信息安全国家标准目录

（2016 版）

全国信息安全标准化技术委员会秘书处

2017 年 2 月

一、 基础标准

1、安全术语						
序号	标准编号	标准名称	对应国际标准	发布日期	实施日期	范围
1.	GB/T 5271.8-2001	信息技术 词汇 第8部分：安全	ISO/IEC 2382-8:1998	2001-07-16	2002-03-01	本标准给出了与信息技术安全相关概念的基本术语及其定义，并明确了这些条目之间的关系。本标准适用于信息和数据安全保护方面的有关标准及国内外交流。 本标准详细定义了有关密码技术、信息分类与信息访问控制、数据与信息的恢复和安全违规等数据与信息安全保护方面的术语及其定义，包括一般概念、信息分类、密码技术、访问控制、安全违规、敏感信息的保护、数据恢复、拷贝保护。
2.	GB/T 25069-2010	信息安全技术 术语		2010-09-02	2011-02-01	本标准界定了与信息安全技术领域相关的概念的术语和定义，并明确了这些条目之间的关系。本标准适用于信息安全技术概念的理解，其他信息安全技术标准的制定以及信息安全技术的国内外交流。
3.	GB/T 28458-2012	信息安全技术 安全漏洞标识与描述规范		2012-06-29	2012-10-01	本标准规定了计算机信息系统安全漏洞的标识与描述规范。本标准适用于计算机信息系统安全管理部门进行安全漏洞信息发布和漏洞库建设。
4.	GB/T 19715.1-2005	信息技术 信息技术安全管理指南 第1部分：信息技术安全概念和模型	ISO/IEC TR 13335-1:1996	2005-04-19	2005-10-01	本部分提出了基本的管理概念和模型，将这些概念和模型引入IT安全管理是必要的。
5.	GB/T 19715.2-2005	信息技术 信息技术安全管理指南 第2部分：管理和规划信息技术安全	ISO/IEC TR 13335-1:1996	2005-04-19	2005-10-01	本部分中的指南提出IT安全管理的一些基本专题以及这些专题之间的关系。这些指南对标识和管理IT安全各个方面是有用的。

6.	GB/T 29246-2012	信息技术 安全技术 信息安全管理体系 概述和词汇	ISO/IEC 27000:2009	2012-12-31	2013-06-01	本标准提供： a） ISMS标准族的概述； b） 信息安全管理体系（ISMS）的介绍； c） “规划-实施-检查-处置”（PDCA）过程的简要描述； d） ISMS标准族所用的术语和定义。 本标准适用于所有类型的组织（例如，商业企业、政府机构、非赢利组织）。

2、测评基础

序号	标准编号	标准名称	对应国际标准	发布日期	实施日期	范围
7.	GB 17859-1999	计算机信息系统 安全保护等级划分准则		1999-09-13	2001-01-01	本标准规定了计算机信息系统安全保护能力的五个等级，即： 第一级：用户自主保护级； 第二级：系统审计保护级； 第三级：安全标记保护级； 第四级：结构化保护级； 第五级：访问验证保护级。 本标准适用于计算机信息系统安全保护技术能力等级的划分。计算机信息系统安全保护能力随着安全保护等级的增高，逐渐增强。

8.	GB/T 18336.1-2015	信息技术　安全技术　信息技术安全评估准则　第1部分：简介和一般模型	ISO/IEC 15408-1：2008	2015-05-15	2016-01-01	GB/T 18336的本部分建立了IT安全评估的一般概念和原则，详细描述了GB/T 18336各部分给出的一般评估模型，该模型整体上可作为评估IT产品安全属性的基础。 本部分给出了GB/T 18336的总体概述。它描述了GB/T 18336的各部分内容；定义了在GB/T 18336各部分将使用的术语及缩略语；建立了关于评估对象（TOE）的核心概念；论述了评估背景；并描述了评估准则针对的读者对象。此外，还介绍了IT产品评估所需的基本安全概念。本部分定义了裁剪ISO/IEC 15408-2和ISO/IEC 15408-3描述的功能和保障组件时可用的各种操作。 本部分还详细说明了保护轮廓（PP）、安全要求包和符合性这些关键概念，并描述了评估产生的结果和评估结论。GB/T 18336的本部分给出了规范安全目标（ST）的指导方针并描述了贯穿整个模型的组件组织方法。关于评估方法的一般信息以及评估体制的范围将在IT安全评估方法论中给出。
9.	GB/T 18336.2-2015	信息技术　安全技术　信息技术安全评估准则　第2部分：安全功能组件	ISO/IEC 15408-2：2008	2015-05-15	2016-01-01	为了安全评估的意图，GB/T 18336的本部分定义了安全功能组件所需要的结构和内容。本部分包含一个安全组件的分类目录，将满足许多IT产品的通用安全功能要求。
10.	GB/T 18336.3-2015	信息技术　安全技术　信息技术安全评估准则　第3部分：安全保障组件	ISO/IEC 15408-3：2008	2015-05-15	2016-01-01	GB/T 18336的本部分定义了保障要求，包括：评估保障级（EAL）——为度量部件TOE的保障定义了一种尺度；组合保障包（CAP）——为度量组合TOE的保障提供了一种尺度；组成保障级和保障包的单个保障组件；PP和ST的评估准则。

11.	GB/T 20274.1-2006	信息安全技术　信息系统安全保障评估框架　第1部分：简介和一般模型		2006-05-31	2006-12-01	本部分给出了信息系统安全保障的基本概念和模型，并建立了信息系统安全保障框架。本部分适用于从事信息系统安全保障工作的所有相关方，包括设计开发者、工程实施者、评估者、认证认可者等。本部分不适用于一下方面：a)人员技能和能力的评估，但对人员安全的要求在管理保障中体现;b)系统评估方法学；c)密码算法固有质量的评价。
12.	GB/T 20274.2-2008	信息安全技术 信息系统安全保障评估框架 第2部分：技术保障		2008-07-18	2008-12-01	本部分建立了信息系统安全技术保障的框架，确立了组织机构内的启动、实施、维护、评估和改进信息安全技术体系的指南和通用原则。GB/T 20274的本部分的定义说明了信息系统安全技术体系建设和评估中反映组织机构信息安全的技术体系架构能力级，以及组织机构信息系统安全的技术要求。GB/T 20274的本部分适用于启动、实施、维护、评估和改进信息安全技术体系的组织机构和涉及信息系统安全技术工作的所有用户、开发人员和评估人员。
13.	GB/T 20274.3-2008	信息安全技术 信息系统安全保障评估框架 第3部分：管理保障		2008-07-18	2008-12-01	本部分建立了信息系统安全技术保障的框架，确立了组织机构内的启动、实施、维护、评估和改进信息安全技术体系的指南和通用原则。本部分的定义说明了信息系统安全管理保障能力的安全管理能力级，以及提供组织机构信息安全管理保障内容的管理保障控制类要求。本部分适用于涉及信息系统安全管理工作的组织机构的所有用户、开发者和评估者。
14.	GB/T 20274.4-2008	信息安全技术 信息系统安全保障评估框架 第4部分：工程保障		2008-07-18	2008-12-01	本部分建立了信息系统安全技术保障的框架，确立了组织机构内的启动、实施、维护、评估和改进信息安全技术体系的指南和通用原则。GB/T 20274的本部分定义和说明了信息系统安全工程保障工作中反映组织机构信息安全工程保障能力级，以及组织机构信息安全工程保障内容的安全工程保障控制类要求。GB/T 20274的本部分适用于启动、实施、维护、评估和改进信息安全工程的组织机构和涉及信息系统安全工程工作的所有用户、开发人员和评估人员。

15.	GB/Z 20283-2006	信息安全技术 保护轮廓和安全目标的产生指南	ISO/IEC TR 15446:2004	2006-05-31	2006-12-01	本标准描述保护轮廓（PP）与安全目标（ST）中的内容及其各部分内容之间的相互关系的详细指南。 本标准给出PP与ST文档内容的概述、示例目录清单和目标用户最关心的内容，陈述了PP与ST之间的关系，以及PP与ST的开发编写过程。 本标准给出编写指南，它用来指导PP与ST的描述部分的编写，内容涵盖PP与ST的引言、针对用户和使用者的评估对象（TOE）描述以及针对 ST作者和TOE开发者的PP应用注释；给出了TOE安全环境的定义；规定了安全目的，选择IT安全要求组件，描述了GB/T 18336中定义的功能组件和保证组件的使用方法，以及非GB/T 18336定义的组件的使用方法；规定了 ST中TOE概要规范的编制方法和基本原理的编制方法；给出了复合 TOE的PP与ST的编制方法，复合TOE是由两个或多个TOE组成；指导安全功能包和保证包的构成方法。标准以附录的形式给出了指南的核查表、防火墙 PP与ST示例、数据库示例。 本标准适用于开发者、使用者、测评者等用来更规范地描述安全目标和安全要求。
16.	GB/Z 29830.1-2013	信息技术 安全技术 信息技术安全保障框架 第 1 部分：综述和框架	ISO/IEC TR 15443-1:2005	2013-11-12	2014-02-01	本部分的意图是，以一种能使递增地获得交付件安全功能确信度的方式，按照一般生存周期模型，介绍交付件的安全保障方法、联系及其分类。通过标识各种不同保障途径和保障阶段的框架，概述了一些所需要的基本概念和术语，以便理解并应用其中所涉及的保障方法。
17.	GB/Z 29830.2-2013	信息技术 安全技术 信息技术安全保障框架 第 2 部分：保障方法	ISO/IEC TR 15443-2:2005	2013-11-12	2014-02-01	本指导性技术文件的第2部分收集了一些保障方法，其中还包括一些对整体ICT安全具有作用但不是专对ICT安全的保障方法。第2部分概括了这些方法的目标，描述了它们的特征以及引用文件和标准等。

18.	GB/Z 29830.3-2013	信息技术 安全技术 信息技术安全保障框架 第 3 部分：保障方法分析	ISO/IEC TR 15443-3:2007	2013-11-12	2014-02-01	本部分的意图是，为保障机构选择合适类型的ICT（信息通信技术）保障方法提供指导，并为特定环境铺设分析特定保障方法的框架。本部分可使用户把特定保障需求和/或典型保障情况与一些可用的保障方法所提供的一般性表现特征相匹配。本部分的指导适用于具有安全需求的ICT产品和ICT系统的开发、实现及运行。
19.	GB/T 30270-2013	信息技术 安全技术 信息技术安全性评估方法	ISO/IEC 18045:2005	2013-12-31	2014-07-15	本标准描述了在采用ISO/IEC 15408《信息技术 安全技术 信息技术安全性评估准则》所定义的准则和评估证据进行评估时，评估者应执行的最小行为集，是ISO/IEC 15408的配套标准。
20.	GB/Z 30286-2013	信息安全技术 信息系统保护轮廓和信息系统安全目标产生指南		2013-12-31	2014-07-15	本指导性技术文件给出了编制信息系统保护轮廓（ISPP）和信息系统安全目标（ISST）的过程，为编写ISPP和ISST提供指导。 本指导性技术文件适用于应用GB/T 20274进行信息系统安全性保障评估的评估者和确认评估者行为的认证者、系统开发者等。
21.	GB/T 30279-2013	信息安全技术 安全漏洞等级划分指南		2013-12-31	2014-07-15	本标准规定了信息系统安全漏洞（简称漏洞）的等级划分要素和危害程度级别。 本标准适用于信息安全漏洞管理组织和信息安全漏洞发布机构对信息安全漏洞危害程度的评估和认定，适用于信息安全产品生产、技术研发、系统运营等组织、机构在相关工作中参考。
22.	GB/T 31495.1-2015	信息安全技术 信息安全保障指标体系及评价方法 第1部分：概念和模型		2015-05-15	2016-01-01	GB/T 31495的本部分界定了信息安全保障评价的基本概念，确立了信息安全保障评价的一般模型。 本部分适用于信息安全保障评价工作。
23.	GB/T 31495.2-2015	信息安全技术 信息安全保障指标体系及评价方法 第2部分：指标体系		2015-05-15	2016-01-01	GB/T 31495的本部分规定了用于开展信息安全保障评价的指标及其释义。 本部分适用于信息安全保障评价工作。

24.	GB/T 31495.3-2015	信息安全技术　信息安全保障指标体系及评价方法　第3部分：实施指南		2015-05-15	2016-01-01	GB/T 31495的本部分规定了信息安全保障评价活动的实施指南。 本部分适用于信息安全保障评价工作。
3、管理基础						
序号	标准编号	标准名称	对应国际标准	发布日期	实施日期	范围
25.	GB/T 22080-2016	信息技术　安全技术　信息安全管理体系　要求	ISO/IEC 27001:2005	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的要求。本标准还包括了根据组织需求所剪裁的信息安全风险评估和处置的要求。 本标准规定的要求是通用的，适用于各种类型、规模或性质的组织。当组织声称符合本标准时，不能排除第4章到第10章中所规定的任何要求。
26.	GB/T 25067-2016	信息技术　安全技术　信息安全管理体系　审核和认证机构要求	ISO/IEC 27006:2007	2016-10-13	2017-05-01	本标准对信息安全管理体系（以下简称ISMS）审核和认证的机构规定了要求并提供了指南，以作为对ISO/IEC 17021：2011和GB/T 22080-2008中相关要求的补充。本标准的主要目的是为提供ISMS认证的认证机构的认可提供支持。 任何提供ISMS认证的机构需要在能力和可靠性方面证实其满足本标准的要求。本标准的指南为这些要求提供了进一步的解释。
27.	GB/T 22239-2008	信息安全技术 信息系统安全等级保护基本要求		2008-06-19	2008-11-01	本标准规定了不同安全保护等级信息系统的基本保护要求，包括基本技术要求和基本管理要求，适用于指导分等级的信息系统的安全建设和监督管理。
28.	GB/T 22240-2008	信息安全技术 信息系统安全等级保护定级指南		2008-06-19	2008-11-01	本标准规定了信息系统安全等级保护的定级方法，适用于为信息系统安全等级保护的定级工作提供指导。

29.	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GB17859-1999《计算机信息系统安全保护等级划分准则》划分的五个安全保护等级，规定了信息系统安全所需要的各个安全等级的管理要求。本标准详细给出了信息系统安全管理要素及其强度，包括策略和制度、机构和人员管理、风险管理、环境和资源管理、运行和维护管理、业务连续性管理、监督和检查管理、生存周期管理；信息系统安全管理分等级的各种要求，它有利于对安全管理的实施、评估和检查。本标准适用于相关组织机构（部门）按等级化要求进行的信息系统安全的管理。
30.	GB/T 28453-2012	信息安全技术 信息系统安全管理评估要求		2012-06-29	2012-10-01	本标准依据GB/T 20269-2006规定的信息系统分等级安全管理要求，从信息系统生存周期的不同阶段，规定了对信息系统进行安全管理评估的原则和模式、组织和活动、方法和实施，提出了信息安全等级保护第一级到第五级的信息系统安全管理评估的要求。本标准适用于相关组织机构（部门）对信息系统实施安全等级保护所进行的安全管理评估与自评估，以及评估者和被评估者对评估的管理。
31.	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	本标准规定了信息系统安全工程（以下简称安全工程）的管理要求，是对信息系统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，各方可以此为依据建立安全工程管理体系。 本标准按照GB 17859-1999划分的五个安全保护等级，规定了信息系统安全工程管理的不同要求。
32.	GB/T 22081-2016	信息技术 安全技术 信息安全控制实践指南	ISO/IEC 27002:2005	2016-08-29	2017-03-01	本标准为组织的信息安全标准和信息安全管理实践提供了指南，包括考虑了组织信息安全风险环境的控制的选择、实现和管理。本标准被设计用于组织： a) 选择控制，即基于GB/T 22080[10]，在实现一个信息安全管理体系的过程中选择控制；b) 实现通用的、可接受的信息安全控制；c) 制定组织自己的信息安全管理指南。

33.	GB/T 28450-2012	信息安全技术 信息安全管理体系审核指南		2012-06-29	2012-10-01	本标准在GB/T19011-2003的基础上为信息安全管理体系（简称ISMS）的审核原则、审核方案管理和审核实施提供了指导，并对审核员的能力及其评价提供了指导。 本标准适用于需要实施ISMS内部审核、外部审核或对审核进行管理的所有组织。
34.	GB/T 31496-2015	信息技术 安全技术 信息安全管理体系实施指南	ISO/IEC 27003:2010	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）所需要的关键方面。本标准描述了ISMS规范及其设计的过程，从开始到产生实施计划。本标准为实施ISMS描述了获得管理者批准的过程，为实施ISMS定义了一个项目（本标准称作ISMS项目），并就如何规划该ISMS项目提供了相应的指导，产生最终的ISMS项目实施计划。 本标准可供实施一个ISMS的组织使用，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）。每个组织的复杂性和风险都是独特的，并且其特定的要求将驱动ISMS的实施。小型组织将发现，本标准中所提及的活动可适用于他们，并可进行简化。大型组织或复杂的组织可能会发现，为了有效地管理本标准中的活动，需要层次化的组织架构或管理体系。然而，无论是大型组织还是小型组织，都可应用本标准来规划相关的活动。 本标准提出了一些建议及其说明，但并没有规定任何要求。期望把本标准与GB/T 22080-2008和GB/T 22081-2008一起使用，但不期望修改和/或降低GB/T 22080-2008中所规定的要求，或修改和/或降低GB/T 22081-2008所提供的建议。因此，不宜声称符合这一标准。

35.	GB/T 31497-2015	信息技术　安全技术　信息安全管理　测量	ISO/IEC 27004:2009	2015-05-15	2016-01-01	为了评估按照GB/T 22080-2008规定实施的信息安全管理体系（Information Security Management System，简称ISMS）和控制措施或控制措施组的有效性，本标准提供了如何编制测度和测量以及如何使用的指南。 本标准适用于各种类型和规模的组织。
36.	GB/T 31722-2015	信息技术　安全技术　信息安全风险管理	ISO/IEC 27005:2008	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。知晓GB/T 22080和GB/T 22081中所描述的概念、模型、过程和术语,对于完整地理解本标准是重要的。本标准适用于各种类型的组织(例如,商务企业、政府机构、非盈利性组织),这些组织期望管理可能危及其信息安全的风险。
37.	GB/Z 32916-2016	信息技术　安全技术　信息安全控制措施审核员指南		2016-08-29	2017-03-01	本指导性技术文件为评审控制措施的实现和运行提供指南，包括对信息系统控制措施的技术符合性检查，以符合组织所建立的信息安全标准。
38.	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。

4、物理安全

序号	标准编号	标准名称	对应国际标准	发布日期	实施日期	范围
39.	GB/T 9361-2011	计算机场地安全要求		2011-12-30	2012-05-01	本标准规定了计算站场地的安全要求，适用于各类地面计算站，不建站的地面计算机机房，按本标准对计算机机房的有关要求执行，改建的计算机机房参照本标准执行，非地面计算机机房参照本标准执行。

40.	GB/T 2887-2011	计算机场地通用规范		2011-07-29	2011-11-01	本标准规定了电子计算机场地定义、要求、测试方法与验收规则。 本标准适用于各类电子计算机系统的场地，其他电子设备系统的场地可参照本标准执行。
41.	GB 50174-1993	电子计算机机房设计规范		1993-02-17	1993-09-01	本标准适用于陆地上新建、改建和扩建的主机房建筑面积大于或等于140平方米的电子计算机机房的设计。本标准不适用于工业控制用计算机机房和微型计算机机房。
42.	GB 4943.1-2011	信息技术 设备 安全 第1部分：通用要求	IEC 60950:1999	2011-12-30	2012-12-01	本标准规定了信息技术设备涉及人员（含使用人员、维修人员，以及其他人员，如参观人员、卫生打扫人员等）安全的各种有关要求。本标准适用于电网电源供电的或电池供电的、额定电压不超过600V的信息技术设备，包括电气事务设备和与之相关的设备。 本标准所指的安全是各种危险有可能造成的伤害和危害，这些危险包括电击、与能量有关的危险、着火、与热有关的危险、机械危险、辐射和化学危险。 本标准首先给出了安全的总则，包括一般要求、试验的一般条件、元器件、电源接口、标记和说明；然后详细规定了危险的防护，包括电击和能量危险的防护、安全特低电压电路、通信网络电压电路、限流电路、受限制电路、接地和连接保护措施、一次性电路过流保护和接地故障保护、安全联锁装置、电气绝缘、电气间隙和爬电及绝缘穿透距离；布线、连接和供电，包括一般要求、与交流电网电源的连接、外部导线用的接线端子、交流电网电源的断接、设备的互连；结构要求，包括稳定性、机械强度、结构设计、危险运动件的防护、发热要求、外壳的开孔、防火；电气要求和模拟异常条件，包括接触电流和保护导体电流、抗电强度、异常工作和故障条件；与通信网络的连接，包括对通信网络的维修人员和有关设备的使用人员受设备危害的防护、对设备使用人员受来自网络上过电压的防护、通信配线系统的过热保护。

43.	GB/T 21052-2007	信息安全技术 信息系统物理安全技术要求		2007-08-23	2008-01-01	本标准规定按照计算机信息系统物理安全等级划分所需的检验试验的技术要求。 本标准适用于对计算机信息系统物理安全等级划分，适用于计算机信息系统物理安全的试验、检测、设计、施工、及相关产品的采购。
5、安全模型						
序号	标准编号	标准名称	对应国际标准	发布日期	实施日期	范围
44.	GB/T 17965-2000	信息技术 开放系统互连 高层安全模型	ISO/IEC 10745:1995	2000-01-03	2000-08-01	本标准定义一个体系结构模型，以此为基础：开发OSI高层独立于应用的安全服务和协议；利用这些服务和协议满足各种应用的安全要求，以便使包含内部安全服务的应用特定的ASE的需求量最少。 本标准特别规定：OSI 高层中通信的安全，高层中对开放系统 OSI 安全体系结构和安全框架中定义的安全服务的支持，根据 GB/T 9387.2 和 GB/T17176 高层中安全服务和机制的放置及其之间的关系，提供和使用安全服务时，高层之间的交互及高层和低层之间的交互，高层中管理安全信息的要求。在访问控制方面，本标准的范围包括控制访问 OSI 资源和通过 OSI 可接近的资源的服务和机制。
45.	GB/T 18237.1-2000	信息技术 开放系统互连 通用高层安全 第1部分：概述、模型和记法	ISO/IEC 11586-1:1996	2000-10-17	2001-08-01	本部分定义了如下内容：1、基于 OSI 高层安全模型（GB/T17965）中描述的概念的安全交换协议功能和安全变换的通用模型；2、一组记法工具，这组工具支持抽象语法规范中的选择字段保护需求的规范，并支持安全交换和安全变换规范；3、由本系列标准包含的通用高层安全设施的应用方面的一组信息性指南。

46.	GB/T 18237.2-2000	信息技术　开放系统互连　通用高层安全第2部分：安全交换服务元素（SESE）服务定义	ISO/IEC 11586-2:1996	2000-10-17	2001-08-01	本部分定义了由安全交换服务元素（SESE）提供的服务。该SESE是一个允许安全信息通信以支持在应用层内提供安全服务的ASE。
47.	GB/T 18237.3-2000	信息技术　开放系统互连　通用高层安全第3部分：安全交换服务元素（SESE）协议规范	ISO/IEC 11586-3:1996	2000-10-17	2001-08-01	本部分定义了由安全交换服务元素（SESE）提供的协议。该SESE是一个允许安全信息通信以支持在应用层内提供安全服务的ASE。
48.	GB/T 18237.4-2003	信息技术　开放系统互连　通用高层安全第4部分：保护传送语法规范	ISO/IEC 11586-4:1996	2000-10-17	2001-08-01	本部分定义了保护传送语法，也就是使用安全变换的传送语法，这种语法与用来支持应用层中的安全服务的表示有关。本部分详细规定了有关服务的概念，包括服务措施、下层服务的用法；各种规程元素，包括使用的应用协议数据单元（APDU）、传送规程、用户发起型夭折规程、提供者发起型夭折规程；SESE APDU的结构和编码，包括通用的APDU规范和抽象语法的构造方法；到下层服务的映射，主要是到ACSE服务的映射；一致性要求。
49.	GB/T 18231-2000	信息技术　低层安全	ISO/IEC TR 13594:1995	2000-10-17	2001-08-01	本标准描述了在OSI参考模型低层（运输、网络、数据链路和物理层）中提供安全服务的跨层的内容，包括1、基于GB/T9387.2中定义的低层公共的体系结构概念；2、低层协议之间与安全有关的交互作用的基础；3、OSI的低层与高层之间与安全有关的任何交互作用的基础；4、与其他低层安全协议有关的安全协议的放置以及这种放置的有关作用。在低层安全协议和本标准中描述的模型之间不应该存在冲突。
50.	GB/T 17963-2000	信息技术　开放系统互连　网络层安全协议	ISO/IEC 11577:1995	2000-01-13	2004-10-14	本标准规定的协议将由端系统和中间系统使用，以在网络层提供安全服务，而网络层由GB/T15126和GB/T15274定义。本标准中定义的协议称为网络层安全协议（NLSP）。

6、安全体系结构						
序号	标准编号	标准名称	对应国际标准	发布日期	实施日期	范围
51.	GB/T 9387.2-1995	信息处理系统　开放系统互连　基本参考模型　第2部分：安全体系结构	ISO 7498-2:1989	1995-06-02	1996-02-01	本标准描述了安全服务、特定的普遍性的安全机制，以及安全服务与安全机制之间的关系。详细规定了安全服务和安全机制与OSI各层之间的关系；安全服务和安全机制的配置，并分别规定了物理层、数据链路层、网络层、运输层、会话层、表示层和应用层的服务和机制；安全管理，包括OSI安全管理的分类（含系统安全、安全服务和安全机制管理）、特定的系统安全管理活动、安全机制的管理功能。
52.	GB/T 16264.8-2005	信息技术 开放系统互连 目录 第8部分：公钥和属性证书框架	ISO/IEC 9594-8: 2001	2005-05-25	2005-12-01	本部分描述了一套作为所有安全服务基础的框架，并规定了在鉴别及其它服务方面的安全要求。
53.	GB/T 18794.1-2002	信息技术　开放系统互连开放系统安全框架 第1部分:概述	ISO 10181-1:1996	2002-07-18	2002-12-01	本部分主要描述了安全框架的整体组织，定义了多个安全框架中所需要的安全概念，描述在框架的其他部分中所标识的服务和机制的相互关系。本部分详细规定了安全框架系列标准的组成及其主要内容；安全框架共同的基本概念，包括安全信息、安全域、具有安全服务的安全政策、可信实体、可信、可信第三方；通用安全信息，包括安全标签、密码校验值、安全证书、安全权标；通用安全设施，包括与管理相关的设施和与操作相关的设施；安全机制间的交互；拒绝服务的可用性。

54.	GB/T 18794.2-2002	信息技术　开放系统互连 开放系统安全框架 第2部分:鉴别框架	ISO 10181-2:1996	2002-07-18	2002-12-01	本部分定义了鉴别服务的一般框架，包括定义鉴别的基本概念、确定可能的鉴别机制类、定义用于这些鉴别机制类的服务、确定为支持这些鉴别机制类的协议的功能需求、确定鉴别的通用管理需求。 本部分给出了有关鉴别的各种描述，包括鉴别的基本概念、鉴别服务的有关内容、用于鉴别的原则、鉴别的 9 个阶段、可信第三方的参与、主角类型、人类用户鉴别、鉴别攻击类型；详细规定了鉴别信息和设施；鉴别机制特征，包括对称/非对称、使用密码/非密码技术、鉴别的类型；鉴别机制，包括依脆弱性分类（共分为 5 个级）、鉴别证书的作用、双向鉴别、等级特征、依配置分类（分为 2 种）；与其他安全服务/机制交互，包括访问控制、数据完整性、数据保密性、抗抵赖、审计。
55.	GB/T 18794.3-2003	信息技术　开放系统互连 开放系统安全框架　第3部分:访问控制框架	ISO 10181-3:1996	2003-01-01	2004-08-01	本部分首先给出了访问控制的一般性论述，包括访问控制的目标、基本内容、访问控制组件的分布、对访问控制的威胁；详细规定了访问控制策略，包括访问控制策略的表示和管理、粒度和容量、继承原则和优先原则、策略映射；访问控制信息和设施；访问控制机制的分类，包括访问控制列表方案、权力方案、基于标签的方案、基于上下文；与其他安全服务和机制的交互，包括鉴别、数据完整性、数据机密性、审计、其他与访问相关的服务。标准以附录的形式给出了组件间访问控制证书的交换、在OSI参考模型（仅在第3、4、7层）中的访问控制、访问控制身份的非惟一性、访问控制组件的分布、基于规则策略与基于身份策略的区别等。
56.	GB/T 18794.4-2003	信息技术　开放系统互连开放系统安全框架　第4部分:抗抵赖框架	ISO 10181-4:1997	2003-11-24	2004-08-01	本部分定义了抗抵赖的基本概念，定义通用的抗抵赖服务，确定提供抗抵赖服务的可能的机制，确定抗抵赖服务和机制的通用管理需求。

57.	GB/T 18794.5-2003	信息技术　开放系统互连开放系统安全框架　第5部分：机密性框架	ISO 10181-5:1996	2003-11-24	2004-08-01	本部分定义了机密性的基本概念，识别可能的机密性机制类型，对每种机密性机制的设施进行分类和识别，识别用来支持各种类别的机密性机制所需的管理，阐述机密性机制和支持服务与其他安全服务和机制的交互。许多不同类型的标准能使用这个框架，其中包括，体现机密性概念的标准；规定含有机密性的抽象服务的标准；规定使用机密性服务的标准；规定在开放系统体系结构内机密性服务的提供方法的标准，规定机密性机制的标准。
58.	GB/T 18794.6-2003	信息技术　开放系统互连开放系统安全框架　第6部分：完整性框架	ISO 10181-6:1996	2003-11-24	2004-08-01	本部分定义了数据完整性的基本概念；识别可能的完整性机制分类，识别每一类完整性机制的设施，识别支持完整性机制分类所需的管理；阐述完整性机制和支持服务与其他安全服务和机制的交互。许多不同类型的标准能使用这个框架，其中包括，体现完整性概念的标准；规定含有完整性的抽象服务的标准；规定使用完整性服务的标准；规定在开放系统体系结构内完整性服务的提供方法的标准，规定完整性机制的标准。 本部分论述的完整性是通过数据值的不变性来定义的。
59.	GB/T 18794.7-2003	信息技术　开放系统互连开放系统安全框架　第7部分：安全审计和报警框架	ISO 10181-7:1996	2003-11-24	2004-08-01	本部分定义了安全审计和报警的基本概念，为安全审计和报警提供一个通用的模型，识别安全审计和报警服务与其他安全服务的关系。和其他安全服务一样，安全审计只能在规定的安全策略范围内提供。许多不同类型的标准能使用这个框架，其中包括，体现审计和报警概念的标准；规定含有审计和报警的抽象服务的标准；规定使用审计和报警的标准；规定在开放系统体系结构内提供审计和报警方法的标准，规定审计和报警机制的标准。

60.	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	本标准规定了可信连接架构的层次、实体、部件、接口、实现流程、评估、隔离和修补以及各个接口的具体实现，解决终端连接到网络的双向用户身份鉴别和平台鉴别问题，实现终端连接到网络的可信网络连接。 本标准适用于具有可信平台控制模块的终端与网络的可信网络连接。 本标准不适用于完全点对点的网络环境。
61.	GB/T 31502-2015	信息安全技术 电子支付系统安全保护框架		2015-05-15	2016-01-01	本标准在给出电子支付系统模型的基础上，为公共类电子支付系统的信息安全提供了一个公共框架，主要包括安全问题定义、安全目的、安全功能需求和安全保障需求。 本标准适用于安全构建、运行公共类电子支付系统。

二、 技术与机制标准

1、密码技术						
序号	标准编号	标准名称	对应国际标准	发布日期	实施日期	范围
62.	GB/T 15277-1994	信息处理 信息技术安全技术 N位块密码算法的操作方式	ISO/IEC 10116:1997	1994-12-07	1995-08-01	本标准描述了采用秘密密钥的任意一种64bit分组密码算法的四种工作方式。
63.	GB/T 15278-1994	信息处理 数据加密物理层互操作性要求		1994-12-07	1995-08-01	本标准适用于在数据通信物理层中加密ADP信息的系统。本标准规定了适用于使用各种加密算法的要求。本标准规定了同步操作的两种可选方式：延迟选项和立即选项。这两种方式互不兼容。本标准还规定了对异步操作中断(BREAK)的两种可选动作：A类和B类。这两种动作互不兼容。
64.	GB/T 18238.1-2000	信息技术 安全技术 散列函数 第1部分：概述	ISO/IEC 10118-1:1994	2000-10-17	2001-08-01	本部分规定了散列函数，它可用于提供鉴别、完整性和抗抵赖服务。本部分包含GB/T 18238各个部分所共用的定义、符号、缩略语和要求。
65.	GB/T 18238.2-2002	信息技术 安全技术 散列函数 第2部分：使用n位块密码的散列函数	ISO/IEC 10118-2:2000	2002-07-18	2002-12-01	本部分规定了采用n位块密码算法的散列函数,这些函数适合于已实现这样一个算法的环境。 本部分规定了四种散列函数。第一种提供了长度小于或者等于n的散列代码，其中n是采用算法的块长度。第二种提供了长度小于或者等于2n的散列代码。第三种提供了长度等于2n的散列代码。第四种提供了长度等于3n的散列代码。 本部分规定的全部四种散列函数符合ISO/IEC 10118-1中规定的通用模型。
66.	GB/T 18238.3-2002	信息技术 安全技术	ISO/IEC 10118-3:2004	2002-07-18	2002-12-01	本部分规定了专用散列函数，即专门设计的散列函数。本标准的散列

		散列函数 第3部分：专用散列函数				函数基于循环函数的迭代使用。本标部分规定了三种不同的循环函数，从而产生了不同的专用散列函数。第一种和第三种提供了长度达160位的散列码，第二提供了长度达128位的散列码。
67.	GB/T 15852.1-2008	信息技术 安全技术 消息鉴别码 第1部分：采用分组密码的机制	ISO/IEC 9797-1:1999	2008-07-02	2008-12-01	本部分规定了一种使用密钥和n比特块密码算法计算m比特码校验值的方法。本部分适用于任何安全体系结构、进程或应用的安全服务。
68.	GB/T 17964-2008	信息安全技术 分组密码算法的工作模式	ISO/IEC 10116:1997	2008-6-26	2008-11-01	本标准描述了分组密码算法的其中工作模式，以便规范分组密码的使用。
69.	GB/T 17901.1-1999	信息技术 安全技术 密钥管理 第1部分:框架		1999-01-31	2000-05-01	本标准：1)确定密钥管理的目标；2)描述作为密钥管理机制基础的一般模型；3)定义对GB/T 17901所有部分通用的密钥管理基本概念；4)定义密钥管理服务；5)确定密钥管理机制的特性；6)规定对密钥材料在其生存期内进行管理的需求；7)描述对密钥材料在其生存期内进行管理的框架。本框架定义了与任何特定密码算法的使用无关的密钥管理一般模型，但是某些密钥分发机制可能与特定的算法特性(如非对称算法的特性)有关。
70.	GB/T 32905-2016	信息安全技术 SM3密码杂凑算法		2016-08-29	2017-03-01	本标准规定了SM3密码杂凑算法的计算方法和计算步骤，并给出了运算示例。本标准适用于商用密码应用中的数字签名和验证、消息认证码的生成与验证以及随机数的生成，可满足多种密码应用的安全需求。
71.	GB/T 32907-2016	信息安全技术 SM4分组密码算法		2016-08-29	2107-03-01	本标准规定了SM4分组密码算法的算法结构和算法描述，并给出了运算示例。本标准适用于商用密码产品中分组密码算法的实现、检测和应用。
72.	GB/T 32915- 2016	信息安全技术 二元序列随机性检测方法		2016-08-29	2107-03-01	本标准规定了商用密码应用中的随机性检测指标和检测方法。本标准适用于对随机数发生器产生的二元序列的随机性检测。
73.	GB/T 32918.1-2016	信息安全技术 SM2椭圆曲线公钥密码算法		2016-08-29	2107-03-01	本部分给出了SM2椭圆曲线公钥密码算法涉及的必要数学基础知识与相关密码技术，以帮助实现其它各部分所规定的密码机制。本部分适

		第1部分：总则				用于基域为素域和二元扩域的椭圆曲线公钥密码算法的设计、开发、使用。
74.	GB/T 32918.2-2016	信息安全技术 SM2椭圆曲线公钥密码算法 第2部分：数字签名算法		2016-08-29	2107-03-01	本部分规定了SM2椭圆曲线公钥密码算法的数字签名算法，包括数字签名生成算法和验证算法，并给出了数字签名与验证示例及其相应的流程。本部分适用于商用密码应用中的数字签名和验证，可满足多种密码应用中的身份鉴别和数据完整性、真实性的安全需求。
75.	GB/T 32918.3-2016	信息安全技术 SM2椭圆曲线公钥密码算法 第3部分：密钥交换协议		2016-08-29	2107-03-01	本部分规定了SM2椭圆曲线公钥密码算法的密钥交换协议，并给出了密钥交换与验证示例及其相应的流程。本部分适用于商用密码应用中的密钥交换，可满足通信双方经过两次或可选三次信息传递过程，计算获取一个由双方共同决定的共享秘密密钥（会话密钥）。
76.	GB/T 32918.4-2016	信息安全技术 SM2椭圆曲线公钥密码算法 第4部分：公钥加密算法		2016-08-29	2107-03-01	本部分规定了SM2椭圆曲线公钥密码算法的公钥加密算法，并给出了消息加解密示例和相应的流程。本部分适用于商用密码应用中的消息加解密，消息发送者可以利用接收者的公钥对消息进行加密，接收者用对应的私钥进行解密，获取消息。
77.	GB/T 33133.1-2016	信息安全技术 祖冲之序列密码算法 第1部分：算法描述		2016-10-13	2017-05-01	本部分给出了祖冲之序列密码算法的一般结构，基于该结构可实现本标准其它各部分所规定的密码机制。本部分适用于祖冲之序列密码算法相关产品的研制、检测和使用,可应用于涉及非国家秘密范畴的商业应用领域。
2、鉴别机制						
序号	标准编号	标准名称	对应国际标准	发布日期	实施日期	范围
78.	GB/T 15843.1-2008	信息技术　安全技术　实体鉴别　第1部分:概述	ISO/IEC 9798-1:1997	2008-06-19	2008-11-01	本部分规定了采用安全技术的实体鉴别机制的鉴别模型及一般要求和限制。
79.	GB/T 15843.2-2008	信息技术　安全技术	ISO/IEC 9798-2:1999	2008-06-19	2008-11-01	本部分规定了采用对称加密算法的实体鉴别机制。其中有四种是两个

		实体鉴别　第2部分：采用对称加密算法的机制				实体间无可信第三方参与的鉴别机制，而这四种机制中有两种是单个实体鉴别（单向鉴别），另两种是两个实体相互鉴别。其余的机制都要求有一个可信第三方参与，以便建立公共秘密密钥，实现相互或单向的实体鉴别。本部分中规定的机制采用诸如时间戳、序号或随机数等时变参数，防止先前有效的鉴别信息以后又被接受或者被多次接受。
80.	GB/T 15843.3-2016	信息技术　安全技术　实体鉴别　第3部分：采用数字签名技术的机制	ISO/IEC 9798-3:1998	2016-04-25	2016-11-01	本部分规定了采用数字签名技术的实体鉴别机制。有两种鉴别机制是单个实体的鉴别（单向鉴别），其余的是两个实体的相互鉴别机制。本部分中规定的机制采用诸如时间戳、序号或随机数等时变参数，防止先前有效的鉴别信息以后又被接受或者被多次接受。如果采用时间戳或序号，则单向鉴别只需一次传递，而相互鉴别则需两次传递。如果采用使用随机数的激励-响应方法，单向鉴别需两次传递，相互鉴别则需三次或四次传递（依赖于所采用的机制）。
81.	GB/T 15843.4-2008	信息技术　安全技术　实体鉴别　第4部分：采用密码校验函数的机制	ISO/IEC 9798-4:1999	2008-06-09	2008-11-01	本部分规定了采用密码校验函数的实体鉴别机制。
82.	GB/T 15843.5-2005	信息技术　安全技术　实体鉴别　第5部分：采用零知识技术的机制	ISO/IEC 9798-5:1999	2005-04-19	2005-10-01	本部分规定了采用零知识技术的实体鉴别机制。
83.	GB/T 15852.1-2008	信息技术　安全技术　消息鉴别码　第1部分：采用分组密码的机制	ISO/IEC 9797-1:1999	2008-07-02	2008-12-01	本部分规定了一种使用密钥和n比特块密码算法计算m比特码校验值的方法。本标准适用于任何安全体系结构、进程或应用的安全服务。
84.	GB/T 17903.1-2008	信息技术　安全技术	ISO/IEC 13888-1:2004	2008-06-26	2008-11-01	本部分描述了基于密码技术提供证据的抗抵赖机制的一种模型，并且

		抗抵赖　第1部分：概述				描述了如何使用对称或非对称密码技术生成密码校验值并以此形成证据
85.	GB/T 17903.2-2008	信息技术　安全技术　抗抵赖　第2部分：使用对称技术的机制	ISO/IEC 13888-2:1998	2008-06-26	2008-11-01	本部分描述了可用于抗抵赖服务的通用结构，以及能用来提供原发抗抵赖(NRO)、交付抗抵赖(NRD)、提交抗抵赖(NRS)和传输抗抵赖(NRT)等有关的特殊通信机制。其他抗抵赖服务可用第8章所描述的通用结构组成，以满足安全策略的要求。
86.	GB/T 17903.3-2008	信息技术　安全技术　抗抵赖　第3部分：使用非对称技术的机制	ISO/IEC 13888-3:1998	2008-07-02	2008-12-01	本部分规定了使用非对称技术提供与通信有关的特殊抗抵赖服务的机制。抗抵赖机制可以提供以下四种抗抵赖服务：a)原发抗抵赖；b)交付抗抵赖；c)提交抗抵赖；d)传输抗抵赖。抗抵赖机制涉及专用于每种抗抵赖服务的抗抵赖权标交换。抗抵赖权标由数字签名和附加数据组成。抗抵赖权标可做为抗抵赖信息予以存储，发生争议是由争议双方顺序使用。
87.	GB/T 28455-2012	信息安全技术 引入可信第三方的实体鉴别及接入架构规范		2012-06-29	2012-10-01	本标准规定了引入可信第三方的实体鉴别及接入架构的一般方法。包括：a) 引入可信第三方的实体鉴别及接入架构的框架；b) 引入可信第三方的实体鉴别及接入架构的基本原理；c) 定义引入可信第三方的实体鉴别及接入架构的不同级别以及相应收发数据时的端口的行为；d) 定义引入可信第三方的实体鉴别及接入架构的参与实体间的消息交互协议；e) 定义使用消息交互协议完成引入可信第三方的实体鉴别及接入架构的过程；f) 规定协议交互消息中的数据编码；g) 建立引入可信第三方的实体鉴别及接入架构管理的需求，识别管理对象，定义管理操作；h) 描述远程管理者利用简单网络管理协议（SNMP）所能进行的管理操作；i) 描述符合本文件的设备应满足的需求，见附录A。 本标准适用于无线网络访问控制、有线网络访问控制和IP网络访问控制系统等。
88.	GB/T 15852.2-2012	信息技术 安全技术 消息鉴别码 第2部分：采	ISO/IEC 9797-2: 2002	2012-12-31	2013-06-01	GB/T 15852的本部分规定了三种采用专用杂凑函数的消息鉴别码算法。这些消息鉴别码算法可用作数据完整性检验,检验数据是否被非授

		用专用杂凑函数的机制				权地改变。同样这些消息鉴别码算法也可用作消息鉴别,保证消息源的合法性。数据完整性和消息鉴别的强度依赖于密钥的长度及其保密性、杂凑函数的算法强度及其输出长度、消息鉴别码的长度和具体的消息鉴别码算法。 本部分适用于任何安全体系结构、进程或应用的安全服务。
89.	GB/T 29242-2012	信息安全技术 鉴别与授权 安全断言标记语言		2012-12-31	2013-06-01	本标准定义了一系列遵从XML编码格式的关于安全断言的语法、语义规范、系统实体间传递和处理SAML断言的协议集合和SAML系统管理相关的处理规则。本标准适用于在互联网跨安全域应用场景中,身份鉴别,认证与授权服务的开发、测试、评估和采购。
90.	GB/T 30275-2013	信息安全技术 鉴别与授权 认证中间件框架与接口规范		2013-12-31	2014-07-15	本标准规范了认证中间件体系框架、组件、功能及通用接口，并给出了认证中间件的工作流程。 本标准适用于认证中间件及其组件的开发，并可指导对该类系统的检测及相关应用的开发。
3、授权机制						
序号	标准编号	标准名称	对应国际标准	发布日期	实施日期	范围
91.	GB/T 25062-2010	信息安全技术 鉴别与授权 基于角色的访问控制模型与管理规范		2010-09-02	2011-02-01	本标准规定了基于角色的访问控制（RBAC）模型、RBAC系统和管理功能规范。本标准适用于信息系统中RBAC子系统的设计与实现，相关系统的测试和产品采购亦可参照使用。
92.	GB/T 30281-2013	信息安全技术 鉴别与授权 可扩展访问控制标记语言规范		2013-12-31	2014-07-15	本标准规定了可扩展访问控制标记语言(XACML)的数据流模型、语言模型和语法。 本标准适用于大规模分布式应用中资源统一访问控制策略语言的编写与分析。
93.	GB/T 30280-2013	信息安全技术 鉴别与授权 地理空间可扩展访问控制置标语言		2013-12-31	2014-07-15	本标准给出了XACML策略语言的一种扩展，使其可以支持对地理信息访问权限约束的申明和执行。本标准定义了访问规则中几何数据类型必须依赖的几何模型， 不同几何数据类型的编码语言，几何体之间

						拓扑关系的测试函数，几何函数。本标准适用于地理信息服务场景中，地理信息保护和访问控制的定义与实施。
94.	GB/T 31501-2015	信息安全技术　鉴别与授权　授权应用程序判定接口规范		2015-05-15	2016-01-01	本标准定义了访问控制服务为授权应用提供的授权判定编程应用接口，并定义了与判定接口相关的数据结构和C语言形式的接口。本标准适用于访问控制服务中授权判定接口的设计和实现。
4、电子签名						
序号	标准编号	标准名称	对应国际标准	发布日期	实施日期	范围
95.	GB 15851-1995	信息技术　安全技术　带消息恢复的数字签名方案	ISO/IEC 9796:1991	1995-12-13	1996-08-01	本标准规定了对有限长消息使用公开密钥体制的带消息恢复的数字签名方案。这种数字签名方案包含下列两个进程:—签名进程，它使用秘密签名密钥和签名函数来对消息签名; —验证进程，它使用公开验证密钥和验证函数来验证签名，同时恢复出消息。签名进程中，必要时，欲签名的消息需填充和扩展，然后加上与消息本身有关的人为的冗余，对消息中是否存在自然的冗余不作假定这人为的冗余将由验证进程揭示出来，把这人为的冗余去掉便恢复出消息。本标准不规定密钥产生进程、签名函数和验证函数。附录A(提示的附录)给出了一个公开密钥体制的例子，包含密钥产生、签名函数和验证函数。附录B(提示的附录)通过例子来说明这些操作的各步。这个方案中的若干参数与安全性有关:本标准不规定为要达到给定的安全性水平而对这些参数应取什么值。然而以这样一种方式规定，即在本标准使用中，如果这些参数中有的必须要改变时，使所作的改变最小。
96.	GB/T 17902.1-1999	信息技术　安全技术　带附录的数字签名第1部分：概述	ISO/IEC 14888-1:1998	1999-11-01	2000-05-01	本部分描述了带附录的数字签名的基本原则和要求以及该系列标准通用的定义和符号。它适用于带附录的数字签名方案。本标准适用于提供实体鉴别、数据原发鉴别、数据完整性和抗抵赖的方案。 本部分所规定的机制是基于非对称密码技术，所有非对称数字签名机

						制都涉及密钥对产生、密钥签名和验证密钥三个基本操作（进程）。标准给出了数字签名机制的一般模型，并对三个进程进行了详细规定，其中，密钥产生进程由产生域参数与产生签名密钥和验证密钥组成；对签名进程规定了数据项和验证过程，这些验证过程包括产生预签名、准备消息、计算证据、计算签名；对验证进程规定了数据项和验证过程，这些验证过程包括准备消息、检索证据、计算验证函数、验证证据；还规定了带两部分签名的随机化机制。
97.	GB/T17902.2-2005	信息技术　安全技术　带附录的数字签名　第2部分：基于身份的机制	ISO/IEC 14888-2:1999	2005-04-19	2005-10-01	本部分规定了任意长度消息的带附录的基于身份的数字签名机制的签名和验证过程的总的结构和基本过程。
98.	GB/T17902.3-2005	信息技术　安全技术　带附录的数字签名　第3部分：基于证书的机制	ISO/IEC 14888-3:1998	2005-04-19	2005-10-01	本部分规定了带附录的基于证书的数字签名机制。本部分提供了：1）基于证书的签名机制的一般描述，其安全性是基于所用交换群上的离散对数问题的困难性。2）基于证书的签名机制的一般描述，其安全机制是基于因子分解的困难性。3）使用任意长度消息的基于证书机制的带附录的各种常规数字签名机制。
99.	GB/T 25061-2010	信息安全技术 公钥基础设施 XML数字签名语法与处理规范		2010-09-02	2011-02-01	本标准规定了创建和表示XML数字签名的语法和处理规则。XML数字签名为任何类型的数据提供了完整性、消息鉴别和签名者鉴别服务。本标准适用于制作和处理XML数字签名的应用程序、系统或服务。
100.	GB/T 25064-2010	信息安全技术 公钥基础设施 电子签名格式规范		2010-09-02	2011-02-01	本标准针对基于公钥密码学生成的数字签名类型的电子签名，定义了电子签名与验证的主要参与方、电子签名的类型、验证和仲裁要求。本标准还规范了电子签名和数据格式，包括基本数据格式、验证数据格式、签名策略格式等。本标准适用于电子签名产品的设计和实现，同时相关产品的测试、评估和采购亦可参照使用。
101.	GB/T 25065-2010	信息安全技术 公钥基础设施 签名生成应用		2010-09-02	2011-02-01	本标准规定了产生可靠电子签名的签名生成应用程序（SAC）的安全要求，内容包括：定义一种签名生成环境的模型和签名生成应用程序

		程序的安全要求				的功能模型；规定适用于功能模型中所有功能模块的总体要求；规定签名生成应用程序中每个功能模块的安全要求，除了SSCD。
102.	GB/T 30274-2013	信息安全技术 公钥基础设施 电子签名卡应用接口测试规范		2013-12-31	2014-07-15	本标准规定了电子签名卡的测试环境、测试内容、测试方法，以及预期测试结果。本标准适用于规范和指导电子签名卡的测试，指导电子签名卡的开发和应用。
103.	GB/T 25057-2010	信息安全技术 公钥基础设施 电子签名卡应用接口基本要求		2010-09-02	2011-02-01	本标准规定了电子签名卡的基本命令报文和相应的响应报文，以及电子签名卡的文件组织结构。本标准适用于规范和指导电子签名卡的开发，规范与指导与电子签名卡进行通信，访问卡内文件，应用私钥生成电子签名的应用系统的开发。本标准不适用于在电子签名卡内创建文件或使用公钥的应用系统的开发。
104.	GB/T 31503-2015	信息安全技术 电子文档加密与签名消息语法		2015-05-15	2016-01-01	本标准规定了电子文档加密与签名消息语法，此语法可用于对任意消息内容进行数字签名、摘要、鉴别或加密。 本标准适用于电子商务和电子政务中电子文档加密与签名消息的产生、处理以及验证。
5、公钥基础设施						
序号	标准编号	标准名称	对应国际标准	发布日期	实施日期	范围
105.	GB/T 19714-2005	信息技术 安全技术 公钥基础设施 证书管理协议	IETF RFC 2510	2005-04-09	2005-10-01	本标准描述了公钥基础设施(PKI)中的证书管理协议，定义了与证书产生和管理相关的各方面所需要的协议消息，这些消息主要包括申请证书、撤销证书、密钥更新、密钥恢复、交叉认证等。本标准主要适用于在安全或不安全环境中实施PKI组件并实施管理，可作为PKI运营机构、PKI组件开发者的参考指南。
106.	GB/T 19713-2005	信息技术 安全技术 公钥基础设施 在线证书状态协议	IETF RFC 2560	2005-04-19	2005-10-01	本标准规定了一种无需请求证书撤销列表（CRL）即可查询数字证书状态的机制（即在线证书状态协议--OCSP）。该机制可代替CRL或作为周期性检查 CRL的一种补充方式，以便及时获得证书撤销状态的有

						关信息。本标准主要描述了以下内容：a）具体描述了在线证书状态协议的请求形式；b）具体描述了在线证书状态协议的响应形式；c）分析了处理在线证书状态协议响应时可能出现的各种异常情况；d）说明了在线证书状态协议基于超文本传输协议（HTTP）的应用方式；e）提供了采用抽象语法记法1（ASN.1）描述的在线证书状态协议。
107.	GB/T 19771-2005	信息技术 安全技术 公钥基础设施 PKI组件最小互操作规范		2005-05-25	2005-12-01	本标准支持大规模公钥基础设施（PKI负责发布、撤销和管理用于数字签名及密钥管理的公钥证书）的互操作性。本标准为不同的PKI开发者所开发的组件产品提供了基本的互操作性参考。
108.	GB/T 20518-2006	信息安全技术 公钥基础设施 数字证书格式		2006-08-30	2007-02-01	本标准规定了中国数字证书的基本结构，并对数字证书中的各数据项内容进行了描述；规定了一些标准的证书扩展域，并对每个扩展域的结构进行了定义，特别是增加了一些专门面向国内应用的扩充项。本标准详细规定了数字证书的各种格式，包括基本证书域的数据结构、TBSCertificate及其数据结构、各种证书扩展域及其数据结构；数字证书可支持的密码算法。标准以附录的形式给出了各种证书的结构、证书的结构实例、数字证书编码举例，以及算法举例。本标准适用于国内数字证书认证机构、数字证书认证系统的开发商以及基于数字证书的安全应用开发商。本标准主要根据IETF（互联网工程任务组）RFC 2459文件，并结合我国情况制定的。
109.	GB/T 20519-2006	信息安全技术 公钥基础设施 特定权限管理中心技术规范		2006-08-30	2007-02-01	本标准详细规定了特定权限管理中心架构，包括权限管理中心架构的内容、各逻辑层结构的组成、权限管理中心的管理结构；系统相关协议，包括代理点与属性注册机构之间、属性注册机构与属性授权机构（AA）之间、属性授权机构与认证机构源之间的通信协议，以及密码服务支持协议；各种证书的发布模式；PMI/AA的安全实施，包括证书撤消安全、算法强度安全、身份标识安全、LDAP服务访问安全、属性安全；PMI应用模型。标准以附录的形式给出了属性证书格式、系统相关协议应用实例、基于角色的属性管理模式。

						本标准适用于特定权限管理中心基础设施的设计、建设和检测；对于特殊需求的应用系统，可根据具体的业务需求和情况进行灵活配置。 本标准依据GB/T 20518-2006《信息安全技术 公钥基础设施 数字证书格式》，并结合我国相关规范制定的，它是GB/T 20518-2006的配套技术标准。
110.	GB/T 20520-2006	信息安全技术 公钥基础设施 时间戳规范		2006-08-30	2007-02-01	本标准规定了时间戳系统部件的组成、时间戳的管理、时间戳的格式和时间戳系统安全管理等方面的要求。 本标准还详细规定了时间戳的产生和颁发，包括时间戳申请和颁发的方式和过程、产生方法；时间戳管理包括时间戳的保存、备份、检索、删除和销毁、查看和验证；时间戳的格式包括对时间戳机构的要求、密钥标识、时间的表示格式、申请和响应消息格式等；时间戳系统的安全包括物理安全和软件安全。 本标准适用于时间戳系统的设计和实现，时间戳系统的测试和采购亦可参考使用。
111.	GB/T 21053-2007	信息安全技术 公钥基础设施 PKI系统安全等级保护技术要求		2007-08-23	2008-01-01	本标准参照GB17859-1999《计算机信息系统安全保护等级划分准则》的五个安全保护等级的划分，对PKI系统安全保护进行等级划分，规定了不同等级PKI系统所需要满足的评估内容。 本标准详细规定了PKI系统第一、二、三、四、五级的安全保护技术要求，包括上述各级的物理安全、角色与责任、访问控制、标识与鉴别、数据输入输出、密钥管理、轮廓管理、证书管理、配置管理、分发和操作、开发、指导性文档、生命周期支持、测试，以及审计、备份与恢复、脆弱性评定。标准以附录的形式给出了PKI系统安全要素各个要求级别的划分。 本标准适用于PKI的安全保护等级的评估，对于PKI系统安全功能的研制、开发、测试和产品采购亦可参照使用。
112.	GB/T 21054-2007	信息安全技术 公钥基		2007-08-23	2008-01-01	本标准依据GB/T 21054-2007《信息安全技术 公钥基础设施 PKI系统

		础设施 PKI系统安全等级保护评估准则				安全等级保护评估准则》的五个安全保护等级的划分，规定了不同等级PKI系统所需要安全技术要求。 本标准详细规定了PKI系统第一、二、三、四、五级的安全评阅内容，包括上述各级的物理安全、角色与责任、访问控制、标识与鉴别、数据输入输出、密钥管理、轮廓管理、证书管理，以及审计、备份与恢复。标准以附录的形式给出了PKI系统安全要素各个要求级别的划分。 本标准适用于PKI系统的设计和实现，对于PKI系统安全功能的研制、开发、测试和产品采购亦可参照使用。
113.	GB/T 25055-2010	信息安全技术 公钥基础设施安全支撑平台技术框架		2010-09-02	2011-02-01	本标准规定了基于公钥基础设施的安全支撑平台的技术框架。本标准适用于网络信息系统中安全支撑平台的设计、建设、检测、运营及管理，为网络信息系统和业务应用系统提供统一可信的软、硬件安全支撑服务。同时，本标准还可为安全产品生产商提供产品和技术的标准定位以及标准化的参考，指导安全产品生产商对安全支撑平台的设计和建设，提高安全产品的可信性与互操作性。对于特定的安全支撑平台的建设，可根据具体的业务需求和情况进行灵活配置。
114.	GB/T 25059-2010	信息安全技术 公钥基础设施 简易在线证书状态协议		2010-09-02	2011-02-01	本标准规定了一种简易在线证书状态协议-SOCSP。该协议可作为标准OCSP协议的补充。本标准描述了一下内容：a) 具体描述了简易在线证书状态协议的请求形式；b) 具体描述了简易在线证书协议的响应形式；c)分析了简易在线证书状态协议响应时可能出现的各种异常情况；d) 说明了简易在线证书状态协议基于超文本传输协议（HTTP）的应用方式。本标准适用于各类基于公开密钥基础设施的应用程序和计算环境。
115.	GB/T 25060-2010	信息安全技术 公钥基础设施 X.509数字证书应用接口规范		2010-09-02	2011-02-01	本标准定义了数字证书应用标识及一组证书应用接口。本标准适用于基于数字证书的安全中间件的设计和实现，对基于数字证书的安全功能的研制，开发、测试亦可参照使用。
116.	GB/T 26855-2011	信息安全技术 公钥基		2011-07-29	2011-11-01	本标准定义了证书策略（CP）和认证业务声明（CPS）的概念，解释

		础设施 证书策略与认证业务声明框架				二者之间的区别，并规定了CP和CPS应共同遵守的文档标题框架，包括在标题中所应包含的信息类型。本标准提出的框架一般假设使用GB/T16264.8-2005证书格式，但并不意味着此框架仅限于使用这种证书格式，也可用于其他格式的证书。 本标准适用于CP和CPS的撰写和比较。本标准所给出的框架应作为一个灵活的工具来使用，用以指明在特定的CP或CPS中所应考虑的主题，而不是作为生成CP或CPS的固定公式。 本标准不适用于通用安全策略的定义，如组织安全策略、系统安全策略或数据标记策略。
117.	GB/T 28447-2012	信息安全技术 电子认证服务机构运营管理规范		2012-06-29	2012-10-01	本标准规定了电子认证服务机构在业务运营、认证系统运行、物理环境与设施安全、组织与人员管理、文档、记录、与介质管理、业务连续性、审计与改进等多方面应遵循的要求。本标准适用于在开放互联环境中提供数字证书服务的电子认证服务机构的建设、管理及评估。对于在封闭环境中（如在特定团体或某个行业内）运行的电子认证服务机构可根据自身安全风险评估以及国家有关的法律法规有选择性的参考本标准。国家有关的测评机构、监管部门也可以将本标准作为测评和监管的依据。
118.	GB/T 29767-2013	信息安全技术 公钥基础设施 桥CA体系证书分级规范		2013-04-28	2014-05-01	本标准规定了桥CA体系证书安全等级划分。 本标准适用于桥CA体系证书策略的设计与实现。桥CA系统的研制、开放、测试和产品采购也可参照使用。
119.	GB/T 29243-2012	信息安全技术 数字证书代理认证路径构造和代理验证规范		2012-12-31	2013-06-01	本标准规定了数字证书代理认证路径构造和代理验证两种服务的概念和协议要求,以及满足协议要求的代理服务协议。 本标准适用于PKI系统运营机构的代理认证路径构造和代理验证服务的实现和应用。
120.	GB/T 30272-2013	信息安全技术 公钥基础设施 标准一致性测试评价指南		2013-12-31	2014-07-15	本标准规定了公钥基础设施相关组件的测试评价指南，涉及CA、RA、终端实体、证书资料库、时间戳子系统、特定权限管理子系统、在线证书状态查询子系统。

						本标准适用于按照国家标准：GB/T 19713-2005、GB/T 19714-2005、GB/T 19771-2005、GB/T 20518-2006、GB/T 20519-2006和GB/T 20520-2006，进行研制开发的产品类公钥基础设施相关组件的测试和评价。
121.	GB/T 30277-2013	信息安全技术 公钥基础设施 电子认证机构标识编码规范		2013-12-31	2014-07-15	本标准确立了电子认证机构标识代码编制规范的一般原则。 在基于PKI的应用系统中，统一的电子认证机构编码为建立全国性的CA目录查询提供了基础条件。 本标准提出了实现要求和编制规范，以满足PKI的安全互操作服务需求。
122.	GB/Z 19717-2005	基于多用途互联网邮件扩展（MIME）的安全报文交换		2005-04-19	2005-10-01	本指导性技术文件阐述了安全发送和接收基于多用途互联网邮件扩展（MIME）数据的基本方法。该方法基于广泛使用的多用途互联网邮件扩展协议（MIME），向各种Internet报文应用提供鉴别、报文的完整性、抗抵赖性、机密性等多种安全服务。传统的邮件用户代理使用该方法可以向所发送的报文增加各种加密服务，并能有效处理所收报文中的加密服务。本指导性技术文件还描述了S/MIME的增强安全服务。 本指导性技术文件不限于电子邮件，它还可以用于任何传输MIME数据的传输机制（如超文本传输协议，HTTP)。 该规范利用了MIME面向对象的特点，使得在各种传输系统中能够交换安全报文。
123.	GB/T 31504-2015	信息安全技术 鉴别与授权 数字身份信息服务框架规范		2015-05-15	2016-01-01	本标准定义了数字身份信息服务参考模型、XML Schema的框架、命名空间、扩展方式以及通用的数字身份信息对象属性类型，还定义了通用的数字身份信息创建、查询、修改和删除的交换信息格式以及处理规则。 本标准适用于数字身份信息服务的开发，并可指导对该类系统的检测及相关应用的开发。
124.	GB/T 31508-2015	信息安全技术 公钥基		2015-05-15	2016-01-01	本标准通过分类分级的方式，规范了用于商业交易、设备和公众服务

		础设施 数字证书策略分类分级规范				领域的电子认证服务中的8种数字证书策略。 本标准适用于我国电子商务和公众服务中所涉及的数字证书。
125.	GB/T 32213-2015	信息安全技术 公钥基础设施 远程口令鉴别与密钥建立规范		2015-12-10	2016-08-01	本标准定义了基于非对称密码技术实现远程口令鉴别与密钥建立的数学定义和协议构造。 本标准适用于采用基于口令鉴别与密钥建立技术的鉴别系统的设计和开发。
6、通信安全技术						
序号	标准编号	标准名称	对应国际标准	发布日期	实施日期	范围
126.	GB/T 21643-2008	IP认证头（AH）	IETF RFC 2402:1998,MOD	2008-04-10	2008-11-01	本标准规定了AH协议的技术要求，包括AH协议头格式、AH协议处理、一致性要求等。 本标准适用于支持AH协议的数据设备。
7、涉密系统通用技术要求						
序号	标准编号	标准名称	对应国际标准	发布日期	实施日期	范围
127.	BMB1-1994	电话机电磁泄漏发射限值和测试方法				本标准规定了电话机电磁泄漏辐射发射、传导发射的限值和测试方法。 本标准适用于党政专用电话网使用的有线电话机（不包括无绳电话机、数字电话机），适用于需要保密通信的电话机。
128.	BMB5-2000	涉密信息设备使用现场的电磁泄漏发射防护要求				本标准规定了对涉密信息系统的设备选用、使用环境和工程安装等防护要求。本标准适用于涉密信息设备使用现场的电磁泄漏发射防护。
129.	BMB6-2001	密码设备电磁泄漏发射限值				本标准规定了密码设备电场辐射发射、磁场辐射发射和传导发射限值以及等级划分。

130.	BMB21-2007	涉及国家秘密的载体销毁与信息消除安全保密要求				本标准规定了涉密载体销毁和信息消除的等级、实施方法、技术指标以及相应的安全保密管理要求，适用于涉密单位、保密工作部门授权的涉密载体销毁机构对涉密载体销毁和信息消除，以及涉密载体销毁设备和信息消除产品的研制、生产和检测。
131.	GGBB1-1999	信息设备电磁泄漏发射限值				本标准规定了信息设备电磁泄漏辐射发射、传导发射的限值。本标准适用于党政机关、重要企事业单位的涉密部门使用的信息设备。

三、 管理与服务标准

1、涉密服务						
序号	标准编号	标准名称	对应国际标准	发布日期	实施日期	范围
132.	BMB8-2004	国家保密局电磁泄漏发射防护产品检测实验室认可要求				本标准规定了“国家保密局电磁泄漏发射防护产品检测中心”及其分中心的检测实验室在组织管理、技术能力以及检测人员、检测场地、检测设备、设施配置等方面应达到的认可要求。本标识适用于申请获得实验室资格认可的单位的检查和评审，本标准供国家保密局认可实验室使用。
133.	BMB14-2004	涉及国家秘密的信息系统安全保密测评实验室要求				本标准规定了“国家保密局涉密信息系统安全保密测评中心”及其系统测评分中心的系统测评实验室在组织管理、技术能力以及系统测评人员、检测设备、设施配置等方面应达到的要求。本标准适用于申请获得实验室资格的单位的检查和评审，以及实验室的管理。
134.	BMB18-2006	涉及国家秘密的信息系统工程监理规范				本标准规定了涉及国家秘密的信息系统新建、改建和扩建过程中工程监理的工作方法和工作内容，适用于涉密信息系统使用单位、承建单位和监理单位组织开展涉密信息系统的安全保密建设和工程监理，也可用于保密工作部门对涉密信息系统工程监理的管理和指导。
135.	BMB20-2007	涉及国家秘密的信息系统分级保护管理规范				本标准规定了涉密信息系统分级保护管理过程、管理要求和管理内容，适用于涉密信息系统的设计单位、建设使用单位（主持建设、使用涉密信息系统的单位）对涉密信息系统的建设、使用和管理，也可用于保密工作部门对涉密信息系统的管理和审批。
136.	BMB23-2008	涉及国家秘密的信息系统分级保护方案设计指南				本标准规定了涉密信息系统分级保护方案应包括的主要内容，适用于涉密信息系统建设使用单位（主持建设、使用涉密信息系统的单位）和集成资质单位对涉密信息系统分级保护方案的设计，也可用于保密

						工作部门对涉密信息系统的审批管理。
2、安全控制与服务						
序号	标准编号	标准名称	对应国际标准	发布日期	实施日期	范围
137.	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不同阶段的实施要点和工作形式。本标准适用于规范组织开展的风险评估工作。
138.	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。
139.	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。 本标准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。
140.	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。 本标准适用于信息系统灾难恢复的规划、审批、实施和管理。
141.	GB/Z 20985-2007	信息技术　安全技术 信息安全事件管理指南	ISO/IEC TR 18044:2004	2007-06-14	2007-11-01	本指导性技术文件修改采用ISO/IEC TR 18044:2004《信息技术 安全技术 信息安全事件管理》。 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。 本指导性技术文件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。
142.	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。
143.	GB/T 24363-2009	信息安全技术 信息安全应急响应计划规范		2009-09-30	2009-12-01	本标准规定了编制信息安全应急响应计划的前期准备，确立了信息安全应急响应计划文档的基本要素，内容要求和格式规范。本标准适用于包括整个组织，组织中的部门和组织的信息系统（包括网络系统）的各层面上的信息安全应急响应计划。本标准为负责制定和维护信息安全应急响应计划的人员提供指导
144.	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。 本标准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（以下简称“机构”）。机构在进行灾难恢复中心建设与运维管理时，适用本标准进行灾难恢复中心管理组织机构、灾难恢复中心基础设施、灾难恢复中心信息系统及配套资源和灾难恢复中心运行维护管理体系的建设及管理。 灾难恢复中心的建设与运维管理应与机构的自身业务及信息技术活动需求相适应，并适用本标准开展工作。
145.	GB/T 20261-2006	信息技术 系统安全工程 能力成熟度模型	ISO/IEC 21827:2002	2006-03-14	2006-07-01	本标准是系统安全工程的一个过程参考模型，关注的是信息技术安全领域内某个或若干个相关系统实现安全的需求，主要描述了用来实现信息技术安全的过程，尤其是过程的成熟度。
146.	GB/T 30283-2013	信息安全技术 信息安全服务 分类		2013-12-31	2014-07-15	本标准规定了信息安全服务定义、信息安全服务基本类别。 本标准适用于信息安全行业对信息安全服务概念的理解和分类管理，适用于信息安全服务的开发、提供、选用和采购。 本标准不适用于仅依附于某一信息安全产品的服务（如：信息安全产品的使用、维保等服务）。
147.	GB/T 31500-2015	信息安全技术 存储介质数据恢复服务要求		2015-05-15	2016-01-01	本标准规定了实施存储介质数据恢复服务所需的服务原则、服务条件、服务过程要求及管理要求。 本标准适用于指导提供存储介质数据恢复服务机构针对非涉及国家秘

						密的数据恢复服务实施和管理。
148.	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。
149.	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	ISO/IEC 18028-3:2005	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。它还提供安全网关的选择和配置指南。尽管个人防火墙使用类似的技术，但因为它不作为安全网关使用，所以它不在本部分的范围之内。本部分适用于技术和管理人员，例如IT管理者、系统管理员、网络管理员和IT安全人员。本部分提供的指南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。
150.	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	ISO/IEC 18028-4:2005	2010-09-02	2011-02-01	本部分规定了安全使用远程接入（使用公共网络将一台计算机远程连接到另一台计算机或某个网络的方法及其IT安全含义）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。本标准使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。
151.	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	ISO/IEC 18028-5:2006	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。它是根据ISO/IEC 18028-1中的网络管理导则而构建的。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。本部分提供VPN综述，提出VPN的安全目标，并概括VPN的安全要求，它给出安全VPN的选择、实施以及VPN安全的网络监控指南。它也提供有关VPN所使用的典型技术和协议的信息。
152.	GB/T 25068.1-2012	信息技术 安全技术	ISO/IEC 18028-1:2006	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

		IT网络安全 第1部分：网络安全管理				统网络自身的互连以及将远程用户连接到网络。总的来说，它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。本部分支持识别和分析与通信相关的因素，这些因素宜在建立网络安全要求时考虑到；针对与通信网络连接相关的安全，介绍如何识别适当的控制域；综述可能的控制域，包括在GB/T 25068.2至GB/T 25068.5中详细论述的那些技术设计和实施主题。
153.	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	ISO/IEC 18028-2:2006	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的端到端网络安全建议的基础。
154.	GB/T 28454-2012	信息技术 安全技术 入侵检测系统的选择、部署和操作	ISO/IEC 18043:2006	2012-06-29	2012-10-01	本标准给出了帮助组织准备部署IDS的指南。特别是，详细说明了IDS的选择、部署和操作。同时给出了这些指导方针来源的背景信息。
155.	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,适用于政府部门采购和使用云计算服务,也可供重点行业和其他企事业单位参考。
156.	GB/Z 32906-2016	信息安全技术 中小电子商务企业信息安全建设指南		2016-08-29	2017-03-01	本指导性技术文件给出了中小电子商务企业信息安全建设结构与模式、安全风险、安全需求、安全设计、安全实现与部署运管的指南。本指导性技术文件适用于中小电子商务企业的信息安全建设，为电子商务项目开发、运行、维护提供技术参考。
157.	GB/T 32914-2016	信息安全技术 信息安全服务提供方管理要求		2016-08-29	2017-03-01	本标准针对信息安全服务提供方，提出了组织级管理和项目级管理的要求。本标准适用于信息安全服务提供方对其服务要素和服务风险进行管控，对信息安全服务需求方、评价机构和监管部门具有参考意义。
158.	GB/T 32924-2016	信息安全技术 网络安		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。本标准为及时准

		全预警指南				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。
159.	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。本标准适用于政府部门采购和使用信息技术服务。政府部门开展涉密信息技术服务外包工作，应参照国家保密局相关保密规定和标准执行，不在本标准范围内。
160.	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。 本标准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。
3、网络安全管理						
序号	标准编号	标准名称	对应国际标准	发布日期	实施日期	范围
161.	GB/T 17143.1-1997	信息技术 开放系统互连 系统管理 第1部分:客体管理功能	ISO/IEC 10164-1:1993	1997-12-01	1998-08-01	本部分定义的客体管理功能由服务、功能单元和类属定义组成。 本部分详细规定了客体管理的模型；类属定义，包括事件类型、事件信息和事件应答；创建、删除、活动等 9 种服务定义；客体管理的各种功能单元；各种协议，包括规程元素、抽象语法和功能单元协商的协议；与其他功能的关系；一致性要求。
162.	GB/T 17143.2-1997	信息技术 开放系统互连 系统管理 第2部分:状态管理功能	ISO/IEC 10164-2:1993	1997-12-01	1998-08-01	本部分定义的状态管理功能由服务和类属定义组成。 本部分详细规定了状态管理的模型，包括类属状态和状况属性；类属定义，包括类属属性、类属通知和被管客体；各种服务定义；功能单元；各种协议，包括规程元素、抽象语法和功能单元协商的协议；与其他功能的关系；一致性要求。
163.	GB/T 17143.3-1997	信息技术 开放系统	ISO/IEC 10164-3:1993	1997-12-01	1998-08-01	本部分定义的表示关系的属性由服务和类属定义组成。

		互连　系统管理 第3部分:表示关系的属性				本部分详细规定了表示关系属性的模型，包括表示关系的分类、关系的类型和关系的角色；类属定义，包括类属属性、类属通知和被管客体；各种服务定义；功能单元；各种协议，包括规程元素、抽象语法和功能单元协商的协议；与其他功能的关系；一致性要求。
164.	GB/T 17143.4-1997	信息技术　开放系统互连　系统管理 第4部分:告警报告功能	ISO/IEC 10164-4:1992	1997-12-01	1998-08-01	本部分定义的告警报告功能由服务、类属定义和功能单元组成。 本部分详细规定了告警报告的模型；类属定义，包括类属通知和被管客体；各种服务定义；功能单元；各种协议，包括规程元素、抽象语法和功能单元协商的协议；与其他功能的关系；一致性要求。
165.	GB/T 17143.5-1997	信息技术　开放系统互连　系统管理 第5部分:事件报告管理功能	ISO/IEC 10164-5:1993	1997-12-01	1998-08-01	本部分定义的事件报告管理功能由服务和两种功能单元组成。 本部分详细规定了事件报告管理的模型；类属定义，包括被管客体和引入的类属定义；各种服务定义；功能单元，包括事件报告管理和监控事件报告管理两种功能单元；各种协议，包括规程元素、抽象语法和功能单元协商的协议；与其他功能的关系；一致性要求。
166.	GB/T 17143.6-1997	信息技术　开放系统互连　系统管理 第6部分:日志控制功能	ISO/IEC 10164-6:1993	1997-12-01	1998-08-01	本部分定义的日志控制功能由服务和两种功能单元组成。 本部分详细规定了日志控制的模型；类属定义，包括被管客体和引入的类属定义；各种服务定义；功能单元，包括日志控制和监控日志两种功能单元；各种协议，包括规程元素、抽象语法和功能单元协商的协议；与其他功能的关系；一致性要求。
167.	GB/T 17143.7-1997	信息技术　开放系统互连　系统管理　第7部分：安全报警报告功能	ISO/IEC 10164-7:1992	1997-12-01	1998-08-01	本部分位于GB 9387的应用层，并按照GB/T17176提供的模型定义。系统管理功能的作用由GB/T17142描述。由本系统管理功能定义的安全告警通知提供关于操作条件和服务质量的信息，他们附属于安全。本标准为需要用来支持安全告警报告功能的服务定义建立用户需求；定义由安全告警报告功能提供的服务；规定为提供服务所需的协议；定义与其他系统管理功能之间的关系；规定一致性要求。
168.	GB/T 17143.8-1997	信息技术　开放系统互连　系统管理　第8	ISO/IEC 10164-8:1993	1997-12-15	1998-08-01	本部分位于GB/T9387的应用层，并按GB/T17176提供的模型定义。系统管理功能的作用由GB/T17142描述。本标准为需要用来支持安全审计

		部分：安全审计跟踪功能				跟踪报告功能的服务定义而建立用户需求；定义由安全审计跟踪报告功能提供的服务；规定为提供服务所必需的协议；定义服务与管理通知之间的关系；定义与其他系统管理功能之间的关系；规定一致性要求。
4、行业/领域安全管理						
序号	标准编号	标准名称	对应国际标准	发布日期	实施日期	范围
169.	GB/Z 24294-2009	信息安全技术 基于互联网电子政务信息安全实施指南		2009-07-30	2010-02-01	本指导性技术文件确立了基于互联网电子政务信息安全保障总体架构，为基于互联网电子政务所涉及的信息安全技术、信息安全管理、信息安全工程建设等方面安全要求的实施提供指导。本指导性技术文件主要对统一的安全政务网络平台、安全政务办公平台、可信公共服务平台和安全支撑平台的建设提出规范与要求。对于相关政务部门专有的业务系统，其安全防护根据明确责任、各负其责的原则，由主管部门采取适当的安全措施，本指导性技术文件适用于地市级（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建设提供管理和技术参考。
170.	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。
171.	GB/T 32919-2016	信息安全技术 工业控制系统安全控制应用指南		2016-08-29	2017-03-01	本标准提供了可用于工业控制系统的安全控制列表，规约了工业控制系统的安全控制选择过程，以便构造工业控制系统的安全程序--一种概念层面上的安全解决方案。 本标准适用于：1）方便规约工业控制系统的安全功能需求，为安全设计（包括安全体系结构设计）和安全实现奠定有力的基础。2）指导工

						业控制系统安全整改中安全能力的调整和提高，以便能使工业控制系统保持持续安全性。本标准的适用对象是组织中负责工业控制系统建设的组织者、负责信息安全工作的实施者和其他从事信息安全工作的相关人员。
172.	GB/T 32920-2016	信息技术 安全技术 行业间和组织间通信的信息安全管理		2016-08-29	2017-03-01	本标准给出了信息安全管理体系（ISMS）标准族的补充指南，用于在信息共享团体中实现信息安全管理。本标准特别为组织间和行业间通信给出了有关发起、实现、维护与改进信息安全的控制和指南。本标准适用于行业间各种公共和私有的、国内的和国际的所有形式的敏感信息交换与共享。特别是，本标准可适用于与组织或国家关键基础设施的供给、维护和保护相关的信息交换与共享。
173.	GB/T 32921-2016	信息安全技术 信息技术产品供应方行为安全准则		2016-08-29	2017-03-01	本标准规定了信息技术产品供应方在提供信息技术产品过程中，为保护用户相关信息、维护用户信息安全应遵守的基本准则。 本标准适用于信息技术产品供应、运行或维护过程中的供应方行为管理，也可为信息技术产品的研发、运维及测评等提供依据。
174.	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		2016-08-29	2017-03-01	本标准规定了政府部门联网计算机终端的安全要求。本标准适用于政府部门开展联网计算机终端安全配置、使用、维护与管理工作。

四、 测评标准

1、密码产品						
序号	标准编号	标准名称	对应国际标准	发布日期	实施日期	范围
175.	GB/T 25056-2010	信息安全技术 证书认		2010-09-02	2011-02-01	本标准规定了为公众服务的数字证书认证系统的设计、建设、检测、

		证系统密码及其相关安全技术规范				运行及管理规范。本标准为实现数字证书认证系统的互联互通和交叉认证提供统一的依据，指导第三方证书认证机构的数字证书认证系统的建设和检测评估，规范数字证书认证系统中密码及相关安全技术的应用。本标准适用于第三方证书认证机构的数字证书认证系统的设计、建设、检测、运行及管理。非第三方证书认证机构的数字证书认证系统的设计、建设、检测、运行及管理，可参照本标准。
176.	GB/T 29829-2013	信息安全技术 可信计算密码支撑平台功能与接口规范		2013-11-12	2014-02-01	本标准描述可信计算密码支撑平台功能原理与要求，并详细定义了可信计算密码支撑平台的密码算法、密钥管理、证书管理、密码协议、密码服务等应用接口规范。本标准适用于可信计算密码支撑平台相关产品的研制、生产、测评与应用开发。
177.	GB/T 32922-2016	信息安全技术 IPSec VPN安全接入基本要求与实施指南		2016-08-29	2017-03-01	本标准明确了采用IPSec VPN技术实现安全接入的场景，提出了IPSec VPN安全接入应用过程中有关网关、客户端以及安全管理等方面的要求，同时给出了IPSec VPN安全接入的实施过程指导。本标准适用于采用IPSec VPN技术开展安全接入应用的机构，指导其进行基于IPSec VPN技术开展安全接入平台或系统的需求分析、方案设计、配置实施、测试与备案、运行管理，也适用于设备厂商参考其进行产品的设计和开发。
178.	GB/T 33131-2016	信息安全技术 基于IPSec的IP存储网络安全技术要求		2016-10-13	2017-05-01	本标准规定了利用IPSec保护IP存储网络安全的技术要求，主要涉及了iSCSI、iFCP、FCIP等协议和因特网存储名称服务（iSNS）。本标准适用于IP存储网络安全设备的研制、生产和测试。
2、通用产品						
序号	标准编号	标准名称	对应国际标准	发布日期	实施日期	范围
179.	GB/T 17900-1999	网络代理服务器的安全技术要求		1999-11-11	2000-05-01	本标准规定了网络代理服务器的安全技术要求，并作为网络代理服务器的安全技术检测依据。本标准详细规定了代理服务器的安全环境，

						包括安全条件假设、对安全的威胁；安全目标，包括信息技术和非信息技术安全目标；信息技术安全要求，包括各种功能要求和各种保证要求；基本原理，包括信息技术安全目标、非信息技术安全目标、信息技术功能要求的基本原理。
180.	GB/T 18018-2007	信息安全技术 路由器安全技术要求		2007-06-13	2007-12-01	本标准分等级规定了路由器的安全功能 要求和安全保证要求，适用于指导路由器产品安全性的设计和实现，对路由器产品进行的测试、评估和管理也可参照使用。
181.	GB/T 20008-2005	信息安全技术 操作系统安全评估准则		2005-11-11	2006-05-01	本标准从信息技术方面规定了按照GB/T 17859-1999的五个安全保护等级对操作系统安全保护等级划分所需要的评估内容。本标准适用于计算机通用操作系统的安全保护等级评估，对于通用操作系统安全功能的研制、开发和测试亦可参照使用。
182.	GB/T 20009-2005	信息安全技术 数据库管理系统安全评估准则		2005-11-11	2006-05-01	本标准从信息技术方面规定了按照GB/T 17859-1999的五个安全保护等级对数据库管理系统安全保护等级划分所需要的评估内容。本标准适用于数据库管理系统的安全保护等级评估，对于数据库管理系统安全功能的研制、开发和测试亦可参照使用。
183.	GB/T 20010-2005	信息安全技术 包过滤防火墙评估准则		2005-11-11	2006-05-01	本标准从信息技术方面规定了按照GB 17859-1999的五个安全保护等级对采用“传输控制协议/网间协议（TCP/IP)”的包过滤防火墙产品安全保护等级划分所需要的评估内容。本标准适用于包过滤防火墙安全保护等级的评估，对于包过滤防火墙的研制、开发、测试和产品采购也可参照使用。
184.	GB/T 20011-2005	信息安全技术 路由器安全评估准则		2005-11-11	2006-05-01	本标准从信息技术方面规定了按照GB 17859-1999的五个安全保护等级的前三个等级，对路由器产品安全保护等级划分所需要的评估内容。本标准适用于路由器安全保护等级的评估，对路由器的研制、开发、测试和产品采购也可参照使用
185.	GB/T 20272-2006	信息安全技术 操作系统安全技术要求		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，根据操作系统在信息系统中的作用，规定了各个安全等级的操作系统所需要的安全

						技术要求。本标准使用于按等级化要求进行的操作系统安全的设计和实现，对按等级化要求进行的操作系统安全的测试和管理可参照使用。
186.	GB/T 20273-2006	信息安全技术 数据库管理系统安全技术要求		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，根据数据库管理系统在信息系统中的作用，规定了各个安全等级的数据库管理系统所需要的安全技术要求。本标准使用于按等级化要求进行的安全数据库管理系统的设计和实现，对按等级化要求进行的数据库管理系统安全的测试和管理可参照使用。
187.	GB/T 20275-2006	信息安全技术 入侵检测系统技术要求和测试评价方法		2006-05-31	2006-12-01	本标准规定了入侵检测系统的技术要求和测评方法，技术要求包括产品功能要求、产品安全要求、产品保证要求，并提出了入侵检测系统的分级要求。 本标准首先对入侵检测系统的等级进行了划分，即分为三级，并以网络型或主机型入侵检测系统的等级进行了划分；然后，在标准中对入侵检测系统技术要求和入侵检测系统测评方法的各三个级别的产品功能要求、产品安全要求、产品保证要求分别进行了详细规定。 本标准适用于入侵检测系统的设计、开发、测试和评估。
188.	GB/T 20276-2016	信息安全技术 具有中央处理器的IC卡嵌入式软件安全技术要求		2016-08-29	2017-03-01	本标准规定了对EAL4增强级和EAL5增强级的具有中央处理器的IC卡嵌入式软件进行安全保护所需要的安全技术要求。本标准适用于具有中央处理器的IC卡嵌入式软件产品的测试、评估和采购，也可用于指导该类产品的研制和开发。
189.	GB/T 20277-2015	信息安全技术 网络和终端隔离产品测试评价方法		2015-05-15	2016-01-01	本标准依据GB/T 20279-2015的技术要求，规定了网络和终端隔离产品的测试评价方法。本标准适用于按照GB/T 20279-2015的安全等级要求所开发的网络和终端隔离产品的测试和评价。
190.	GB/T 20278-2013	信息安全技术 网络脆弱性扫描产品安全技术要求		2013-12-31	2014-07-15	本标准规定了网络脆弱性扫描产品的安全功能要求、自身安全要求和安全保证要求，并根据安全技术要求的不同对网络脆弱性扫描产品进行了分级。本标准适用于网络脆弱性扫描产品的研制、生产和检测。
191.	GB/T 20279-2015	信息安全技术 网络		2015-05-15	2016-01-01	本标准规定了网络和终端隔离产品的安全功能要求、安全保证要求、

		和终端隔离产品安全技术要求				环境适应性要求及性能要求。本标准适用于网络和终端隔离产品的设计、开发与测试。
192.	GB/T 20280-2006	信息安全技术　网络脆弱性扫描产品测试评价方法		2006-05-31	2006-12-01	本标准规定对采用传输控制协议/网际协议（TCP/IP）的网络脆弱性扫描产品的测试、评价方法。 本标准首先给出了网络脆弱性扫描产品的测试环境；然后详细规定了网络脆弱性扫描产品测试评价的各种方法和步骤，包括基本型网络脆弱性扫描产品的基本功能、性能要求、安全保证要求，增强型网络脆弱性扫描产品的基本功能及性能、增强功能、安全保证要求的各种测试评价方法和步骤。标准以附录的形式给出了产品厂商应向测试单位提供的必要资料和证据。 网络脆弱性扫描产品测评的内容，测评功能目标及测试环境，给出产品基本功能、增强功能和安全保证要求必须达到的具体目标。 本标准适用于对计算机信息系统进行人工或自动的网络脆弱性扫描的安全产品的评测、研发和应用。 本标准不适用于专门对数据库系统进行脆弱性扫描的产品。
193.	GB/T 20281-2015	信息安全技术　防火墙安全技术要求和测试评价方法		2015-05-15	2016-01-01	本标准规定了防火墙的安全技术要求、测试评价方法及安全等级划分。 本标准适用于防火墙的设计、开发与测试。
194.	GB/T 20945-2013	信息安全技术 信息系统安全审计产品技术要求和测试评价方法		2013-12-31	2014-07-15	本标准规定了信息系统安全审计产品的技术要求和测试评价方法，技术要求包括安全功能要求、自身安全功能要求和安全保证要求，并提出了信息系统安全审计产品的分级要求。 本标准适用于信息系统安全审计产品的设计、开发、测试和评价。
195.	GB/T 20979-2007	信息安全技术　虹膜识别系统技术要求		2007-06-18	2007-11-01	本标准规定了用虹膜识别技术为身份鉴别提供支持的虹膜识别系统的技术要求。 本标准适用于按信息安全等级保护的要求所进行的虹膜识别系统的设计与实现，对虹膜识别系统的测试、管理也可参照使用。

196.	GB/T 21028-2007	信息安全技术 服务器安全技术要求		2007-06-29	2007-12-01	本标准依据GB17859-1999《计算机信息系统安全保护等级划分准则》划分的五个安全保护等级，规定了服务器所需要的安全技术要求，以及每一个安全保护等级的不同安全技术要求。 本标准详细规定了服务器的安全功能要求和安全分等级要求。其中，服务器安全功能要求包括设备安全、运行安全和数据安全；服务器安全分等级要求包括五个安全保护等级各自涵盖的安全功能要求和安全保证（含服务器安全子系统的自身安全保护、设计和实现、管理）要求。标准还以附录的形式给出了服务器安全方面有关概念的说明。 本标准适用于按GB17859-1999的五个安全保护等级要求所进行的等级化服务器的设计、实现、选购和使用。按五个等级对服务器安全进行的测试和管理也可参照使用。
197.	GB/T 21050-2007	信息安全技术 网络交换机安全技术要求（评估保证级3）		2007-08-24	2008-01-01	本标准规定了网络交换机EAL3级的安全技术要求，主要包括网络交换机的安全假设、威胁和组织策略安全环境，以及网络交换机EAL3级的安全目的、安全功能和安全保证要求。本标准适用于网络交换机的研制、开发、测试、评估和采购。本标准主要适用于信息系统安全工程师、产品生产商、安全产品评估者。
198.	GB/T 22186-2016	信息安全技术 具有中央处理器的IC卡芯片安全技术要求		2016-08-29	2017-03-01	本标准规定了对具有中央处理器的IC卡芯片达到EAL4+、EAL5+、EAL6+所要求的安全功能要求及安全保障要求。 本标准适用于IC卡芯片产品的测试、评估和采购，也可用于指导该类产品的研制和开发。
199.	GB/T 25063-2010	信息安全技术 服务器安全测评要求		2010-09-02	2011-02-01	本标准规定了服务器安全的测评要求，包括第一级、第二级、第三级和第四级服务器安全测评要求。本标准没有规定第五级服务器安全测评的具体内容要求。本标准适用于评测机构从信息安全等级保护角度对服务器安全进行的测评工作。信息系统的主管部门及运营使用单位、服务器软硬件生产厂商也可参考使用。
200.	GB/T 25066-2010	信息安全技术 信息安		2010-09-02	2011-02-01	本标准规定了信息安全产品的主要类别与代码，包括物理安全类、主

		全产品类别与代码				机及其计算环境安全类、网络通信安全类、边界安全类、应用安全类、数据安全类、安全管理与支持类及其他类八个方面。本标准适用于国家信息安全等级保护建设与信息安全行业分类管理。本标准不适用于提供密码算法运算的商用密码产品（如密码芯片和密码模块等）。
201.	GB/T 28451-2012	信息安全技术 网络型入侵防御产品技术要求和测试评价方法		2012-06-29	2012-10-01	本标准规定了网络型入侵防御产品的功能要求、产品自身安全要求和产品保证要求，并提出了入侵防御产品的分级要求。标准适用于网络型入侵防御产品的设计、开发、测试和评价。
202.	GB/T 28456-2012	IPsec协议应用测试规范		2012-06-29	2012-10-01	本标准对IPsec协议应用的测试内容及测试步骤进行了规范。本标准适用于IPsec协议应用的开发单位、第三方授权测试认证机构、用户等对IPsec协议应用测试时参考使用。
203.	GB/T 28457-2012	SSL协议应用测试规范		2012-06-29	2012-10-01	本标准规定了SSL协议应用的测试内容和基本测试步骤。本标准适用于SSL协议应用的开发单位、第三方授权测试认证机构、用户等对SSL协议应用的测试。
204.	GB/T 29766-2013	信息安全技术 网站数据恢复产品技术要求与测试评价方法		2013-04-28	2014-05-01	本标准规定了网站数据恢复产品技术要求与测试评价方法。 本标准适用于对网站数据恢复产品的研制、生产、测试和评价。
205.	GB/T 29765-2013	信息安全技术 数据备份与恢复产品技术要求与测试评价方法		2013-04-28	2014-05-01	本标准规定了数据备份与恢复产品的技术要求与测试评价方法。本标准适用于对数据备份与恢复产品的研制、生产、测试、评价。 本标准所指的数据备份与恢复产品是指实现和管理信息系统数据备份和恢复过程的产品，不包括数据复制产品和持续数据保护产品。
206.	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。 本标准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。 注：本标准主要规定从开机引导到操作系统内核加载前的信任链传递。
207.	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。本标准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。
208.	GB/T 30282-2013	信息安全技术 反垃圾邮件产品技术要求和测试评价方法		2013-12-31	2014-07-15	本标准规定了反垃圾邮件产品的技术要求和测试评价方法。 本标准适用的反垃圾邮件产品范围包括透明的反垃圾邮件网关、基于转发的反垃圾邮件系统、安装于邮件服务器的反垃圾邮件软件以及与邮件服务器一体的反垃圾邮件的邮件服务器。 本标准适用于对反垃圾邮件产品的研制、生产、测试和评价。
209.	GB/T 31499-2015	信息安全技术 统一威胁管理产品技术要求和测试评价方法		2015-05-15	2016-01-01	本标准规定了统一威胁管理产品功能要求、性能指标、产品自身安全要求和产品保证要求，以及统一威胁管理产品的分级要求，并根据技术要求给出了测试评价方法。 本标准适用于统一威胁管理产品的设计、开发、测试和评价。
210.	GB/T 31505-2015	信息安全技术 主机型防火墙安全技术要求和测试评价方法		2015-05-15	2016-01-01	本标准规定了主机型防火墙的安全技术要求、测评评价方法及安全等级划分。 本标准适用于主机型防火墙的设计、开发与测试。
211.	GB/T 31507-2015	信息安全技术 智能卡通用安全检测指南		2015-05-15	2016-01-01	本标准规定了智能卡类产品进行安全性检测的一般性过程和方法。 本标准适用于智能卡安全性检测评估和认证。
212.	GB/T 32917-2016	信息安全技术 WEB应用防火墙安全技术要求与测试评价方法		2016-08-29	2017-03-01	本标准规定了WEB应用防火墙的安全功能要求、自身安全保护要求、性能要求和安全保证要求，并提供了相应的测试评价方法。本标准适用于WEB应用防火墙的设计、生产、检测及采购。
213.	GB/T 32927-2016	信息安全技术 移动智能终端安全架构		2016-08-29	2017-03-01	本标准提出了移动智能终端的安全架构，描述了移动智能终端的安全需求。本标准适用于移动智能终端涉及的设计、开发、测试和评估。
3、安全保密产品						
序号	标准编号	标准名称	对应国际标准	发布日期	实施日期	范围
214.	BMB1-1994	电话机电磁泄漏发射				本标准规定了电话机电磁泄漏辐射发射、传导发射的限值和测试方法。

		限值和测试方法				本标准适用于党政专用电话网使用的有线电话机（不包括无绳电话机、数字电话机），适用于需要保密通信的电话机。
215.	BMB2-1998	使用现场的信息设备电磁泄漏发射检查测试方法和安全判据				本标准规定了使用现场的信息设备电磁泄漏辐射发射、传导发射检查测试方法和信息安全判据。本标准适用于保密部门对信息设备进行现场保密检查。
216.	BMB3-1999	处理涉密信息的电磁屏蔽室的技术要求和测试方法				本标准规定了处理涉密信息的电磁屏蔽室的电磁场屏蔽效能要求、传导泄漏发射抑制要求和测试方法。本标准适用于对处理涉密信息的电磁屏蔽室性能进行检测。
217.	GGBB2-1999	信息设备电磁泄漏发射测试方法				本标准规定了信息设备电磁泄漏辐射发射、传导发射的测试方法。本标准适用于党政机关、重要企事业单位的涉密部门使用的信息设备。
218.	BMB4-2000	电磁干扰器技术要求和测试方法				本标准规定了电磁干扰器的辐射发射要求、传导发射及抑制要求、抗视频信息还原性能要求和测试方法以及等级划分。本标准适用于保护满足GB9254-1998A级、B级或其它等同标准要求计算机的电磁干扰器。
219.	BMB7-2001	密码设备电磁泄漏发射测试方法（总则）				本标准规定了密码设备电场辐射发射、磁场辐射发射和传导发射测试方法的总要求以及红黑信号识别的测试方法。
220.	BMB10-2004	涉及国家秘密的计算机网络安全隔离设备的技术要求和测试方法				本标准规定了安全隔离计算机、安全隔离卡及安全隔离线路选择器的技术要求和测试方法。本标准适用于安全隔离计算机、安全隔离卡及安全隔离线路选择器的开发和检测。
221.	BMB11-2004	涉及国家秘密的计算机信息系统防火墙安全技术要求				本标准规定了涉及国家秘密的计算机信息系统使用的防火墙产品或系统的安全技术要求。本标准适用于涉密信息系统内使用的防火墙产品或系统安全功能的研制、开发、生产、测试、评估和产品的采购。
222.	BMB12-2004	涉及国家秘密的计算机信息系统漏洞扫描产品技术要求				本标准规定了涉密信息系统内使用的漏洞扫描产品的技术要求。本标准适用于涉密信息系统内使用的漏洞扫描产品的设计、研制、生产、测试、评估和采购。

223.	BMB13-2004	涉及国家秘密的计算机信息系统入侵检测产品技术要求				本标准规定了涉密信息系统内使用的网络型和主机型入侵检测产品的技术要求。本标准适用于涉密信息系统内使用的网络型和主机型入侵检测产品的设计、研制、生产、测试、评估和采购。
224.	BMB16-2004	涉及国家秘密的信息系统安全隔离与信息交换产品技术要求				本标准规定了涉密信息系统使用的安全隔离与信息交换产品技术要求。本标准适用于涉密信息系统使用的安全隔离与信息交换产品的设计、研制、生产、测试、评估和采购。
225.	BMB19-2006	电磁泄漏发射屏蔽机柜技术要求和测试方法				本标准规定了电磁泄漏发射屏蔽机柜技术要求和测试方法。
226.	BMB9.1-2007	保密会议室移动通信干扰器技术要求和测试方法				本标准规定了用于保密会议的移动通信无线信号干扰器的技术要求和测试方法。
227.	BMB9.2-2007	保密会议室移动通信干扰器安装使用指南				本标准规定了移动通信无线信号干扰器在保密会议场所的安装使用指南。
228.	BMB24-2010	涉密计算机及移动存储介质保密管理系统技术要求				
229.	BMB15-2011	涉及国家秘密的信息系统安全监控与审计产品技术要求				

4、通用系统

序号	标准编号	标准名称	对应国际标准	发布日期	实施日期	范围
230.	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	本标准依据GB17859-1999《计算机信息系统安全保护等级划分准则》划分的五个安全保护等级，规定了各个安全等级的网络系统所需要的

						基础安全技术的要求。 本标准详细给出了网络安全的组成及它们的相互关系；网络安全功能的基本要求，包括身份鉴别、自主访问控制、标记、强制访问控制、数据流控制、安全审计、用户数据完整性、用户数据保密性、可信路径、抗抵赖、网络安全监控；网络安全功能分层分级要求；按GB17859-1999的五个安全保护等级，对每一个安全保护等级的安全功能技术要求和安全保证技术要求做了详细描述。标准还以附录的形式给出了标准中各概念的说明。 本标准适用于按等级化要求进行的网络系统的设计和实现，对按等级化要求进行的网络系统安全的测试和管理可参照使用。
231.	GB/T 20271-2006	信息安全技术　信息系统通用安全技术要求		2006-05-31	2006-12-01	本标准依据GB17859-1999《计算机信息系统安全保护等级划分准则》划分的五个安全保护等级，规定了信息系统安全所需要的安全技术的各个安全等级要求。 本标准主要从信息系统安全保护等级划分角度，说明为实现GB17859-1999中每一个安全保护等级的安全功能要求应采取的安全技术措施，以及各安全保护等级的安全功能在具体实现上的差异。 本标准首先对信息安全等级保护所涉及的安全功能技术要求和安全保证技术要求做了比较全面的描述，然后按GB17859-1999的五个安全保护等级，对每一个安全保护等级的安全功能技术要求和安全保证技术要求做了详细描述。标准以附录的形式给出了标准中各概念的说明，等级化信息系统安全设计的参考，以及安全技术要素与安全技术分等级要求之间的对应关系。 本标准适用于按等级化要求进行的安全信息系统的设计和实现，对按等级化要求进行的信息系统安全的测试和管理可参照使用。
232.	GB/T 20983-2007	信息安全技术　网上银行系统信息安全保		2007-06-14	2007-11-01	本标准规定了网上银行系统的描述、安全环境、安全保障目的、安全保障要求及网上银行系统信息安全保障目的和安全保障要求的符合性

		障评估准则				声明。本标准适用规范网上银行系统在网上交易过程中涉及信息安全的评估工作。
233.	GB/T 20987-2007	信息安全技术 网上证券交易系统信息安全保障评估准则		2007-06-14	2007-11-01	本标准规定了网上证券交易系统的描述、安全环境、安全保障目的、安全保障要求及网上证券系统信息安全保障目的和安全保障要求的符合性声明。本标准适用于规范网上证券系统在交易过程中涉及信息安全的评估工作。
234.	GB/T 22239-2008	信息安全技术 信息系统安全等级保护基本要求		2008-06-19	2008-11-01	本标准规定了不同安全保护等级信息系统的基本保护要求，包括基本技术要求和基本管理要求，适用于指导分等级的信息系统的安全建设和监督管理。
235.	GB/T 22240-2008	信息安全技术 信息系统安全等级保护定级指南		2008-06-19	2008-11-01	本标准规定了信息系统安全等级保护的定级方法，适用于为信息系统安全等级保护的定级工作提供指导。
236.	GB/T 25058-2010	信息安全技术 信息系统安全等级保护实施指南		2010-09-02	2011-02-01	本标准规定了信息系统安全等级保护实施的过程，适用于指导信息系统安全等级保护的实施。
237.	GB/T 25070-2010	信息安全技术 信息系统等级保护安全设计技术要求		2010-09-02	2011-02-01	本标准依据国家信息安全等级保护要求，规定了信息系统等级保护安全设计技术要求。本标准适用于指导信息系统运营使用单位、信息安全企业、信息安全服务机构开展信息系统等级保护安全技术方案的设计和实施，也可作为信息安全职能部门进行监督、检查和指导的依据。
238.	GB/T 28448-2012	信息安全技术 信息系统安全等级保护测评要求		2012-06-29	2012-10-01	本标准规定了对实现的信息系统是否符合GB/T 22239-2008所进行的测试评估活动的要求，包括对第一级信息系统、第二级信息系统、第三级信息系统和第四级信息系统进行测试评估的要求。本标准略去对第五级信息系统进行测评的要求。本标准适用于信息安全测评服务机构、信息系统的主管部门及运营使用单位对信息系统安全等级保护状况进行的安全测试评估。信息安全监管职能部门依法进行的信息安全等级保护监督检查可以参考使用。

239.	GB/T 28449-2012	信息安全技术 信息系统安全等级保护测评过程指南		2012-06-29	2012-10-01	本标准规定了信息系统安全等级保护测评（以下简称“等级测评”）工作的测评过程，对等级测评的活动、工作任务以及每项任务的输入/输出产品等提出指导性建议。本标准适用于测评机构、信息系统的主管部门及运营使用单位对信息系统安全等级保护状况进行的安全测评。
240.	GB/T 28452-2012	信息安全技术 应用软件系统通用安全技术要求		2012-06-29	2012-10-01	本标准规定了按照GB 17859-1999的五个安全保护等级的划分对应用软件系统进行等级保护所涉及的通用安全管理要求。本标准适用于信息系统的所有者、管理者以及应用软件系统开发和运维的管理人员、技术人员对应用软件系统开发部署和运行维护的安全管理。对于按照GB 17859-1999的五个安全保护等级的划分的应用软件系统进行安全等级保护的检查、评估也可参照使用。
241.	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。本标准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。
242.	GB/T 29241-2012	信息安全技术 公钥基础设施 PKI互操作性评估准则		2012-12-31	2013-06-01	本标准规定了 PKI 系统和 PKI 应用的五个互操作能力等级,完成了分等级的 PKI 互操作性评估准则,为 PKI 系统和 PKI 应用提供了互操作能力等级评估的依据。 本标准适用于需要进行跨域互操作的 PKI 系统和 PKI 应用,可用于 PKI 系统和 PKI 应用的设计、开发、制造、采购、测试、评估、使用等过程。
243.	GB/T 30284-2013	信息安全技术 移动通信智能终端操作系统安全技术要求（EAL2级）		2013-12-31	2014-07-15	本标准规定了EAL2级移动通信智能终端操作系统的安全技术要求，适用于移动通信智能终端操作系统安全的设计、开发、测试和评估。
244.	GB/T 30273-2013	信息安全技术 信息系统安全保障通用评估指南		2013-12-31	2014-07-15	本标准描述了评估者在使用GB/T 20274所定义的准则进行评估时需要完成的评估活动，为评估者在具体评估活动中的评估行为和活动提供指南。

						本标准的目标读者主要是采用GB/T 20274对信息系统进行安全性评估的评估者以及评估申请者、开发者、ISPP/ISST编制者。
5、涉密信息系统						
序号	标准编号	标准名称	对应国际标准	发布日期	实施日期	范围
245.	BMB17-2006	涉及国家秘密的信息系统分级保护技术要求				本标准规定了涉密信息系统的等级划分准则和相应等级的安全保密技术要求。本标准适用于涉密信息系统的设计单位、建设单位、使用单位对涉密信息系统的建设、使用和管理，也可用于保密工作部门对涉密信息系统的管理和审批。
246.	BMB22-2007	涉及国家秘密的信息系统分级保护测评指南				本标准规定了涉密信息系统分级保护测评工作流程、测评内容、测评方法和测评结果判定准则，适用于获得国家保密局授权的涉密信息系统风险评估机构或单位对涉密信息系统进行安全保密测评，也可用于保密工作部门对涉密信息系统进行检查、获得国家保密局涉密信息系统风险评估资质的单位和涉密信息系统使用单位对涉密信息系统进行自评估的依据。
247.	BMB25-2011	涉及国家秘密的信息系统保密技术检查指南				
248.	BMB26-2012	保密会议室保密要求和测试方法				
249.	BMB27-2012	涉及国家秘密的信息系统安全保密检测评估实施规范				

6、通信安全						
序号	标准编号	标准名称	对应国际标准	发布日期	实施日期	范围
250.	GB/T 20275-2013	信息安全技术 网络入侵检测系统技术要求和测试评价方法		2013-12-31	2014-07-15	本标准规定了网络入侵检测系统的技术要求和测试评价方法，要求包括安全功能要求、自身安全功能要求、安全保证要求和测试评价方法，并提出了网络入侵检测系统的分级要求。 本标准适用于网络入侵检测系统的设计、开发、测试和评价。
251.	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。
7、政府安全检查						
序号	标准编号	标准名称	对应国际标准	发布日期	实施日期	范围
252.	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。本标准中涉及保密工作的，按照保密法规和标准执行；涉及密码工作的，按照国家密码管理规定执行。 本标准适用于各级政府部门，其他单位可以参考使用。
8、安全能力评估						
序号	标准编号	标准名称	对应国际标准	发布日期	实施日期	范围
253.	GB/T 30271-2013	信息安全技术 信息安全服务能力评估准则		2013-12-31	2014-07-15	本标准定义了服务过程模型和信息安全服务商的服务能力的评估准则。本标准既可用于对信息安全服务提供商的能力进行评估，也可为服务提供商对于自身能力的改善提供指导。

254.	GB/T 31168-2014	信息安全技术 云服务安全能力要求		2014-09-03	2015-04-01	本标准描述了以社会化方式为特定客户提供云计算服务时,云服务商应具备的安全技术能力。本标准适用于对政府部门使用的云计算服务进行安全管理,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,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。

注：以上标准收集截止日期为 2017 年 2 月 26 日