网络安全常用标准手册

中共河北省委网络安全和信息化委员会办公室

河北省网络安全和标准化技术委员会

2020 年 5 月

说　明

为便于各单位全面了解网络安全国家标准的现状和整体情况，推进网络安全国家标准在我省的应用实施，河北省委网信办依托河北省网络安全和标准化技术委员会，对常用网络安全国家标准进行了总结梳理，编写了《网络安全常用标准手册（2020版）》。

本手册介绍了网络安全国家标准的整体情况，总结梳理了截至2020年4月的部分现行和即将实施的网络安全标准，按照网络安全基础制度、网络安全管理、新技术新应用等领域进行划分，从基本情况、主要内容、应用说明等三个方面对相关标准进行了解读，适用于各机关单位在日常网络安全管理和运维工作中参考使用。

获取更多网络安全标准信息，请访问全国信息安全标准化技术委员会网站（www.tc260.org.cn）和国家标准全文公开系统（openstd.samr.gov.cn）。

目　录

一、网络安全监督管理制度相关标准

（一）关键信息基础设施保护

《中华人民共和国网络安全法》第三十一条规定，国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。目前关键信息基础设施网络安全保护工作，主要有《信息安全技术 关键信息基础设施网络安全框架》、《信息安全技术 关键信息基础设施网络安全保护基本要求》、《信息安全技术 关键信息基础设施安全控制措施》、《信息安全技术 关键信息基础设施安全检查评估指南》、《信息安全技术 关键信息基础设施安全保障指标体系》等五项标准，其中部分标准还在起草制定中，可先行了解参考。

序号	标准号	标准名称	发布日期	实施日期	备注
1	——	信息安全技术 关键信息基础设施网络安全框架	——	——	《信息安全技术 关键信息基础设施网络安全框架》作为基础标准，阐明构成框架的基本要素及其关系，统一通用术语和定义。
2	——	信息安全技术 关键信息基础设施网络安全保护基本要求	——	——	《信息安全技术 关键信息基础设施网络安全保护基本要求》作为基线类标准，对关键信息基础设施运营者开展网络安全保护工作提出最低要求。
3	——	信息安全技术 关键信息基础设施安全控制措施	——	——	《信息安全技术 关键信息基础设施安全控制措施》作为实施类标准，根据基本要求提出相应的控制措施。
4	——	信息安全技术 关键信息基础设施安全检查评估指南	——	——	《信息安全技术 关键信息基础设施安全检查评估指南》作为测评类标准，依据基本要求明确关键信息基础设施检查评估的目的、流程、内容和结果。

序号	标准号	标准名称	发布日期	实施日期	备注
5	——	信息安全技术 关键信息基础设施安全保障指标体系	——	——	《信息安全技术 关键信息基础设施安全保障指标体系》作为测评类标准，依据检查评估结果、日常安全检测等情况对关键信息基础设施安全保障状况进行定量评价。

（二）网络安全等级保护

《中华人民共和国网络安全法》第二十一条规定，国家实行网络安全等级保护制度。2019 年网络安全等级保护进入 2.0 时代，保护对象范围在传统信息系统的基础上增加了云计算、移动互联、物联网、大数据等，对等级保护制度提出了新的要求。各单位应严格对照相关网络安全国家标准，落实等级保护工作中的网络定级及评审、备案及审核、等级测评、安全建设整改等要求。

序号	标准号	标准名称	发布日期	实施日期	备注
1	GB/T 25058-2019	信息安全技术 网络安全等级保护实施指南	2019/8/30	2020/3/1	本标准规定了等级保护对象实施网络安全等级保护工作的过程，适用于指导网络安全等级保护工作的实施。
2	GB/T 25070-2019	信息安全技术 网络安全等级保护安全设计技术要求	2019/5/10	2019/12/1	本标准规定了网络安全等级保护第一级到第四级等级保护对象的安全设计技术要求，适用于指导运营使用单位、网络安全企业、网络安全服务机构开展网络安全等级保护安全技术方案的设计和实施，也可作为网络安全职能部门进行监督、检查和指导的依据。
3	GB/T 22239-2019	信息安全技术 网络安全等级保护基本要求	2019/5/10	2019/12/1	本标准规定了网络安全等级保护的第一级到第四级等级保护对象的安全通用要求和安全扩展要求，适用于指导分等级的非涉密对象的安全建设和监督管理。

序号	标准号	标准名称	发布日期	实施日期	备注
4	GB/T 36958-2018	信息安全技术 网络安全等级保护安全管理中心技术要求	2018/12/28	2019/7/1	本标准从安全管理中心的功能、接口、自身安全等方面，对 GB/T 25070 中提出的安全管理中心及其安全技术和机制进行了进一步规范，提出了通用的安全技术要求，指导安全厂商和用户依据本标准要求设计和建设安全管理中心。
5	GB/T 22240-2020	信息安全技术 网络安全等级保护定级指南	2020/4/28	2020/11/1	本标准规定了定级方法，为各系统建设使用单位定级工作提供指导。

二、网络安全管理运维工作相关标准

（一）信息安全管理体系

信息安全管理体系（ISMS）是组织在整体或特定范围内建立信息安全方针和目标，以及完成这些目标所用方法的体系。各单位应结合自身实际建立信息安全管理体系,可以有效规范工作人员行为，保证各种技术手段的有效落实，合理统筹管理软硬件，对有序、高效开展网络安全工作具有重大意义。

序号	标准号	标准名称	发布日期	实施日期	备注
1	GB/T 20269-2006	信息安全技术 信息系统安全管理要求	2006/05/31	2006/12/01	本标准依据 GB 17859-1999 的五个安全保护等级的划分，规定了信息系统安全所需要的各个安全等级的管理要求。
2	GB/T 20282-2006	信息安全技术 信息系统安全工程管理要求	2006/05/31	2006/12/01	本标准规定了信息安全工程的管理要求，是对信息安全工程中所涉及到的需求方、实施方与第三方工程实施的指导性文件，各方可以此为依据建立安全工程管理体系。本标准按照 GB17859-1999 划分的五个安全保护等级，规定了信息安全工程的不同要求。本标准适用于该系统的需求方和实施方的工程管理，其他有关各方也可参照使用。

序号	标准号	标准名称	发布日期	实施日期	备注
3	GB/T 22080-2016	信息技术 安全技术 信息安全管理体系要求	2016/08/29	2017/03/01	本标准规定了在组织环境下建立、实现、维护和持续改进信息安全管理体系要求。
4	GB/T 31496-2015	信息技术 安全技术 信息安全管理体系实施指南	2015/05/15	2016/01/01	本标准依据 GB/T 22080-2008，关注设计和实施一个成功的信息安全管理体系（ISMS）所需要的关键方，描述了 ISMS 规范及其设计的过程，从开始到产生实施计划，适用于各种规模和类型的组织（例如，商业企业、政府机构、非赢利组织）。
5	GB/T 31722-2015	信息技术 安全技术信息安全风险管理	2015/06/02	2016/02/01	本标准为信息安全风险管理提供指南。本标准支持GB/T 22080 所规约的一般概念，旨在为基于风险管理方法来符合要求地实现信息安全提供帮助。
6	GB/T 32923-2016	信息技术 安全技术 信息安全治理	2016/08/29	2017/03/01	本标准就信息安全治理的概念和原则提供指南，通过本标准， 组织可以对其范围内的信息安全相关活动进行评价、指导、监视和沟通。本标准适用于所有类型和规模的组织。

（二）风险管理

实施网络安全风险管理，将安全风险控制在可接受的水平是网络安全工作的基本方法论。随着政府部门、企事业单位以及各行各业对信息系统依赖程度的日益增强,运用风险评估去识别安全风险、解决信息安全问题得到了广泛的认识和应用。各单位应积极开展风险评估和管理工作，主动避免风险，有效控制和管理风险。

序号	标准号	标准名称	发布日期	实施日期	备注
1	GB/T 20984-2007	信息安全技术 信息安全风险评估规范	2007/06/14	2007/11/01	本标准提出了风险评估的基本概念、要素关系、分析原理、 实施流程和评估方法，以及风险评估在信息系统生命周期

序号	标准号	标准名称	发布日期	实施日期	备注
					不同阶段的实施要点和工作形式适用于规范组织开展的风险评估工作。
2	GB/T 31509-2015	信息安全技术 信息安全风险评估实施指南	2015/05/15	2016/01/01	本标准规定了信息安全风险评估实施的过程和方法，适用于各类安全评估机构或被评估组织对非涉密信息系统的信息安全风险评估项目的管理，指导风险评估项目的组织、实施、验收等工作。
3	GB/T 33132-2016	信息安全技术 信息安全风险处理实施指南	2016/10/13	2017/05/01	本标准给出了信息安全风险处理实施的管理过程和方法，适用于指导信息系统运营使用单位和信息安全服务机构实施信息安全风险处理活动。
4	GB/Z 24364-2009	信息安全技术 信息安全风险管理指南	2009/09/30	2009/12/01	本指导文件规定了信息安全风险管理的内容和过程，为信息系统生命周期不同阶段的信息安全风险管理提供指导。本指导性技术文件适用于指导组织进行信息安全风险管理工作。

（三）运维管理

部分单位在日常网络安全工作中存在重安全建设、轻安全运维的情况，而安全运维是避免网络安全事件的最有效手段。下述标准从多个方面为安全运维工作提供了规范性参考，各单位应积极学习对照，推动网络安全运维管理工作规范化、长效化。

序号	标准号	标准名称	发布日期	实施日期	备注
1	GB/T 36626-2018	信息安全技术 信息系统安全运维管理指南	2018/09/17	2019/04/01	本标准从技术方面规定，为目前企业和政府在 IT 安全运维管理方面提供了指导。主要技内容：从角色和责任、部门 IT 安全策略、IT 项目安全资源、管理控制、系统开发生命周期的安全性、信息和 IT 设备识别和分类、安全风险管理、事件管理等几个方面进行描述。

（四）事件管理

网络安全没有绝对的安全，管理和处置各类网络安全事件，是做好网络安全工作的重要方面。各单位要认真学习网络安全事件管理相关国家标准，明确网络安全事件的分级分类及处置流程，科学正确处置各种数据丢失、网络瘫痪、网站被篡改等网络安全事件。

序号	标准号	标准名称	发布日期	实施日期	备注
1	GB/T 20985.1-2017	信息技术 安全技术 信息安全事件管理 第1部分：事件管理原理	2017/12/29	2018/07/01	本指导性技术文件描述了信息安全事件的管理过程，提供了规划和制定信息安全事件管理策略和方案的指南，给出了管理信息安全事件和开展后续工作的相关过程和规程，可用于指导信息安全管理者，信息系统、服务和网络管理者对信息安全事件的管理。
2	GB/T 20988-2007	信息安全技术 信息系统灾难恢复规范	2007/06/14	2007/11/01	本标准规定了信息系统灾难恢复应遵循的基本要求，适用于信息系统灾难恢复的规划、审批、实施和管理。
3	GB/T 30285-2013	信息安全技术 灾难恢复中心建设与运维管理规范	2013/12/31	2014/07/15	本标准规定了灾难恢复中心建设与运维的管理过程，适用于开展信息系统灾难恢复及业务连续性活动的机构或提供信息系统灾难恢复及业务连续性服务的服务机构。
4	GB/Z 20986-2007	信息安全技术 信息安全事件分类分级指南	2007/06/14	2007/11/01	本指导性技术文件为信息安全事件的分类分级提供指导，用于信息安全事件的防范与处置，为事前准备、事中应对、事 后处理提供一个基础指南，可供信息系统和基础信息传输网络的运营和使用单位以及信息安全主管部门参考使用。
5	GB/T 36957-2018	信息安全技术 灾难恢复服务要求	2018/12/28	2019/07/01	标准范围包括：对灾难备份与恢复服务提供者应具备的服务提供者能力要求、服务过程要求，以及对提供信息系统灾难备份与恢复服务的组织进行评估的方法。

序号	标准号	标准名称	发布日期	实施日期	备注
6	GB/T 37046-2018	信息安全技术 灾难恢复服务能力评估准则	2018/12/28	2019/07/01	本标准适用于信息系统灾难恢复服务机构。主要技术内容:1.确立灾难恢复服务机构的服务资质等级；2.规定各等级灾难恢复服务机构的基本资格；3.明确各等级灾难恢复服务机构的基本能力要求；4.制定各等级灾难恢复服务机构的质量管理能力衡量标准；5.提出各等级灾难恢复服务机构的灾难恢复服务能力要求。

（五）监测预警

网络安全监测预警，是重要的网络安全日常基础性工作。各单位应深入了解网络攻击的类型、技术、方式，明确网络安全事件或威胁的重要程度和可能造成的影响，规范开展网络安全监测预警工作，提高网络安全风险威胁防御保障能力，为抵御攻击夯实基础。

序号	标准号	标准名称	发布日期	实施日期	备注
1	GB/T 32924-2016	信息安全技术 网络安全预警指南	2016/08/29	2017/03/01	本标准给出了网络安全预警的分级指南与处理流程，为及时准确了解网络安全事件或威胁的影响程度、可能造成的后果，及采取有效措施提供指导，也适用于网络与信息系统主管和运营部门参考开展网络安全事件或威胁的处置工作。
2	GB/T 37027-2018	信息安全技术 网络攻击定义及描述规范	2018/12/28	2019/07/01	本标准明确了网络攻击的基本要求，提出了网络攻击与防范的基本行为准则适用于对计算机网络实施攻击和防范的个人、企事业单位和社会团体等组织。

（六）可信计算

随着物联网、大数据、云计算等新技术普及，网络安全压力增大，采用可信技术以确保数据存储可信、操作行为可信、体系结构

可信、资源配置可信和策略管理可信。

序号	标准号	标准名称	发布日期	实施日期	备注
1	GB/T 29827-2013	信息安全技术可信计算规范可信平台主板功能接口	2013/11/12	2014/02/01	本标准规定了可信平台主板的组成结构、信任链构建流程、功能接口，适用于基于可信平台控制模块的可信平台主板的设计、生产和使用。
2	GB/T 29828-2013	信息安全技术可信计算规范可信连接架构	2013/11/12	2014/02/01	本标准规定了可信平台主板的组成结构、信任链构建流程、功能接口，适用于基于可信平台控制模块的可信平台主板的设计、生产和使用。
3	GB/T 36639-2018	信息安全技术可信计算规范服务器可信支撑平台	2018/09/17	2019/04/01	本标准适用于云计算环境下可信服务器平台的研发、生产、集成。可信服务器的测试及管理可参照本标准。本标准主要内容包括：1.TPCM 和 TSB 在可信服务器平台中应用；2.虚拟环境下，可信服务器平台完整性度量、传递与报告；3.虚拟 TPCM 的组成结构、功能及安全性要求；4.虚拟机可信迁移及远程证明的流程及功能要求；5.根据服务器主板的特点，对 GB/T 29827-2013《信息安全技术可信计算规范可信平台主板功能接口》的功能扩展。
4	GB/T 37935-2019	信息安全技术可信计算规范可信软件基	2019/8/30	2020/3/1	本标准规定了可信软件基的功能结构、工作流程、保障要求和交互接口规范，适用于可信软件基的设计、生产和测评。

（七）电子政务

随着政府部门办公信息化程度不断提高，网络安全隐患也随之暴露，越来越成为不法分子攻击的重点目标。为加强电子政务办公领域网络安全反顾和，国家从网络、软件、硬件、技术、管理等多个方面出台一系列国家标准，各单位要认真学习遵循、同步整改。

序号	标准号	标准名称	发布日期	实施日期	备注
1	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	2016/08/29	2017/03/01	本标准建立了政府部门信息技术服务外包信息安全管理模型，提出了政府部门信息技术服务外包信息安全管理生命周期各阶段活动的管理要求，适用于政府部门采购和使用信息技术服务。
2	GB/T 32925-2016	信息安全技术 政府联网计算机终端安全管理基本要求	2016/8/29	2017/3/1	本标准是 GB/T29245—2012《信息安全技术 政府部门信息安全管理基本要求》框架下的政府部门信息安全保障标准体系的组成部分，用于指导各级政府部门对所管辖范围内联网计算机终端的管理和安全检查工作，使其具备一定的安全防护能力，可与各种具体的计算机终端应用场景、操作系统和应用软件的配置指南配合使用。
3	GB/T 29244-2012	信息安全技术 办公设备基本安全要求	2012/12/31	2013/06/01	本标准规定了办公设备安全技术要求和安全管理功能要求，适用于政府部门等机构中对办公设备具有高安全要求的信息处理环境，用于办公设备的采购、测评、维护和管理，也可为办公设备的设计提供参考。
4	GB/T 35282-2017	信息安全技术 电子政务移动办公系统安全技术规范	2017/12/29	2018/07/01	本标准基于电子政务移动办公系统的基本结构和主要安全风险，提出了电子政务移动办公系统的整体安全框架，规定了移动终端安全、信道安全、移动接入安全和服务端安全应满足的技术要求。
5	GB/T 35283-2017	信息安全技术 计算机终端核心配置基线结构规范	2017/12/29	2018/07/01	本标准规定了计算机终端核心配置基线的基本要素，规范了基于 XML 的核心配置基线标记规则，给出了核心配置基线应用方法实例，适用于计算机终端的核心配置自动化工作，包括计算机终端核心配置自动化工具的设计、开发和应用。

序号	标准号	标准名称	发布日期	实施日期	备注
6	GB/T 37091-2018	信息安全技术 安全办公U盘安全技术要求	2018/12/28	2019/07/01	本标准将为安全办公U盘产品定义了一组与具体实现无关的、完整的、紧密关联的最小安全要求集合；标准描述了安全办公U盘使用中的环境和面临的威胁；陈述相应保证级别的安全办公U盘应该达到的安全目的和必须满足的安全技术要求和安全保证要求，以及它们之间的基本原理。本项目将结合目前国内外最新技术的发展情况,制定安全办公U盘安全技术要求。
7	GB/T 37096-2018	信息安全技术 办公信息系统安全测试规范	2018/12/28	2019/07/01	本标准从信息技术方面规定了按照《信息安全技术 安全可靠办公信息系统技术要求》对办公信息系统进行测试所需要的内容，适用于政府部门等对信息处理环境具有较高安全要求的办公信息系统的测试，用于安全办公信息系统的测试，也可为办公信息系统的设计提供参考。
8	GB/T 37095-2018	信息安全技术办公信息系统安全基本技术要求	2018/12/28	2019/07/01	本标准主要面向基于国产CPU/OS的办公信息系统(党委、政府、军队、档案馆等系统)的硬件需求、基础软件需求及业务系统需求，从功能性、可靠性、性能、安全性、可维护性、可移植性等方面制定系统的评价指标，为系统的建设提供技术依据。
9	GB/T 37094-2018	信息安全技术 办公信息系统安全管理要求	2018/12/28	2019/07/01	本标准从信息技术方面规定了按照《信息安全技术 安全可靠办公信息系统技术要求》的基础进行信息系统建设、开发的内容，适用于政府部门等对信息处理环境具有较高安全要求的办公信息系统的建设。
10	GB/T 29240-2012	信息安全技术终端计算机通用安全技术要求与测试评价方法	2012/12/31	2013/06/01	本标准按照国家信息安全等级保护的要求，规定了终端计算机的安全技术要求和测试评价方法，适用于指导终端计算机的设计生产企业、使用单位和信息安全服务机构实施终端计算机等级保护安全技术的设计、实现和评估工作。

序号	标准号	标准名称	发布日期	实施日期	备注
11	GB/T 37002-2018	信息安全技术 电子邮件系统安全技术要求	2018/12/28	2019/07/01	本标准适用于各级政务部门、研究机构、企事业单位等的互联网邮件系统、电子政务外网邮件系统、电子政务内网邮件系统或单位内网邮件系统的设计、实现和使用，也适用于相关生产厂商用于设计、研制、开发、制造、测试、管理、集成和维护。
12	GB/Z 24294.1-2018	信息安全技术 基于互联网电子政务信息安全实施指南 第1部分：总则	2018/03/15	2018/10/01	本标准适用于地市级(含以下)政府单位，基于互联网开展不涉及国家秘密的电子政务信息安全建设，为工程技术人员设计基于互联网电子政务信息安全保障架构提供技术参考。
13	GB/Z 24294.2-2017	信息安全技术 基于互联网电子政务信息安全实施指南 第2部分：接入控制与安全交换	2017/05/31	2017/12/01	本标准明确了互联网电子政务分域控制的两个阶段，在接入控制阶段，对接入控制结构、接入安全设备功能、接入认证、接入控制规则、接入控制管理等方面给出指南性建议要求；在安全交换阶段，对安全交换模式、定制数据安全交换要求、数据流安全交换要求给出指南性建议要求，适用于没有电子政务外网专线或没有租用通信网络专线条件的组织机构，为管理人员、工程技术人员、信息安全产品提供者进行信息安全规划与建设提供管理和技术参考。
14	GB/Z 24294.3-2017	信息安全技术 基于互联网电子政务信息安全实施指南 第3部分：身份认证与授权管理	2017/05/31	2017/12/01	本部分根据信任体系构建策略要求，明确相关的身份认证及授权管理功能要求，定义身份认证与授权管理技术规范。本部分适用于互联网电子政务系统中身份认证与授权管理系统的设计、研发与建设。

序号	标准号	标准名称	发布日期	实施日期	备注
15	GB/Z 24294.4-2017	信息安全技术 基于互联网电子政务信息安全实施指南 第4部分：终端安全防护	2017/05/12	2017/12/01	GB/Z 24292 的本部分按照终端安全防护策略,明确了基于互联网电子政务终端的安全防护技术要求。适用于没有电子政务外网专线或没有租用通信网络专线条件的组织机构，基于互联网开展不涉及国家秘密的电子政务信息安全建设,提供管理和技术参考。
16	GB/T 29245-2012	信息安全技术政府部门信息安全管理基本要求	2012/12/31	2013/06/01	本标准规定了政府部门信息安全管理基本要求，用于指导各级政府部门的信息安全管理工作。本标准适用于各级政府部门，其他单位可以参考使用。
17	GB/T 31506-2015	信息安全技术政府门户网站系统安全技术指南	2015/05/15	2016/01/01	本标准给出了政府门户网站系统安全技术控制措施。本标准适用于指导政府部门开展门户网站系统安全技术防范工作，也可作为对政府门户网站系统实施安全检查的依据。
18	GB/T 30278-2013	信息安全技术政务计算机终端核心配置规范	2013/12/31	2014/07/15	本标准提出了政务计算机终端核心配置的基本概念和要求，规定了核心配置的自动化实现方法，规范了核心配置实施流程。本标准适用于政务部门开展计算机终端的核心配置工作。
19	GB/T 36619-2018	信息安全技术政务和公益机构域名命名规范	2018/09/17	2019/04/01	本标准规定了政务和公益机构域名的命名规范，党的机关可以参照本规范命名其域名。

（八）通信网络

在网络安全保障工作中，服务器、应用系统往往被认为是防护重点，而作为覆盖面最广的通信网络往往被忽视。网络安全环环相扣，不能有短板，国家也出台了一系列关于网络通讯协议安全、域名系统、端安全、传输安全的相关国家标准，各单位应高度重视通信网络的规划和建设工作。

序号	标准号	标准名称	发布日期	实施日期	备注
1	GB/T 20270-2006	信息安全技术网络基础安全技术要求	2006/05/31	2006/12/01	本标准描述了关键信息基础设施网络安全保护的角色和职责，规定了关键信息基础实施网络安全保护在识别认定、安全防护、检测评估、监测预警、应急处置等环节的基本要求。本标准适用于关键信息基础设施的规划设计、开发建设、运行维护、退出废弃等阶段。
2	GB/T 33134-2016	信息安全技术公共域名服务系统安全要求	2016/10/13	2017/05/01	本标准规定了公共域名服务系统的基本要求、技术要求以及管理要求。本标准适用于顶级域名服务系统，其他各级域名服务系统、递归域名服务系统的开发和管理。
3	GB/T 33562-2017	信息安全技术安全域名系统实施指南	2017/05/12	2017/12/01	本标准规定了域名系统安全扩展协议（DNSSEC）部署过程中权威域名系统安全、递归域名系统安全、DNS 事务安全、DNS 数据安全等 DNS 安全技术指南。本标准适用于运行域名系统的组织内域名系统安全管理人员。
4	GB/T 25068.1-2012	信息技术 安全技术 IT 网络安全 第 1 部分:网络安全管理	2012/06/29	2012/10/01	GB/T 25068 的本部分规定了网络和通信安全方面的指导，包括信息系统网络自身的互连以及将远程用户连接到网络，适用于那些负责信息安全管理，尤其是网络安全管理的相关人员。
5	GB/T 25068.2-2012	信息技术 安全技术 IT 网络安全 第 2 部分:网络安全体系结构	2012/06/29	2012/10/01	GB/T 25068 的本部分规定了用于提供端到端网络安全的网络安全体系结构。这种体系结构能应用于关注端到端安全且独立于网络下层技术的各种类型的网络。GB/T 25068 的本部分的目标是作为开发详细端到端网络安全建议的基础。
6	GB/T 25068.3-2010	信息技术 安全技术 IT 网络安全 第 3 部分:使用安全网关的网间通信安全保护	2010/09/02	2011/02/01	本部分规定了各种安全网关技术、组件和各种类型的安全网关体系结构，提供安全网关的选择和配置指南。本部分适用于技术和管理人员，有助于用户正确的选择最能满足其安全要求的安全网关体系结构类型。

序号	标准号	标准名称	发布日期	实施日期	备注
7	GB/T 25068.4-2010	信息技术 安全技术 IT 网络安全 第 4 部分:远程接入的安全保护	2010/09/02	2011/02/01	本部分规定了安全使用远程接入的安全指南。本部分介绍不同类型的远程接入以及使用的协议，讨论与远程接入相关的鉴别问题，并提供安全建立远程接入时的支持。本标准适用于那些计划使用这种连接或者已经使用这种连接并且需要其安全建立及安全操作方式建议的网络管理员和技术员。
8	GB/T 25068.5-2010	信息技术 安全技术 IT 网络安全 第 5 部分:使用虚拟专用网的跨网通信安全保护	2010/09/02	2011/02/01	本部分规定了使用虚拟专用网（VPN)连接到互联网络以及将远程用户连接到网络上的安全指南。本部分适用于在使用 VPN 时负责选择和实施提供网络安全锁必需的技术控制的人员，以及负责随后的 VPN 安全的网络监控人员。

（九）个人信息保护

在大数据、云计算、万物互联的时代，基于数据的应用日益广泛，同时也带来了巨大的个人信息安全问题，个人信息如何被安全的收集、保存、使用、共享、转让和公开成为重中之重，国家积极制定了一系列标准予以规范。各单位要在个人信息的全生命周期中贯彻落实网络安全国家标准，切实做好个人信息保护工作。

序号	标准号	标准名称	发布日期	实施日期	备注
1	GB/Z 28828-2012	信息安全技术 公共及商用服务信息系统个人信息保护指南	2012/11/05	2013/02/01	本指导性技术文件规范了全部或部分通过信息系统进行个人信息处理的过程，为信息系统中个人信息处理不同阶段的个人信息保护提供指导。本指导性技术文件适用于指导除政府 机关等行使公共管理职责的机构以外的各类组织和机构，如电信、金融、医疗等领域的服务机构，开展信息系统中的个人信息保护工作。

2	GB/T 35273-2020	信息安全技术个人信息安全规范	2020/3/1	2020/10/1	本标准规范了开展收集、保存、使用、共享、转让、公开披露等个人信息处理活动应遵循的原则和安全要求。本标准适用于规范各类组织个人信息处理活动，也适用于主管监管部门、第三方评估机构等对个人信息处理活动进行监督、管理和评估。
3	GB/T 37964-2019	信息安全技术个人信息去标识化指南	2019/8/30	2020/3/1	本标准描述了个人信息去标识化的目标和原则，提出了去标识化过程和管理措施。本标准针对微数据提供具体的个人信息去标识化指导，适用于组织开展个人信息去标识化工作，也适用于网络安全相关主管部门、第三方评估机构等组织开展个人信息安全监督管理、评估等工作。

三、新技术、新应用及工控领域网络安全标准

（一）云计算

随着云计算技术的蓬勃发展，政府部门及重点行业等对采用云计算服务有了大量需求，为确保云服务客户安全地使用云计算服务，确保云服务商的安全能力符合国家相关标准要求，国家出台了一系列云安全国家标准，并于2019年由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、财政部制定《云计算服务安全评估办法》，为各单位建设和选用云服务提供了安全标准。

序号	标准号	标准名称	发布日期	实施日期	备注
1	GB/T 31167-2014	信息安全技术云计算服务安全指南	2014/09/03	2015/04/01	本标准描述了云计算可能面临的主要安全风险，提出了政府部门采用云计算服务的安全管理基本要求及云计算服务的生命周期各阶段的安全管理和技术要求。本标准为政府部门采用云计算服务，特别是采用社会化的云计算服务提供全生命周期的安全指导，也可供重点行业和其他企事业单位参考。

序号	标准号	标准名称	发布日期	实施日期	备注
2	GB/T 31168-2014	信息安全技术云计算服务安全能力要求	2014/09/03	2015/04/01	本标准规定了对以社会化方式为特定客户提供云计算服务的云服务商安全能力进行测评的要求。本标准适用于第三方测评机构云服务安全能力进行的测试评估。为信息安全主管部门提供参考，还适用于指导云服务商建设安全的云计算平台和提供安全的云计算服务。
3	GB/T 34942-2017	信息安全技术云计算服务安全能力评估方法	2017/11/01	2018/05/01	本标准给出了依据 GB/T 31168－2014《信息安全技术 云计算服务安全能力要求》，开展评估的原则、实施过程以及针对各项具体安全要求进行评估的方法。本标准适用于第三方评估机构对云服务商提供云计算服务时具备的安全能力进行评估，云服务商在对自身云计算服务安全能力进行自评估时也可参考。也可供重点行业和其他企事业单位使用云计算服务时参考。
4	GB/T 35279-2017	信息安全技术云计算安全参考架构	2017/12/29	2018/07/01	本标准给出了云计算安全参考架构，描述了云计算角色，规范了各角色的安全职责、安全功能组件及其关系。本标准适用于指导所有云计算参与者在进行云计算系统规划时对安全的评估与设计。
5	GB/T 38249-2019	信息安全技术政府网站云计算服务安全指南	2019/10/18	2020/5/1	本标准提出了政府部门采用云计算服务的安全基本要求，以及云计算服务生命周期各阶段的安全管理和技术要求，给出了政府网站采用云计算服务中各种参与角色的安全职责，细化了云服务商和云服务代理商的安全责任，可用于指导云计算服务的政府机构的网站安全保障建设。
6	GB/T 37956/2019	信息安全技术网站安全云防护平台技术要求	2019/8/30	2020/3/1	本标准规定了网站安全云防护平台的技术要求，包括平台功能要求和平台安全要求。适用于网站安全云防护平台的开发、运营及使用，为政府部门、企事业单位、社会团体等组织或个人选购网站安全云防护平台提供参考。
7	GB/T 37972/2019	信息安全技术云计算服务运行监管框架	2019/8/30	2020/3/1	本标准规范了政府部门云服务客户在使用云计算服务的过程中云服务商、运行监管方的相关责任及监管内容，提出了运行监管框架、过程及方式，为云服务商支撑云计算服务运行监管活动提供指导，为运行监管方开展运行监管提供指导。

（二）大数据

大数据服务是针对数量巨大、种类多样、流动速度快、特征多变等特性的数据集，提供覆盖数据生命周期相关数据活动的一种网络信息服务，大数据技术的发展和应用影响着国家的治理模式、企业的决策架构、商业的业务模式以及个人的生活方式。各单位在对大数据进行使用管理时，要按照对应的大数据安全服务能力等级进行全生命周期安全管理，切实做到数据风险安全可控。

序号	标准号	标准名称	发布日期	实施日期	备注
1	GB/T 37973/2019	信息安全技术 大数据安全管理指南	2019/8/30	2020/3/1	本标准提出了大数据安全管理基本原则，规定了大数据安全需求、数据分类分级、大数据活动的安全要求、评估大数据安全风险，适用于各类组织进行数据安全管理，也可供第三方评估机构参考。
2	GB/T 35274-2017	信息安全技术 大数据服务安全能力要求	2017/12/29	2018/7/1	本标准规定了大数据服务提供者应具有的组织相关基础安全能力和数据生命周期相关的数据服务安全能力。适用于对政府部门和企事业单位建设大数据服务安全能力，也适用于第三方机构对大数据服务提供者的大数据服务安全能力进行审查和评估。

（三）工业控制系统

随着工业化和信息化的深度融合，工业控制系统广泛应用于各个与国计民生紧密相关的领域，是工业领域的神经中枢。各单位应按照相关国家标准要求开展工业控制系统信息安全自查自评工作，掌握工业控制系统信息安全总体状况，及时有效发现工业控制系统存在的问题和薄弱环节，提高工业控制系统信息安全防护能力。

序号	标准号	标准名称	发布日期	实施日期	备注
1	GB/T 37980-2019	信息安全技术 工业控制系统安全检查指南	2019/8/30	2020/3/1	本标准用于指导工业控制系统行业用户开展自评工作，掌握工业控制系统信息安全总体状况，及时有效发现工业控制系统存在的问题和薄弱环节，为实现更安全的工业控制系统并在其内部进行有效的风险管理提供帮助。
2	GB/T 36323-2018	信息安全技术 工业控制系统安全管理基本要求	2018/6/7	2019/1/1	本标准针对各行业工业控制系统的安全管理活动的共性特点，提出了工业控制系统安全管理基本框架从领导、规划、支持、运行、绩效评价和持续改进等方面为工业控制系统安全管理活动提出了规范性要求，并给出了为实现该安全管理基本框架所需的安全管理基本控制措施和各级工业控制系统安全管理基本控制措施对应表，以满足组织对各级工业控制系统的安全管理需求，为实现对工业控制系统适度、有效的安全管理控制提供参考。
3	GB/T 36324-2018	信息安全技术 工业控制系统信息安全分级规范	2018/6/7	2019/1/1	本标准规定了基于风险评估的工业控制系统信息安全等级划分规则和定级方法，提出了等级划分模型和定级要素，包括工业控制系统资产重要程度、存在的潜在风险影响程度和需抵御的信息安全威胁程度，并提出了对工业控制系统信息安全划分四个等级的特征。
4	GB/T 36466-2018	信息安全技术 工业控制系统风险评估实施指南	2018/6/7	2019/1/1	本标准在对工业控制系统的资产进行整理分析的基础上，从其资产的安全特性出发，分析工业控制系统的威胁来源与自身脆弱性，归纳出工业控制系统面临的信息安全风险，并给出实施工业控制系统风险评估的指导性建议。本标准主要为第三方安全检测评估机构实施风险评估提供指南，也可供工业控制系统单位自评估时参考。
5	GB/T 32919-2016	信息安全技术 工业控制系统安全控制应用指南	2016/8/29	2017/3/1	本标准适用于工业控制系统拥有者、使用者、设计实现者以及信息安全管理部门，为工业控制系统信息安全设计、实现、整改工作提供指导，也为工业控制系统安全运行、风险评估和安全检查工作提供参考。

序号	标准号	标准名称	发布日期	实施日期	备注
6	GB/T 30976.1-2014	工业控制系统信息安全 第1部分：评估规范	2014/7/24	2015/2/1	GB/T30976的本部分规定了工业控制系统（SCADA，DCS，PLC，PCS等）信息安全评估的目标、评估的内容、实施过程等。本部分适用于系统设计方、设备生产商、系统集成商、工程公司、用户、资产所有人以及评估认证机构等对工业控制系统的信息安全进行评估时使用。
7	GB/T 30976.2-2014	工业控制系统信息安全 第2部分：验收规范	2014/7/24	2015/2/1	本部分规定了对实施安全解决方案的工业控制系统信息安全能力进行验收的验收流程、测试内容、方法及应达到的要求。这些测试是为了证明工业控制系统在增加安全解决方案后满足对安全性的要求，并且保证其主要性能指标在允许范围内。本标准的各项内容可作为实际工作中的指导，适用于各种工艺装置、工厂和控制系统。
8	GB/T 26333-2010	工业控制网络安全风险评估规范	2011/1/14	2011/6/1	本评估标准是一种针对工业控制网络的安全风险评估方法。通过对工业控制网络的安全风险评估可以发现网络的安全隐患，通过采用相应的安全措施弥补安全漏洞，从而增强工业控制网络的安全。本标准规定了工业控制网络安全风险评估的一般方法和准则，描述了工业控制网络安全风险评们一般步骤，侧重于评估对象的分析和评估计划的设计。

（四）物联网

物联网是通过使用射频识别（RFID）、传感器、红外感应器、全球定位系统、激光扫描器等信息采集设备，按约定的协议，把任何物品与互联网连接起来，进行信息交换和通讯，以实现智能化识别、定位、跟踪、监控和管理的一种网络，已经深入应用到了工作和生活中，其感知层和数据传输方面问题安全更是网络安全重灾区

和防范重点。各单位在享受新技术带来便利的同时，应积极对照相关国家标准消除新技术带来的安全隐患。

序号	标准号	标准名称	发布日期	实施日期	备注
1	GB/T 36951-2018	信息安全技术 物联网感知终端应用安全技术要求	2018/12/28	2019/07/01	本标准规定了物联网应用中感知设备的安全技术要求，适用于物联网感知设备。
2	GB/T 37024-2018	信息安全技术 物联网感知层网关安全技术要求	2018/12/28	2019/07/01	本标准通过制定物联网感知层网关安全技术要求，可以为物联网感知层网关安全技术研发与产品产业化提供指导与参考，加强物联网信息安全体系建设，提高物联网应用的安全性。
3	GB/T 37025-2018	信息安全技术 物联网数据传输安全要求	2018/12/28	2019/07/01	本标准通过对不同行业物联网系统的安全性需求进行调研、总结和划分，对物联网感知层数据传输安全要求进行制定和规范。
4	GB/T 37044-2018	信息安全技术 物联网安全参考模型及通用要求	2018/12/28	2019/07/01	本标准通过对不同行业物联网系统安全性需求进行调研、分析和总结，对物联网信息安全参考模型和通用要求进行规范。
5	GB/T 37093-2018	信息安全技术 物联网感知层接入通信网的安全要求	2018/12/28	2019/07/01	本标准规定了物联网多种感知层网络接入公用通信网络的安全技术要求，适用于物联网应用工程中的感知层网络，为其安全通信协议设计和安全接入设计提供指导。

（五）移动互联

随着移动互联技术的快速发展，各单位也越来越多的将电子办公无线化，承载着诸多工作信息的同时也设计大量个人敏感信息，其服务器和终端均易成为攻击者的目标。建议各单位积极研究移动互联方面相关国家标准，进一步完善无线业务系统的服务器安全和终端安全，重点加强移动互联应用中的个人信息保护。

序号	标准号	标准名称	发布日期	实施日期	备注
1	GB/T 35281-2017	信息安全技术 移动互联网应用服务器安全技术要求	2017/12/29	2018/07/01	本标准规定了移动互联网应用服务器的安全技术要求，包括数据安全、业务安全、系统安全、设备安全、协议安全和运 维安全等。本标准适用于支持承载各类移动互联网应用业务 的计算机系统，可用于指导移动互联网应用服务器开发、部署、管理运维和测试评估，也适用于相关产品的设计、实现、测试和服务等。
2	GB/T 35278-2017	信息安全技术 移动终端安全保护技术要求	2017/12/29	2018/07/01	本标准依据《GB/T 18336-2015 信息技术 安全技术 信息技术安全评估准则》规定了移动终端的安全保护技术要求，包括移动终端的安全目的、安全功能要求和安全保障要求。本标准适用于移动终端的设计、开发、测试和评估。
3	GB/T 34978-2017	信息安全技术 移动智能终端个人信息保护技术要求	2017/11/01	2018/05/01	本标准规范了全部或部分通过移动智能终端进行个人信息处理的过程，根据移动智能终端个人信息的分类和不同的处理阶段，对相应的个人信息保护提出了技术要求，适用于指导公共及商业用途的移动智能终端进行个人信息的处理。