息销毁过程存证，包括销毁人员、时间、内容、方式等关键信息；
 - 8) 应确保各节点存储账本数据的一致性；
 - 9) 应通过技术手段实现节点对重复交易的处理。
- c) 应建立严格的配置管理策略，明确基础设施配置的变更、审查、批准和监控流程。

6.4.2.6 平台内容安全监测

平台内容安全监测对供方要求如下：

- a) 应对数字政府区块链基础设施服务供应过程的信息和状态进行监测和记录，主动识别、处置和通报服务供应过程中的违法信息、不良信息、异常节点等安全风险，监测、审计内容包括：
 - 1) 应建立主动巡查等监测机制，发现区块链信息服务中的违法信息、不良信息；
 - 2) 应对链上节点运行状态和信息发布状态进行监控，发现运行异常节点。
- b) 应具备监控数据的分析和处置能力，对云计算基础设施、平台和应用等进行监测、控制和评估，及时发现和处置系统性能下降、安全漏洞等问题，确保云计算基础设施的安全性和稳定性。

6.4.2.7 平台安全评估

平台安全评估对供方要求如下：

- a) 应在数字政府云计算基础设施服务项目供应过程中定期开展风险评估和安全检查：
 - 1) 确保至少每年开展一次风险评估。发生重大变更或者在出现其他可能影响系统安全状态的条件时，应重新开展风险评估；
 - 2) 使用脆弱性扫描工具和技术进行脆弱性扫描。应根据脆弱性扫描结果，及时修复漏洞或有针对性地进行安全整改，将漏洞影响降低到可接受的水平。
- b) 应在数字政府区块链基础设施服务项目供应过程中定期开展风险评估和安全检查：
 - 1) 确保至少每年开展一次对共识机制的安全性进行查验，保证共识机制安全有效运行；
 - 2) 应对智能合约的安全性进行审核，使用智能合约漏洞检测、静态扫描等技术，保证智能合约的安全运行。
- c) 应建立DDoS防御机制，对DDoS攻击行为进行监测和预警，及时发现和处置DDoS攻击风险；
- d) 应提供安全与统一的管理接口，应确保与外部网络或信息系统的连接只能通过严格管理的接口进行，接口上应部署有边界保护设备。

6.4.2.8 平台组件安全

平台组件安全对供方要求如下：

- a) 应建立云计算服务平台组件资产清单，并定期（至少每年一次）或组件发生重要更新时，及时更新维护资产信息；
- b) 应要求供方承诺所使用的云计算软件和第三方组件不存在已公开的中高危漏洞，或对于存在已公开中高危漏洞未修复的情况，但经过评估后存在补救措施的，需提供相应的安全分析报告。

6.4.3 服务结束安全要求

6.4.3.1 基础设施交付

基础设施交付对供方要求如下：

- a) 应满足数字政府基础设施服务采购合同或协议关于基础软硬件的约定安全要求：
 - 1) 提供关键软硬件的备选方案和供应商；
 - 2) 使用多个供应商提供的关键组件；
 - 3) 储备足够的备用组件；
 - 4) 不从约定供应商或国家采购组件或服务。
- b) 涉及物理机房建设的数字政府基础设施服务，网络架构、通信传输及验证、边界防护、访问控制等安全应满足GB/T 22239—2019中所规定的相关要求。

6.4.3.2 数据迁移

数据迁移对供方要求如下：

- a) 应在服务合同到期时，安全地返还云计算平台上的客户数据；在服务合同定义的时间内，删除云计算平台上存储的客户数据，并确保不能以商业市场的技术手段恢复；
- b) 应提供退出服务方案，明确退出云计算服务时客户数据和业务的迁移、退出方案；
- c) 应为需方数据迁移提供技术手段，并协助完成数据迁移，针对客户数据量大等可能导致迁移过程执行受阻的因素，制定应对措施。

6.5 生成式人工智能服务供应链扩展安全要求

6.5.1 服务入场安全要求

6.5.1.1 生成式人工智能服务信息提供

应向数字政府提供关于生成式人工智能服务训练数据来源、规模、类型、标注规则和算法机制等的详细信息。

6.5.2 服务实施安全要求

6.5.2.1 训练数据安全

训练数据安全对供方要求如下：

- a) 数字政府生成式人工智能服务应使用合法来源的数据和基础模型，并采用有效手段提升数据质量，具体措施包括但不限于：
 - 1) 涉及知识产权的，不得侵害他人依法享有的知识产权；
 - 2) 应避免被恶意篡改的训练数据污染；
 - 3) 涉及个人信息的，应当取得个人同意或者符合法律、行政法规规定的其他情形；
 - 4) 使用开源训练数据时，应具有开源许可协议或相关授权文件；
 - 5) 应提高训练数据来源的多样性，对每一种语言（如中文、英文等），以及每一种类型（如文本、图片、音频、视频等），均应有多个来源。
- b) 向境外提供服务的数字政府生成式人工智能服务，其训练数据应遵循国家数据出境相关规定。
- c) 应采取措施保护数字政府生成式人工智能服务训练数据的安全性和完整性，包括但不限于：
 - 1) 设置数据访问控制策略，防止非授权访问；
 - 2) 应采取密码技术对训练数据、测试数据、算法代码、算法模型等进行保护，应对算法代码、算法模型进行完整性保护，应对训练数据、测试数据的存储、传输进行加密保护；
 - 3) 数据标注应在安全可控的环境进行。

6.5.2.2 模型算法安全

模型算法安全对供方要求如下：

- a) 涉及使用第三方算法推荐技术（包括生成合成类、个性化推送类、排序精选类、检索过滤类、调度决策类等）向用户提供信息的数字政府生成式人工智能服务，使用的第三方算法应已按照《互联网信息服务算法推荐管理规定》通过互联网信息服务算法备案；
- b) 在算法设计、训练数据选择、模型生成和优化、提供服务等过程中，采取有效措施防止数字政府生成式人工智能服务产生民族、信仰、国别、地域、性别、年龄、职业、健康等歧视；
- c) 应使用黑盒攻击、白盒攻击和灰盒攻击等技术手段测试数字政府生成式人工智能服务算法的安全性；
- d) 应开展数字政府生成式人工智能服务健壮性验证确认，包括使用包含对抗噪声、自然噪声、系统噪声、假造、仿造、随机、无意义或与算法应用场景无关等类型的数据对算法进行测试；
- e) 数字政府生成式人工智能服务应建立算法人工中断运行机制，确保算法在被攻击或出现意外时可被人工中断运行；
- f) 算力设备应具备审计能力，可对用户算力使用过程的全面监控和记录，审计日志包括算力使用情况、使用时间、用户身份、操作行为等内容。

6.5.2.3 工具算力安全

工具算力安全对供方要求如下：

- a) 宜优先选用数字政府基础设施服务商提供的生成式人工智能服务GPU和CPU等算力。如确实需要应用厂商提供生成式人工智能服务GPU和CPU等算力，应满足国家信创要求，并需保证算力GPU和CPU等供应的持续性和稳定性等；
- b) 数字政府生成式人工智能服务使用到的关键软件如操作系统、数据库、中间件等，应满足国家信创要求。

6.5.2.4 生成内容安全

生成内容安全对供方要求如下：

- a) 数字政府生成式人工智能服务应在输入模块中使用防御性提示语设计，通过关键词匹配和内容分类等技术进行恶意提示语检测，对输入内容进行自动检测并过滤掉有害的提示语；
- b) 应避免歧视现象的产生，在算法设计和训练数据选择中采取有效措施，确保数字政府生成式人工智能服务生成内容不偏向某些特征值或导致社会边缘化和煽动仇恨；
- c) 数字政府生成式人工智能服务应在输出模块中植入可见或隐藏的标识符作为内容水印，帮助避免生成内容的滥用。

6.5.2.5 第三方模型安全

第三方模型安全对供方要求如下：

- a) 应对数字政府生成式人工智能服务项目第三方组件和基础模型的使用进行审核，并对开源代码进行安全评价，保障来源可靠、安全风险可消除或控制；
- b) 应采取必要措施监测和识别数字政府生成式人工智能服务中第三方基础模型和服务的安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或采取其他措施进行风险控制。

6.6 其他服务供应链扩展安全要求

6.6.1 服务实施安全要求

6.6.1.1 业务风险控制

业务风险控制对供方要求如下：

- a) 涉及等保测评、密评和安全咨询服务的数字政府信息技术服务项目，应在测评前与需方进行充分沟通，详细确定测评范围并签订授权书；
- b) 涉及漏洞扫描、渗透测试等可能对需方业务和数据安全性造成影响的数字政府信息技术服务项目，应采取措施将可能造成的影响降至最小：
 - 1) 应对风险进行评估，制定风险应对措施；
 - 2) 应获得需方授权，签订安全测评授权书；
 - 3) 应经授权后，按需方许可的方式开展安全测评。
- c) 涉及渗透测试服务的数字政府信息技术服务项目，应采取措施确保安全实施：
 - 1) 未经授权许可不应私自进入内网越界访问；
 - 2) 在生产环境中实施时不应使用超级权限账号；
 - 3) 未经授权许可不应超出项目测试范围对内部网络使用扫描器等自动化工具；
 - 4) 未经授权许可不应进行高风险操作，包括但不限于服务器提权操作等；
 - 5) 不应恶意对生产环境业务进行可能造成稳定性、可用性受损的操作行为；
 - 6) 不应提交虚假、描述不清的漏洞信息；
 - 7) 不应利用发现的漏洞做出不利于需方的行为。
- d) 涉及信息技术咨询的数字政府信息技术服务项目，应建立并向供方移交相关的知识库，包括业务模型、数据模型、知识索引、政策法规、解决方案、构件和模板等；
- e) 应制定检测工具更新策略，确保检测工具规则库及时更新。

6.6.1.2 测试数据安全

测试数据安全对供方要求如下：

- a) 涉及安全漏洞扫描、渗透测试和攻防演练等服务的数字政府信息技术服务项目，应采取措施保证测试过程中需方数据安全：
 - 1) 未经授权许可不应下载/拖取需方敏感信息和重要数据；
 - 2) 未经授权许可不应私自篡改需方数据信息；
 - 3) 应在操作实施前进行数据备份，实施完成后应消除实施痕迹。
- b) 涉及等保测评、密评的数字政府信息技术服务项目，应建立服务供应过程中的资料、数据记录清单，保证资料数据获取、使用情况可追溯；
- c) 涉及信息技术咨询的数字政府信息技术服务项目，应记录服务供应过程中访谈人员、访谈经过、数据资料提供人、提供时间等信息，确保服务能力管理和服务过程实施可追溯，服务结果可度量或可评估。

附 录 A
(资料性)
安全要求与其他法律法规技术标准的对应关系

本文件与其他法律法规、技术标准的条款之间的对应关系见表A. 1。

表 A. 1 安全要求与其他法律法规技术标准的对应关系

信息技术服务供应链安全要求		GB/T 36637— 2018	GB/T 32926— 2016	GB/T 39770 —2021	GB/T 32914 —2023	GB/T 43698 —2024	网络安 全审查 办法
基本安 全要求	组织机构	7.3.1.2	4.2.3	—	—	5.1.1	—
	安全管理制度	7.3.1.1	5.2.1-5.2.2	—	—	5.1.2	—
	供应商清单	7.3.3.1	6.1、6.5、7.1	—	5.7	5.1.4	—
	供应链产权管理	—	6.2.1	—	6.4	5.1.5	—
	供应链安全事件管理	7.3.2.5-7.3. 2.6	—	—	—	—	—
	供应保障协同	7.3.3.3	—	—	—	5.2.4	—
服务规 划安全 要求	服务供应商选择	7.3.3.2	—	—	5.7	—	—
	安全合规审查	—	—	—	—	—	第五条
	采购合同或协议	7.3.3.2	6.2.1	5.5.1-5.5. 3、6.4	5.5	—	—
服务入 场安全 要求	实施准备	—	5.1.3	—	—	—	—
	供应商人员安全	7.3.1.3-7.3. 1.4	6.1	7.1.1-7.1. 3	5.3、5.4、6.2	5.1.3	—
	人员/设备入场控制	7.2.3-7.2.4	—	7.3	—	—	—
服务实 施安全 要求	供应过程访问控制	7.2.1、 7.3.2.1	—	6.4、 7.2-7.3	—	—	—
	供应过程数据安全	—	—	6.4、 7.2-7.3	5.3	—	—
	供应过程安全监测	7.2.3	7.1	6.4、 7.2-7.3	—	—	—
	供应过程检查评估	—	5.1	—	—	—	—
	供应过程变更安全	7.2.3	—	7.1.4	6.6	—	—
	第三方软件/组件安全	—	—	—	—	5.2.2	—
服务结束安全要求		—	—	6.5、7.4	—	—	—

附 录 B
(资料性)
通用要求对应安全风险

表B. 1给出了数字政府信息技术服务供应链通用安全风险及控制清单。

表B. 1 数字政府信息技术服务供应链通用安全风险及控制清单

序号	阶段	对象/活动	风险点	风险描述	需方应对措施	供方应对措施
1	通用	组织/制度	监督管理 责任缺失	组织若缺乏明确的安全职责和 专业培训，可能导致无法有效 应对安全事件。	5.1.1.1 a) ~ b)	6.1.1.1 a) ~b)
2		供应商	供应商管 理混乱	供应商若未通过必要的安全认 证，可能无法保证其提供的服 务或产品符合安全标准。	5.1.1.3 a) ~ c)	6.1.1.3 a) ~d)
3		流程	缺乏流程 管控	不完善的安全流程可能导致安 全措施执行不到位，如数据备 份流程缺失导致数据丢失。	5.1.1.4 a) ~ d) 5.1.1.5 a) ~ d)	6.1.1.4 6.1.1.5 a) ~c) 6.1.1.8 a)
4		风险	风险处置 不及时	缺乏足够的资源和准备可能导 致对安全事件的响应延迟，影 响供应链攻击事件处理效率。	5.1.1.7 a) ~ c) 5.1.1.8 a) ~ c) 5.1.1.9 a) ~ b)	6.1.1.6 6.1.1.7 a) ~b)
5		知识产权	知识产权 纠纷	产权界定不清可能引发法律纠 纷，如软件使用权争议影响政 府服务的连续性。	5.1.1.6 a) ~ b) 5.1.2.3 b) 5.1.5.2 a)	6.1.1.5 a) ~c) 6.1.5.2 a)
6		工具	工具合规 性不符	使用未经授权的工具可能违反 法律法规，导致法律责任和罚 款。	5.1.1.6 a) 5.1.3.4 a)	6.1.1.5 a) 6.1.3.3 a)
7	规划	数据	数据泄露	未经授权的信息泄露可能损害 公众信任，例如，政府数据库 遭泄露导致公民个人信息外 泄。	5.1.2.3 a) , c) ~e) 5.1.4.2 a) ~ c) 5.1.5.5 b) ~ c)	6.1.4.2 a) ~o) 6.1.5.5 b) ~c)

8		人员	服务人员 能力缺失	供应商员工若缺乏安全意识， 可能无意中引入安全风险，如 未加密的通信渠道被利用。	5.1.2.3 a)	6.1.3.1 a) 6.1.4.2 a) ~c)
9		供应链路	供应中断 风险	供应链中断可能导致政府服务 无法正常运行，如关键 IT 服务 因供应商问题而中断。	5.1.2.1 a) ~ b) 5.1.2.3 e) 5.1.4.1 e) 5.1.5.1 a)	—

表B.1 数字政府信息技术服务供应链安全风险分析及控制清单（续）

序号	阶段	对象/活动	风险点	风险描述	需方应对措施	供方应对措施
10	规划	人员	服务人员不稳定	供应商人员不稳定，可能影响服务质量，如关键技术支持人员的离职影响服务连续性。	5.1.2.3 a) 5.1.3.2 a)	—
11		合规	未尽网络安全审查义务	需求方若未进行充分的网络安全审查，可能未能及时发现和防范安全风险。	5.1.2.2 a) ~b)	6.1.2.1 a) ~b)
12		合规	合同条款不明晰	合同中安全条款的不明确可能导致责任和义务不清，影响安全事件的处理。	5.1.2.3 a) ~e)	—
13		知识产权	知识产权窃取	需求方的知识产权若未得到妥善保护，可能面临被窃取的风险。	5.1.2.3 b)	6.1.1.5 a)
14		知识产权	知识产权违规使用	使用未经授权的基础软件、管理支撑软件、图片、视频等，可能面临版权问题，如未经授权使用专有软件组件。	5.1.2.3 b)	6.1.1.5 a)
15	入场	人员	驻场人员管理混乱	外部人员在需方场所工作时可能带来的安全风险，如未对访问权限进行适当控制。	5.1.3.2 a) ~d) 5.1.3.3 a) ~e) 5.1.4.1 a) ~e) 5.1.4.3 b) 5.1.5.4 a) ~c)	6.1.3.2 a) ~c)
16		访问	未授权访问	供应商若未能实施有效的访问控制，可能导致敏感数据泄露。	5.1.3.3 b) ~e) 5.1.3.4 a) ~c) 5.1.4.1 c) ~e) 5.1.4.3 a) ~b)	6.1.3.3 a) 6.1.4.1 a) ~e)
17	实施	数据	数据非授权访问	数据若未能得到适当保护，可能遭受未经授权的访问和滥用。	5.1.4.2 a)	6.1.4.2 h)
18		数据	数据篡改	数据若被恶意篡改，可能影响政府决策和公共服务的准确性。	5.1.4.3 a) ~b)	—
19		数据	数据损毁	数据损毁可能导致重要信息丢失，影响政府服务的质量	5.1.4.3 a) ~b)	6.1.4.2 e)

				和连续性。		
--	--	--	--	-------	--	--

表B.1 数字政府信息技术服务供应链安全风险分析及控制清单（续）

序号	阶段	对象/活动	风险点	风险描述	需方应对措施	供方应对措施
20	实施	人员	远程越权访问	远程服务管理可能存在安全漏洞，如远程访问未加密。	5.1.4.1 b)	—
21		业务	需方业务中断	需方业务若因安全事件中斷，可能影响公众对政府服务的满意度。	5.1.4.1 e)	—
22		资源	资源滥用	需方资源若被恶意利用，可能导致服务滥用和资源浪费。	5.1.4.3 b) 5.1.4.4 b)	6.1.4.3 a) ~b)
23		漏洞	软件漏洞利用	软件漏洞若未及时修复，如SQL注入、越权访问等，可能被恶意利用，影响系统安全。	5.1.4.3 a) ~b) 5.1.4.4 a)	6.1.4.3 c) 6.1.4.6 d)
24	结束	服务	需方服务降级	需方若未能持续提升安全能力，可能面临更大的安全风险。	5.1.5.1 a)	6.1.5.2 a) ~b)
25		交付	资产转移丢失	资产移交过程中的不完整可能导致重要信息丢失，影响服务的连续性。	5.1.5.2 a)	6.1.5.2 a)
26		交付	交付物伪造	交付的材料若存在虚假，可能误导决策和执行。	5.1.5.2 b)	6.1.5.2 b)
27		交付	变更失控	配置变更若不可控，可能导致系统不稳定和安全漏洞。	5.1.4.5 a) ~b)， e)	6.1.4.5 a) ~b)， e)

附 录 C
(资料性)
扩展要求对应安全风险

表C. 1给出了数字政府信息技术服务供应链扩展安全风险及控制清单。

表C. 1 数字政府信息技术服务供应链扩展安全风险及控制清单

序号	服务类型	对象/活动	风险点	风险描述	需方应对措施	供方应对措施
1	基础设施服务	供应链路	基础软件供应链攻击	基础软件供应商和软件供应商提供的软件，包括操作系统应用程序和中间件，可能存在安全漏洞。由于云服务基于软件运行，如果软件存在漏洞，可能导致云服务遭受攻击，数据泄露或服务中断。	5.4.2.2 b)	6.4.2.7 c)
2	基础设施服务	数据	基础设施配置泄露	基础设施配置在运营中存在数据泄露和隐私风险，可能导致未经授权的获取、窃取敏感数据，包括信息泄露以及用户个人资料外泄，从而侵犯用户隐私权。	—	6.4.2.5 c)
3	基础设施服务	漏洞	虚拟化软件漏洞	云计算基础设施的虚拟化技术存在安全风险，包括未经授权的访问者可能对虚拟机进行攻击或篡改，导致数据泄露、服务中断或其他安全威胁，同时不稳定性可能影响系统运行和业务连续性。	—	6.4.2.7 a) ~ b)
4	基础设施服务	资源	基础设施不可控	云服务商的用户管理接口可以通过互联网访问，并可获得较大的资源集，可能导致多种潜在的风险，使恶意用户能够控制多个虚拟机的用户界面、操作云服务商界面等。	—	6.4.2.7 d)
5	基础设施服务	技术	监控手段缺失	基础设施可能由于监控工具和技术不足，导致未能及时发现系统性能下降和处理安全漏洞，增加了业务中断和安全威胁的风险。	—	6.4.2.6 b)

表C.1 数字政府信息技术服务供应链扩展安全风险及控制清单（续）

序号	服务类型	对象/活动	风险点	风险描述	需方应对措施	供方应对措施
6	基础设施服务	系统	系统过载	基础设施提供商的系统存在过载的风险，可能导致服务中断或性能下降，影响业务运行。	—	6.4.2.3 c) ~ d)
7	基础设施服务	数据	迁移数据泄露	主机、虚拟机、数据等迁移过程中，未制定充分的迁移预案可能导致意外情况处理不当；安全策略同步迁移，可能导致在迁移过程中存在安全漏洞；迁移传输通道的安全问题可能造成数据泄露或篡改；云数据迁移过程中，数据迁移不彻底，备份数据得不到合理处置，容易导致数据泄露。	5.4.1.2 a)	6.4.3.2 a-c)
8	基础设施服务	组件	依赖组件安全漏洞	云平台依赖于供应链中的多个组件和服务，可能存在安全漏洞或恶意行为；关键设备和组件可能依赖外国供应商，供应商可能受到所在国法律的影响，存在供应链中断的风险。	—	6.4.2.8 a-b)
9	基础设施服务	备份	容灾能力不足	无法在故障或灾难情况下及时恢复服务可能导致用户业务长时间中断或业务数据丢失等风险。	5.4.1.2 b)	6.4.2.3 e) ~ f)
10	基础设施服务	数据	数据违规出境	服务提供商针对涉及数据出境的场景梳理不全面、有遗漏，未建立数据出境安全审核机制。	5.4.2.2 c)	6.4.2.3 g)
11	基础设施服务	环境	隔离失败	在云计算环境中，计算能力、存储与网络在多个用户之间共享。如果不能对不同用户的存储、内存、虚拟机、路由等进行有效隔离，恶意用户就可能访问其他用户的数据并进行修改、删除等操作。	—	6.4.2.4 b) ~ c)
12	开发与集成服务	数据	开发数据泄露	开发人员无意间将包含敏感信息的代码上传到公共代码仓库。	5.2.1.2 a) ~ b)	6.2.1.2 a) ~ d)

表C.1 数字政府信息技术服务供应链扩展安全风险及控制清单（续）

序号	服务类型	对象/活动	风险点	风险描述	需方应对措施	供方应对措施
13	开发与集成服务	组件	开源组件漏洞	集成的开源组件若未经充分安全审查，可能带来安全隐患，例如，未经审查的第三方库可能含有恶意代码。	—	6.2.1.4 a) ~ g)
14	开发与集成服务	工具	开发工具污染	若开发环境的安全管控措施不足，可能遭受攻击，如开发服务器缺乏足够的访问控制和监控。	5.2.1.1 a) ~ b)	6.2.1.1 a) ~ b)
15	开发与集成服务	软件	软件后门植入	如开发者账号被盗用后用于植入恶意后门。	—	6.2.2.1 a), d) ~ f)
16	开发与集成服务	软件	产品恶意篡改	在软件开发或编译过程中，若安全措施不到位，产品可能被恶意篡改，例如，编译环境被入侵导致软件被植入恶意代码。	—	6.2.2.1 a) ~ b), g) ~ h)
17	开发与集成服务	软件	产品假冒伪劣	市场上可能存在假冒伪劣的软件产品，这些产品可能未经过正规测试，存在安全漏洞。	—	6.2.2.1 g) ~ h)
18	开发与集成服务	供应商	单一供应来源	过度依赖单一供应商可能导致风险集中，如关键组件供应商出现问题时影响整个开发进度。	5.2.2.1 a)	6.2.2.1 g), j)
19	开发与集成服务	知识产权	开源许可污染	使用不符合许可协议的开源组件可能导致法律风险，例如，未能遵守特定开源许可证的要求。	5.2.2.1 b)	6.2.1.4 b)
20	开发与集成服务	交付	软件交付范围扩大	在产品交付过程中，若未能明确界定交付范围，可能导致功能膨胀或服务超出预期。	5.2.2.1 a) ~ b)	6.2.2.1 l)
21	开发与集成服务	交付	下载与升级劫持	若产品交付过程中的通道未得到有效控制，通过不安全的渠道分发软件可能导致产品被篡改。	—	6.2.2.1 j)
22	开发与集成服务	软件	捆绑下载	软件在安装过程中未经用户明确同意便默认下载和安装额外的应用程序或工具栏，这可能导致用户隐私泄露，甚至可能引入恶意软件。	—	6.2.2.1 j)

表C.1 数字政府信息技术服务供应链扩展安全风险及控制清单（续）

序号	服务类型	对象/活动	风险点	风险描述	需方应对措施	供方应对措施
23	运营与运维服务	数据	数据库拖库	数据库若遭受未经授权的访问和数据提取，可能导致敏感信息泄露，例如，黑客利用 SQL 注入攻击获取并盗走整个数据库内容。	5.1.4.3 a) ~ b)	6.3.2.2 b) , d)
24	运营与运维服务	数据	数据加密勒索	攻击者通过加密数据并要求赎金来解锁，可能导致业务中断和财务损失，如 WannaCry 勒索软件攻击事件。	5.1.4.3 a) ~ b)	6.3.2.2 b)
25	运营与运维服务	数据	污染风险数据注入	恶意数据注入可能破坏数据库的完整性和信任度，例如，攻击者通过输入恶意脚本破坏网页展示的数据。	5.3.2.2 a) ~ e)	—
26	运营与运维服务	依赖	需方业务中断风险	由于系统故障或外部攻击导致的服务中断可能影响需方的正常运营。	5.3.1.1 a) 5.3.2.1 a) ~ d) 5.3.2.2 a) ~ b)	6.3.1.1 a) 6.3.2.1 a) ~ c) 6.3.2.3
27	运营与运维服务	依赖	需方控制能力受限	随着服务外包的增加，需方可能失去对关键服务和数据的直接控制，例如，依赖外部服务商进行数据维护时未能及时响应需方需求。	—	6.3.2.1 a) ~ c)
28	运营与运维服务	环境	生产环境污染	生产环境可能因配置错误、未授权访问或软件漏洞而面临安全风险，如开发环境中的漏洞被利用影响生产系统。	5.3.2.1 a) ~ d)	6.2.1.4 a) ~ c) 6.3.2.2 a) ~ f)
29	运营与运维服务	补丁	补丁更新迟滞	未能及时应用安全补丁可能导致系统易受攻击。	—	6.3.2.4 b)
30	生成式人工智能服务	合规	算法合规风险	人工智能算法具有“黑箱”特性，表现为行为不可控、决策机制难以解释，给人工智能监管带来了一定困难。	5.5.1.1 a)	6.5.2.2 a)

表C.1 数字政府信息技术服务供应链扩展安全风险及控制清单（续）

序号	服务类型	对象/活动	风险点	风险描述	需方应对措施	供方应对措施
31	生成式人工智能服务	合规	生成内容安全合规风险	围绕生成式人工智能服务生成内容，具有一定的随机、不可控的情况，容易出现违规内容、歧视偏见、隐私泄露、内容侵权等诸多风险。	5.5.2.2 a) ~ b)	6.5.2.4 a) ~ c)
32	生成式人工智能服务	语料	训练语料合规风险	不可信的外部训练语料带来合规风险，及涉外服务带来训练语料出境风险。	—	6.5.2.1 a) ~ b)
33	生成式人工智能服务	语料	训练语料投毒	使用不可信来源的语料进行训练时，攻击者可将精心制作的样本插入训练集中来操纵训练数据分布，从而改变模型行为和降低模型性能	—	6.5.2.1 a) ~ c)
34	生成式人工智能服务	语料	训练语料来源不可信	使用不可信来源的语料进行训练时，容易导致产生训练语料投毒、训练语料不合规、生成内容不合规等风险。	—	6.5.2.1 a)
35	生成式人工智能服务	数据	生成内容敏感信息泄露	生成内容中包含个人隐私信息等敏感信息，产生敏感信息泄露	5.5.2.2 a)	—
36	生成式人工智能服务	数据	语料敏感信息泄露	来自内部数据的训练语料未正确进行脱敏处理，导致敏感信息泄露	—	6.5.2.1 c)
37	生成式人工智能服务	算力	算力盗用	生成式人工智能服务的基础算力实施在未经授权许可的情况下被用在生成式人工智能服务计算之外	—	6.5.2.2 f)
38	生成式人工智能服务	内容	提示注入攻击	注入恶意指令的提示可以通过操纵模型的正常输出过程以导致大语言模型产生不适当、有偏见或有害的输出	—	6.5.2.4 a)
39	生成式人工智能服务	插件	违规调用插件	在生成式人工智能服务安全服务中，使用未经授权或不符合安全标准的插件，可能会导致安全漏洞、数据泄露	—	6.1.4.3 c)

表C.1 数字政府信息技术服务供应链扩展安全风险及控制清单（续）

序号	服务类型	对象/活动	风险点	风险描述	需方应对措施	供方应对措施
40	生成式人工智能服务	算力	算力依赖	外部算力中断或 CPU、GPU 算力不可控导致的服务中断安全风险	—	6.5.2.3 a) ~ b)
41	生成式人工智能服务	模型	基础模型缺陷	第三方模型包含恶意代码、漏洞或者使用不安全的算法，导致生成式人工智能服务不安全	5.5.2.3	6.5.2.5 a) ~ b)
42	生成式人工智能服务	模型	模型滥用/恶意使用	使用者因不清楚注意事项，对生成内容滥用、误用产生相关风险	5.5.2.1 a) ~ b)	—
43	其他服务	数据	测试数据泄露	在软件测试过程中，若敏感的测试数据、漏洞数据未被妥善保护，可能导致个人信息、未修复漏洞外泄。	—	6.6.1.2 a)
44	其他服务	业务	测试过程业务中断风险	测评服务过程中，若测试活动影响了生产环境的稳定性，可能会导致需方业务中断，如测试引发的系统故障导致在线服务平台暂时无法使用。	5.6.2.1 a) ~ c)	6.6.1.1 a) ~ c)
45	其他服务	供应商/人员	安全服务降级	选择不当的供应商、服务人员可能导致服务质量不达标，软件和服务未经充分测试可能存在未被发现的安全问题。	5.6.1.1	—
46	其他服务	测试对象	测试范围扩大	在生产环境中实施时使用不该用的超级权限账号，扩大测试功能和范围，导致未知的安全影响。	—	6.6.1.1 a) ~ c)
47	其他服务	测试参数	生产系统破坏	测试过程操作风险较大，在未授权和安全限制情况下可能会导致被测系统业务受影响。	—	6.6.1.1 a) ~ c)
48	其他服务	规则	检测规则滞后	安全检测系统所依赖的规则未能及时更新以适应新兴的威胁和漏洞，陈旧的规则可能导致安全系统产生大量误报，同时漏掉真正的威胁。	—	6.6.1.1 e)

附 录 D
(规范性)
安全评估评分方法

D.1 评估结论组成

供应链安全评估主体分为需方、供方（主要供方），并分别进行供应链安全评估，各评估主体供应链安全评估结论由综合得分和最终评估结论构成。

D.2 综合得分计算

评估项评估结果分值根据其评估结果取值，当评估项为符合时，评估项评估结果分值取1，当评估项为部分符合时，评估项评估结果分值取0.5，当评估项为不符合时，评估项评估结果分值取0。综合得分计算公式如下：

$$P = (\sum s/n) * 100。$$

式中：
P —— 综合得分；
s —— 评估项评估结果分值；
n —— 本次评估项总数，不含未评估项数。

D.3 最终评估结论评判

最终评估结论及判定规则见表 D. 3。

表D.3 评估结论及判别依据

最终评估结论	判别依据
优	评估主体某项服务供应链中存在供应链安全问题，但不会导致此项服务供应链面临中、高等级安全风险，且综合得分 90 分以上（含 90 分），而且供应物辅助验证不存在中、高危漏洞或缺陷。
良	评估主体某项服务供应链中存在供应链安全问题，但不会导致此项服务供应链面临高等级安全风险，且综合得分 80 分以上（含 80 分），而且供应物辅助验证不存在高危漏洞或严重缺陷。
中	评估主体某项服务供应链中存在供应链安全问题，但不会导致此项服务供应链面临高等级安全风险，且系统综合得分 70 分以上（含 70 分）。
差	评估主体某项服务供应链中存在供应链安全问题，而且会导致此项服务供应链面临高等级安全风险，或被测对象综合得分低于 70 分。

附 录 E
(规范性)
增强安全要求

表E.1中的数字政府信息技术服务供应链安全要求为增强安全要求，可根据数字政府信息技术服务类型、规模、服务对象及可能造成的影响选择是否需要满足相关要求。

表E.1 数字政府信息技术服务供应链增强安全要求

服务类型	安全要求序号	内容
通用	5.1.4.1 d)	3) 确保移动工作终端接受移动终端管理服务端的设备生命周期管理、设备远程控制，如：远程锁定、远程擦除等。
	5.1.4.2 b)	数字政府信息技术服务项目实施授权供方下载、导出敏感信息、重要数据的，应对数据进行脱敏处理、添加数据水印
	5.1.4.3 b)	5) 对服务项目的特权账户行为进行监测，及时发现异常登录行为、异常操作行为等安全风险。
	6.1.1.3 b)	应每年对数字政府信息技术服务次级供应商开展不少于 1 次的安全评审，对次级供应商安全资质存续、股权结构变化、业务经营状况等信息进行审查，更新次级供应商管理清单信息。
	6.1.4.6 f)	应通过自动化方式对数字政府信息技术服务项目中的第三方软件进行安装、更新和删除。
开发与集成服务	6.2.2.4 b)	2) 只能存储于项目所属存储资源内。 3) 与项目中的内部数据有明确的标识区别。
	6.2.2.5 d)	数字政府开发与集成服务项目应制定组件使用管控机制，统一管理编码过程中使用的组件版本。
	6.2.2.6 b)	b) 涉及软件开发的数字政府开发与集成服务项目，应建立安全编码规范，针对不同的编程语言，制定相对应安全编码要求，软件安全编码要求和源代码安全检查应符合相关国家标准的要求，主要包括： 1) C/C++语言代码审计应符合 GB/T 34943—2017 中所规定的相关要求； 2) Java 语言代码审计应符合 GB/T 34944—2017 中所规定的相关要求； 3) 其他语言代码审计应符合 GB/T 39412—2020 中所规定的相关要求。
	6.2.2.6 c)	软件漏洞修复和管理应符合 GB/T 28458—2020、GB/T 30276—2020、GB/T 30279—2020 等相关要求。
运营与维护服务	5.3.2.1 b)	5) 应每季度至少进行一次工作终端安全检查，并记录检查结果。
	6.3.1.1 a)	2) 重要程度高的业务运营服务，应确保储备人员满足冗余保障要求。
基础设施服务	6.4.2.3 c)	应建立自有操作系统和容器镜像库。

参 考 文 献

- [1] GB/T 20269—2006 信息安全技术 信息系统安全管理要求
 - [2] GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求
 - [3] GB/T 20274.1—2006 信息安全技术 信息系统安全保障评估框架：简介和一般模型
 - [4] GB/T 29245—2012 信息安全技术 政府部门信息安全管理基本要求
 - [5] GB/T 31509—2015 信息安全技术 信息安全风险评估实施指南
 - [6] GB/T 32926—2016 信息安全技术 政府部门信息技术服务外包信息安全管理规范
 - [7] GB/T 32914—2023 信息安全技术 网络安全服务能力要求
 - [8] GB/T 42446—2023 信息安全技术 网络安全从业人员能力基本要求
 - [9] GB/T 43698—2024 网络安全技术 软件供应链安全要求
 - [10] 广东省人民政府. 关于印发广东省“数字政府”建设总体规划（2018-2020年）的通知: 粤府（2018）105号. 2018年
 - [11] NIST SP.800—218 Secure Software Development Framework (SSDF)
 - [12] NIST (EO) 14028 Critical Software Use Security Measures Guidance
 - [13] NIST (EO) 14028 The Minimum Elements For a Software Bill of Materials (SBOM)
 - [14] NIST(EO)14028 DRAFT Baseline Criteria for Consumer Software Cybersecurity Labeling
 - [15] NIST (EO) 14028 DRAFT Baseline Security Criteria for Consumer IoT Devices
 - [16] NIST (EO) 14028 Guidelines on Minimum Standards for Developer Verification of Software
 - [17] NIST SP.800—161r1 Cybersecurity Supply Chain Risk Management Practices for Systems and Organization
-