ICS 35.040
L80

GA

中华人民共和国公共安全行业标准

GA/T 1390.3 —2017

信息安全技术 网络安全等级保护基本要求

第 3 部分：移动互联安全扩展要求

Information security technology- General requirements for classified protection of cyber security

—Part 3: Special security requirements for mobile interconnection

2017-05-08 发布　　2017-05-08 实施

中华人民共和国公安部 发布

目　次

前　言

GA/T 1390《信息安全技术 网络安全等级保护基本要求》已经或计划发布以下部分：

——第1部分：安全通用要求；

——第2部分：云计算安全扩展要求；

——第3部分：移动互联安全扩展要求；

——第4部分：物联网安全扩展要求；

——第5部分：工业控制安全扩展要求；

——第6部分：大数据安全扩展要求。

本部分是GA/T 1390的第3部分。

本部分按照GB/T 1.1-2009给出的规范起草。

本部分由公安部网络安全保卫局提出。

本部分由公安部信息系统安全标准化技术委员会提出并归口。

本部分起草单位：北京鼎普科技股份有限公司、公安部第三研究所、北京工业大学、工业控制系统信息安全技术国家工程实验室。

本部分主要起草人：王江波、于晴、张宗喜、任卫红、于东升、赵勇、杜静、周颖、谢朝海。

引　言

为了适应移动互联、云计算、大数据、物联网和工业控制等新技术、新应用情况下信息安全等级保护工作的开展，公安部信息系统标准化委员会提出针对移动互联、云计算、大数据、物联网和工业控制等新技术、新应用领域制定公共安全行业系列标准。

本部分是针对等级保护对象中采用移动互联技术部分提出的安全扩展要求，所以等级保护对象需同时符合 GB/T 22239 安全通用要求。

将来可能会随着技术的变化添加新的部分阐述特定领域的安全扩展要求。

信息安全技术 网络安全等级保护基本要求

第3部分：移动互联安全扩展要求

1 范围

GA/T 1390的本部分规定了采用移动互联技术不同安全保护等级保护对象的基本保护要求。

本部分适用于指导分等级的非涉密等级保护对象的安全建设和监督管理。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB 17859-1999 计算机信息系统 安全保护等级划分准则

GB/T 22239 信息安全技术 信息系统安全等级保护基本要求

GB/T 22240 信息安全技术 网络安全等级保护定级指南

GB/T 25069-2010 信息安全技术 术语

3 术语和定义

GB 17859-1999、GB/T 22239、GB/T 22240和GB/T 25069-2010界定的以及下列术语和定义适用于本文件。

3.1

移动终端 mobile device

在移动业务中使用的终端设备，包括智能手机、平板电脑、个人电脑等通用终端和专用终端设备。

3.2

无线接入设备 wireless access device

采用无线通信技术将移动终端接入有线网络的通信设备。

注：本标准中无线接入设备不包括公共的无线接入设备（如公共WiFi、运营商基站等）。

3.3

无线接入网关 wireless access gateway

部署在无线网络与有线网络之间，对有线网络进行安全防护的设备。

3.4

移动应用软件 mobile application

针对移动移动终端开发的应用软件，包括移动终端预置的应用软件，和互联网信息服务提供者提供的可以通过网站、应用商店等移动应用分发平台下载、安装和升级的第三方应用软件。

3.5

移动终端管理系统 mobile device management system

用于进行移动终端设备管理、应用管理和内容管理的专用软件，包括客户端软件和服务端软件。

4 缩略语

下列缩略语适用于本文件。

WEP 有线等效加密（Wired Equivalent Privacy）

MDMS 移动终端管理系统（Mobile Device Management System）

DoS 拒绝服务 （Denial of Service）

SSID 服务集标识（Service Set Identifier）

WPS WiFi 保护设置（Wi-Fi Protected Setup）

AP 无线访问接入点（Wireless Access Point）

WiFi 无线保真（Wireless Fidelity）

5 采用移动互联技术的等级保护对象概述

5.1 安全通用要求

信息安全技术 网络安全等级保护基本要求的通用安全要求应符合 GB/T 22239。

5.2 保护对象构成

采用移动互联技术等级保护对象由移动终端、移动应用和无线网络三部分组成，移动终端通过无线通道连接无线接入设备并访问服务器，如图1。并通过移动终端管理系统的服务端软件向客户端软件发送移动设备管理、移动应用管理和移动内容管理策略对移动终端进行安全管理。

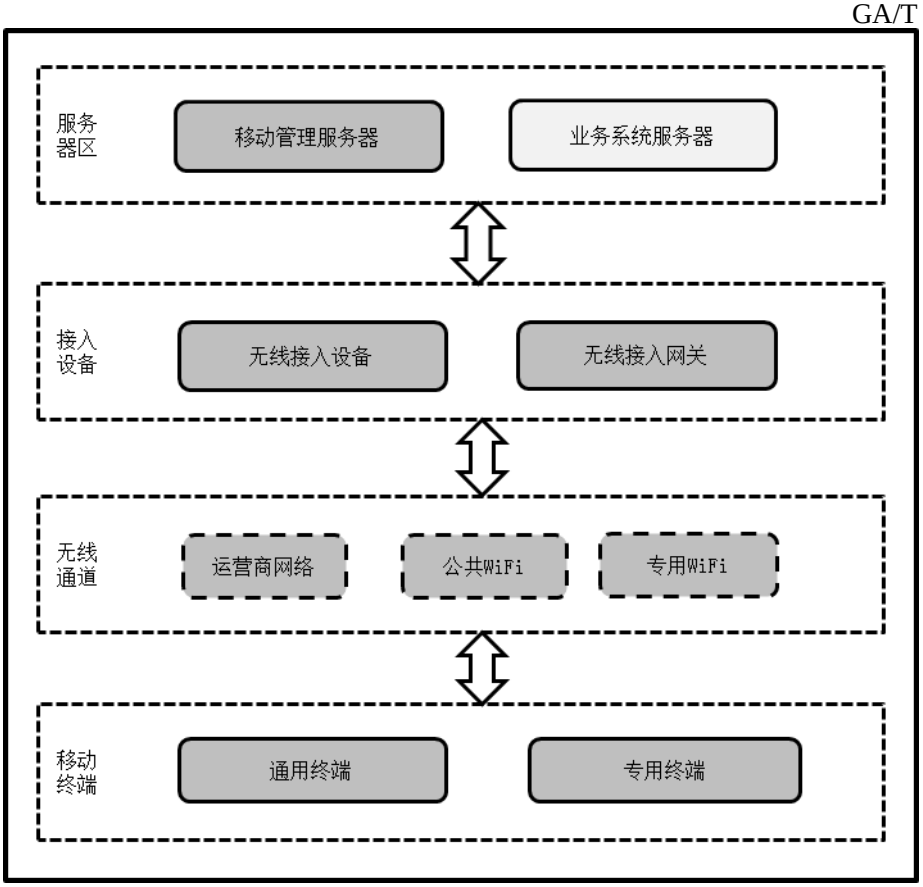

图1 等级保护对象构成

5.3 保护要素

与传统等级保护对象相比，采用移动互联技术等级保护对象中突出三个关键要素：移动终端、移动应用和无线网络。因此，采用移动互联技术等级保护对象的安全防护在传统等级保护对象防护的基础上，主要针对移动终端、移动应用和无线网络在物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个技术层面进行扩展。

5.4 保护对象定级

采用移动互联技术的等级保护对象应作为一个整体对象定级，移动终端、移动应用和无线网络等要素不单独定级。

6 第一级安全要求

6.1 技术要求

6.1.1 物理和环境安全

应为无线接入设备的安装选择合理位置，避免过度覆盖和电磁干扰。

6.1.2 网络和通信安全

6.1.2.1 网络架构

本项要求包括：

a) 无线接入网关的处理能力应满足基本业务需要；

b) 无线接入设备的带宽应满足基本业务需要；

c) 无线接入设备应开启接入认证功能，并且禁止使用 WEP 方式进行认证，如使用口令，长度不小于 8 位字符。

6.1.2.2 边界防护

有线网络与无线网络边界之间的访问和数据流应通过无线接入网关设备。

6.1.2.3 访问控制

应在有线网络与无线网络边界根据访问控制策略设置访问控制规则，默认情况下，除允许通信外，受控接口拒绝所有通信。

6.1.2.4 通信传输

应采用校验技术保证无线通信过程中数据的完整性。

6.1.3 设备和计算安全

6.1.3.1 身份鉴别

本项要求包括：

a) 应对移动终端用户登录、移动终端管理系统登录及其他系统级应用登录进行身份鉴别；

b) 移动终端应具有登录失败处理功能。

6.1.3.2 应用管控

移动终端管理客户端应具有选择应用软件安装、运行的功能。

6.1.3.3 入侵防范

移动终端应遵循最小安装的原则，仅安装需要的组件和应用程序。

6.1.3.4 恶意代码防范

移动终端应安装防恶意代码软件，并定期进行恶意代码扫描，及时更新防恶意代码软件版本和恶意代码库。

6.1.4 应用和数据安全

移动应用软件应采用校验技术保证重要数据存储的完整性。

6.2 管理要求

6.2.1 安全策略和管理制度

应建立等级保护对象移动互联安全管理规范，并纳入等级保护对象管理安全制度。

6.2.2 安全管理机构和人员

6.2.2.1 岗位设置

应将移动互联管理纳入等级保护对象管理员职责。

6.2.2.2 安全意识教育和培训

应对各类人员进行移动互联管理安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。

6.2.3 安全建设管理

6.2.3.1 安全方案设计

应根据等级保护对象的安全保护等级选择移动互联基本安全措施，依据风险分析的结果补充和调整安全措施。

6.2.3.2 产品采购和使用

移动互联信息安全产品采购和使用应符合国家的有关规定。

6.2.3.3 工程实施

应指定或授权专门的部门或人员负责系统移动互联工程实施过程的管理。

6.2.3.4 测试验收

应对系统的移动互联部分进行必要的安全性测试验收。

6.2.3.5 系统交付

本项要求包括：

a) 应根据交付清单对所交接的移动互联设备、移动应用软件和文档等进行清点；

b) 应对负责系统移动互联运行维护的技术人员进行相应的技能培训。

6.2.3.6 服务供应商选择

本项要求包括：

a)移动互联安全服务商的选择应符合国家的有关规定；

b) 应与选定的移动互联安全服务商签订与安全相关的协议，明确约定相关责任。

6.2.4 安全运维管理

6.2.4.1 设备维护管理

应对各种移动互联设备（包括无线接入设备）维护纳入等级保护对象进行管理。

6.2.4.2 漏洞和风险管理

应采取必要的措施识别移动互联安全漏洞和隐患，对发现的安全漏洞和隐患定期进行修补。

6.2.4.3 应用软件来源管理

移动终端安装、运行的应用软件应来自可靠证书签名或可靠分发渠道。

6.2.4.4 恶意代码防范管理

应对移动终端应用软件恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等。

6.2.4.5 备份与恢复管理

本项要求包括：

a) 应识别需要定期备份的移动终端中的关键业务信息、系统数据及软件系统等；

b) 应规定备份信息的备份方式、备份频度、存储介质、保存期等。

7 第二级安全要求

7.1 技术要求

7.1.1 物理和环境安全

应为无线接入设备的安装选择合理位置，避免过度覆盖和电磁干扰。

7.1.2 网络和通信安全

7.1.2.1 网络架构

本项要求包括：

a) 无线接入网关的处理能力应满足业务高峰期需要；

b) 无线接入设备的带宽应满足业务高峰期需要；

c) 无线接入设备应开启接入认证功能，并且禁止使用 WEP 方式进行认证，如使用口令，长度不小于 8 位字符并**且由数字、字母和特殊字符两种或两种以上进行组合**。

7.1.2.2 边界防护

有线网络与无线网络边界之间的访问和数据流应通过无线接入网关设备。

7.1.2.3 访问控制

本项要求包括：

a) 应在有线网络与无线网络边界根据访问控制策略设置访问控制规则，默认情况下，除允许通信外，受控接口拒绝所有通信；

b) 应对来自移动终端的数据流量、数据包和协议等进行检查，以允许/拒绝数据包通过。

7.1.2.4 入侵防范

本项要求包括：

a) 应能够检测、记录非授权无线接入设备；

b) 应能够对非授权移动终端接入的行为进行检测、记录；

c) 应具备对针对无线接入设备的网络扫描、DoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为进行检测、记录；

d) 应能够检测到无线接入设备的 SSID 广播、WPS 等高风险功能的开启状态。

7.1.2.5 通信传输

本项要求包括：

a) 应采用校验技术保证无线通信过程中数据的完整性；

b) **采用加解密结束保证无线通信过程中敏感信息字段或整个报文的保密性。**

7.1.2.6 安全审计

应启用设备安全审计功能，审计覆盖到每个移动终端，对重要的终端行为和重要安全事件进行审计。

7.1.2.7 网络设备防护

本项要求包括：

a) 应能发现系统移动终端、无线接入设备、无线接入网关设备可能存在的漏洞，并在经过充分测试评估后，及时修补漏洞；

b) 应禁用无线接入设备和无线接入网关存在风险的功能，如：SSID 广播、WEP 认证等；

c) 应禁止多个 AP 使用同一个鉴别密钥。

7.1.3 设备和计算安全

7.1.3.1 身份鉴别

本项要求包括：

a) 应对移动终端用户登录、移动终端管理系统登录及其他系统级应用登录进行身份鉴别；

b) 移动终端应具有登录失败处理功能。

7.1.3.2 应用管控

移动终端管理客户端本项要求包括：

a) 应具有软件白名单功能，应能根据白名单控制应用软件安装、运行；

b) 应具有应用软件权限控制功能，应能控制应用软件对移动终端中资源的访问；

c) 应只允许可靠证书签名的应用软件安装和运行。

7.1.3.3 入侵防范

移动终端本项要求包括：

a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；

b) **应能发现可能存在的漏洞，及时修补漏洞；**

c) **应能够发现用户权限异常改变的情况。**

7.1.3.4 恶意代码防范

移动终端应安装防恶意代码软件，并定期进行恶意代码扫描，及时更新防恶意代码软件版本和恶意代码库。

7.1.3.5 资源控制

本项要求包括：

a） **应将移动终端处理访问不同等级保护对象的进行应用级隔离；**

b） **应将移动终端处理访问等级保护对象的应用软件、数据存储区与处理访问非等级保护对象的应用软件、数据存储区等进行隔离；**

c） **应限制用户或进程对移动终端系统资源的最大使用限度，防止移动终端被提权。**

7.1.4 应用和数据安全

7.1.4.1 身份鉴别

本项要求包括：

a） **使用口令登录时，应强制用户首次登录时修改初始口令，对用户的鉴别信息进行复杂度检查；**

b） 用户身份鉴别信息丢失或失效时，应采用鉴别信息重置或其他技术措施保证系统安全。

7.1.4.2 软件审核与检测

等级保护对象业务移动应用软件开发结束后应经合规性审核。

7.1.4.3 数据完整性

移动应用软件本项要求包括：

a） **应采用校验技术或密码技术保证通信过程中数据的完整性；**

b） 应采用校验技术**或密码技术**保证重要数据存储的完整性。

7.1.4.4 数据保密性

移动应用软件本项要求包括：

a） 应采用密码技术保证重要数据在本地存储时的保密性；

b） **应对通信过程中的敏感信息字段进行加密。**

7.2 管理要求

7.2.1 安全策略和管理制度

本项要求包括：

a） 应建立等级保护对象移动互联安全管理规范，并纳入等级保护对象管理安全制度；

b） **应对管理人员或移动终端操作人员执行的日常管理操作建立操作规程。**

7.2.2 安全管理机构和人员

7.2.2.1 岗位设置

应将移动互联管理纳入等级保护对象管理员职责。

7.2.2.2 授权和审批

应针对移动互联系统变更、重要操作、物理访问和系统接入等事项执行审批过程。

7.2.2.3 安全意识教育和培训

应对各类人员进行移动互联管理安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。

7.2.3 安全建设管理

7.2.3.1 安全方案设计

本项要求包括：

a) 应根据等级保护对象的安全保护等级选择移动互联基本安全措施，依据风险分析的结果补充和调整安全措施；

b) **应根据等级保护对象的安全保护等级进行移动互联安全方案设计。**

7.2.3.2 产品采购和使用

移动互联信息安全产品采购和使用应符合国家的有关规定。

7.2.3.3 移动应用软件开发

本项要求包括：

a) 应对移动业务应用软件开发者进行资格审查；

b) 应要求开发移动业务应用软件的签名证书合法性；

c) 应要求移动应用软件开发完提供软件设计文档和使用指南；

d) 应要求应用软件开发使用的工具来源可靠；

e) 自行开发移动应用软件，开发环境与实际运行环境应物理分开，测试数据和测试结果受到控制；

f) 自行开发移动应用软件，应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；

g) 自行开发移动应用软件，应具备软件设计的相关文档和使用指南，并对文档使用进行控制；

h) 自行开发移动应用软件，对程序资源库的修改、更新、发布应进行授权和批准，并严格进行版本控制。

7.2.3.4 工程实施

应指定或授权专门的部门或人员负责系统移动互联工程实施过程的管理。

7.2.3.5 测试验收

应对系统的移动互联部分进行安全性测试验收。

7.2.3.6 系统交付

本项要求包括：

a) 应根据交付清单对所交接的移动互联设备、移动应用软件和文档等进行清点；

b) 应对负责系统移动互联运行维护的技术人员进行相应的技能培训；

c) 应提供移动互联建设过程中的文档和指导用户进行系统运行维护的文档。

7.2.3.7 服务供应商选择

本项要求包括：

a) 移动互联安全服务商的选择应符合国家的有关规定；

b) 应与选定的移动互联安全服务商签订与安全相关的协议，明确约定相关责任；

c） **应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的信息安全相关义务。**

7.2.4 安全运维管理

7.2.4.1 设备维护管理

应对各种移动互联设备（包括无线接入设备）维护纳入等级保护对象进行管理。

7.2.4.2 漏洞和风险管理

应采取必要的措施识别移动互联安全漏洞和隐患，对发现的安全漏洞和隐患**及时进行修补或评估可能的影响后**进行修补。

7.2.4.3 应用软件来源管理

本项要求包括：

a） 移动终端安装、运行的应用软件应来自可靠证书签名或可靠分发渠道；

b） **移动终端安装、运行的等级保护对象业务移动应用软件应由经审核的开发者开发。**

7.2.4.4 恶意代码防范管理

应对移动终端应用软件恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等。

7.2.4.5 备份与恢复管理

本项要求包括：

a） 应识别需要定期备份的移动终端中的重要业务信息、系统数据及软件系统等；

b） 应规定备份信息的备份方式、备份频度、存储介质、保存期等。

7.2.4.6 安全事件处置

本项要求包括：

a） **应报告所发现的移动互联安全弱点和可疑事件；**

b） **应明确移动互联安全事件的报告和处置流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责。**

8 第三级安全要求

8.1 技术要求

8.1.1 物理和环境安全

应为无线接入设备的安装选择合理位置，避免过度覆盖和电磁干扰。

8.1.2 网络和通信安全

8.1.2.1 网络架构

本项要求包括：

a) 无线接入网关的处理能力应满足业务高峰期需要；
b) 无线接入设备的带宽应满足业务高峰期需要；
c) 无线接入设备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算法进行加密。**

8.1.2.2 边界防护

有线网络与无线网络边界之间的访问和数据流应通过无线接入网关设备。

8.1.2.3 访问控制

本项要求包括：

a) 应在有线网络与无线网络边界根据访问控制策略设置访问控制规则，默认情况下，除允许通信外，受控接口拒绝所有通信；
b) 应对来自移动终端的数据流量、数据包和协议等进行检查，以允许/拒绝数据包通过；
c) 应在无线接入网关上对进出无线网络的数据进行内容过滤；
d) 应设置访问控制规则限制移动终端可访问的等级保护对象资源。

8.1.2.4 入侵防范

本项要求包括：

a) 应能够检测、记录、**定位**非授权无线接入设备；
b) **应**能够对非授权移动终端接入的行为进行检测、记录、**定位；**
c) 应具备对针对无线接入设备的网络扫描、DoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为进行检测、记录、**分析定位**；
d) 应能够检测到无线接入设备的 SSID 广播、WPS 等高风险功能的开启状态。

8.1.2.5 通信传输

本项要求包括：

a) 应采用**国家密码管理主管部门批准使用的密码算法**保证无线通信过程中数据的完整性；
b) 应采用**国家密码管理主管部门批准使用的密码算法**保证无线通信过程中敏感信息字段或整个报文的保密性。

8.1.2.6 安全审计

本项要求包括：

a) 应启用设备安全审计功能，审计覆盖到每个移动终端，对重要的终端行为和重要安全事件进行审计；
b) **应能对移动终端接入的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。**

8.1.2.7 网络设备防护

本项要求包括：

a) 应能发现系统移动终端、无线接入设备、无线接入网关设备可能存在的漏洞，并在经过充分测试评估后，及时修补漏洞；

b) 应禁用无线接入设备和无线接入网关存在风险的功能，如：SSID广播、WEP认证等；

c) 应禁止多个AP使用同一个鉴别密钥。

8.1.3 设备和计算安全

8.1.3.1 身份鉴别

本项要求包括：

a) 应对移动终端用户登录、移动终端管理系统登录及其他系统级应用登录进行身份鉴别；

b) 移动终端应具有登录失败处理功能，**应配置并启用限制非法登录次数等措施**。

8.1.3.2 移动终端管控

本项要求包括：

a) **移动终端应安装、注册并运行终端管理客户端软件；**

b) **移动终端应接受等级保护对象移动终端管理服务端的设备生命周期管理、设备远程控制、设备安全管控。**

8.1.3.3 应用管控

移动终端管理客户端本项要求包括：

a) 应具有软件白名单功能，应能根据白名单控制应用软件安装、运行；

b) 应具有应用软件权限控制功能，应能控制应用软件对移动终端中资源的访问；

c) 应只允许**等级保护对象管理者指定证书**签名的应用软件安装和运行；

d) 应具有接受移动终端管理服务端推送的移动应用软件管理策略，并根据该策略对软件实施管控的能力。

8.1.3.4 安全审计

本项要求包括：

a) **应启用移动终端安全审计功能，对终端用户重要操作及软件行为进行审计；**

b) **审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；**

c) **应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。**

8.1.3.5 入侵防范

移动终端本项要求包括：

a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；

b) 应能发现可能存在的漏洞，**并在经过充分测试评估后，**及时修补漏洞；

c) **应关闭不需要的系统服务、默认共享和高危端口；**

d) 应能够发现用户权限异常改变的情况。

8.1.3.6 恶意代码防范

移动终端本项要求包括：

a) 应安装防恶意代码软件，并定期进行恶意代码扫描，及时更新防恶意代码软件版本和恶意代码

库；

b) **应支持移动业务应用软件仅运行在安全容器内，防止被恶意代码攻击**。

8.1.3.7 资源控制

本项要求包括：

a) 应将移动终端处理访问不同等级等级保护对象的**运行环境**进行**操作系统级隔离**；

b) 应将移动终端处理访问等级保护对象的**运行环境**与非处理访问等级保护对象**运行环境**进行**系统级隔离**；

c) 应限制用户或进程对移动终端系统资源的最大使用限度，防止移动终端被提权。

8.1.4 应用和数据安全

8.1.4.1 身份鉴别

本项要求包括：

a) 使用口令登录时，应强制用户首次登录时修改初始口令，对用户的鉴别信息进行复杂度检查；

b) 用户身份鉴别信息丢失或失效时，应采用鉴别信息重置或其他技术措施保证系统安全；

c) 移动应用软件应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，鉴别信息具有复杂度要求；

d) 移动应用软件应提供并启用登录失败处理功能，多次登录失败后应采取必要的保护措施；

e) **应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别。**

8.1.4.2 软件审核与检测

等级保护对象业务移动应用软件开发后**、上线前经专业测评机构安全检测。**

8.1.4.3 数据完整性

移动应用软件本项要求包括：

a) 应采用**密码技术**保证通信过程中数据的完整性；

b) 应采用校验技术或密码技术保证重要数据存储时的完整性，**并在检测到完整性错误时采取必要的恢复措施；**

c) **应采用校验技术保证代码的完整性。**

8.1.4.4 数据保密性

移动应用软件本项要求包括：

a) 应采用密码技术保证重要数据在本地存储时的保密性；

b) **移动应用软件之间的重要数据应不能被互操作；**

c) **移动应用软件数据文件所在的存储空间，被释放或重新分配前应得到完全清除；**

d) 应对通信过程中的敏感信息字段**或整个报文**进行加密。

8.1.4.5 数据备份恢复

移动应用软件本项要求包括：

a) 应提供移动终端重要数据备份与恢复功能；

b) **应将重要数据定时批量传送至备用位置。**

8.2 管理要求

8.2.1 安全策略和管理制度

本项要求包括：

a) 应建立等级保护对象移动互联安全管理制度，并纳入等级保护对象管理安全制度；

b) 应对管理人员或移动终端操作人员执行的日常管理操作建立操作规程；

c) 应在等级保护对象管理制度中建立移动终端管理服务端操作使用管理规定。

8.2.2 安全管理机构和人员

8.2.2.1 岗位设置

本项要求包括：

a) 应将移动互联管理纳入等级保护对象管理员职责；

b) 应设立移动互联信息安全管理工作的职能部门，并制定各负责人的职责；

c) 应为移动终端管理服务端设置专职管理员、操作员，并纳入职能部门职责。

8.2.2.2 人员配备

移动终端管理服务端应配备专职管理员、操作员和审计员。

8.2.2.3 授权和审批

本项要求包括：

a) **应根据各个部门和岗位的职责明确移动互联管理授权审批事项、审批部门和批准人；**

b) 应针对移动互联系统变更、重要操作、物理访问和系统接入等事项执行审批过程；

c) **移动终端管理服务端设置专职管理员、操作员权限应由审批部门或批准人批准。**

8.2.2.4 安全意识教育和培训

本项要求包括：

a) 应对各类人员进行移动互联管理安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施；

b) **应对移动终端管理服务端设置专职管理员、操作员进行专项安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。**

8.2.3 安全建设管理

8.2.3.1 安全方案设计

本项要求包括：

a) 应根据等级保护对象的安全保护等级选择移动互联基本安全措施，依据风险分析的结果补充和调整安全措施；

b） 应根据等级保护对象的安全保护等级进行移动互联安全方案设计，**并纳入系统总体方案设计**；

c） 应组织相关部门和安全专家对系统移动互联安全方案设计进行论证和审定，经过批准后才能正式实施。

8.2.3.2 产品采购和使用

本项要求包括：

a） 移动互联信息安全产品采购和使用应符合国家的有关规定；

b） 密码产品与服务的采购和使用应符合国家密码管理主管部门的要求。

8.2.3.3 移动应用软件开发

本项要求包括：

a） 应对移动业务应用软件开发者进行资格审查；

b） 应要求开发移动业务应用软件的签名证书合法性；

c） 应要求移动应用软件开发完提供软件设计文档、使用指南；

d） 应要求应用软件开发使用的工具来源可靠；

e） 自行开发移动应用软件，开发环境与实际运行环境应物理分开，测试数据和测试结果受到控制；

f） 自行开发移动应用软件，应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；

g） 自行开发移动应用软件，应具备软件设计的相关文档和使用指南，并对文档使用进行控制；

h） 自行开发移动应用软件，应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制。

8.2.3.4 工程实施

应指定或授权专门的部门或人员负责系统移动互联工程实施过程的管理。

8.2.3.5 测试验收

应对系统的移动互联部分进行安全性测试验收。

8.2.3.6 系统交付

本项要求包括：

a） 应根据交付清单对所交接的移动互联设备、移动应用软件和文档等进行清点；

b） 应对负责系统移动互联运行维护的技术人员进行相应的技能培训；

c） 应提供移动互联建设过程中的文档和指导用户进行系统运行维护的文档；

d） 应提供移动终端管理服务端建设过程中的文档和指导用户进行系统运行维护的文档。

8.2.3.7 服务供应商选择

本项要求包括：

a） 移动互联安全服务商的选择应符合国家的有关规定；

b） 应与选定的移动互联安全服务商签订与安全相关的协议，明确约定相关责任；

c） 应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的信息安全相关义务；

d） **应选择安全可靠应用软件分发运营商。**

8.2.4 安全运维管理

8.2.4.1 资产管理

本项要求包括：

a） 应编制并保存与等级保护对象相关的移动终端资产清单，包括资产责任部门、重要程度和使用人等内容；

b） 应根据资产的重要程度对移动终端进行标识管理，根据其价值选择相应的管理措施。

8.2.4.2 设备维护管理

本项要求包括：

a） 应对各种移动互联设备（包括无线接入设备**及移动终端**）维护纳入等级保护对象进行管理；

b） **移动终端在报废或重用前应进行完全清除或被安全覆盖，确保该设备上的敏感数据和授权软件应无法被恢复重用；**

c） **应在移动终端设备丢失后进行远程数据擦除。**

8.2.4.3 漏洞和风险管理

应采取必要的措施识别移动互联安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。

8.2.4.4 应用软件来源管理

本项要求包括：

a） 移动终端安装、运行的应用软件应来自**等级保护对象管理者指定证书签名**或可靠分发渠道；

b） 移动终端安装、运行的**移动应用软件应**由经审核的开发者开发。

8.2.4.5 恶意代码防范管理

本项要求包括：

a） 应对移动终端应用软件恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等；

b） **应对截获的恶意代码进行及时分析处理；**

c） **移动终端管理服务端应将移动应用软件运行策略推送给移动终端。**

8.2.4.6 配置管理

移动终端管理服务端本项要求包括：

a） 应记录和保存移动终端基本配置信息，包括操作系统、软件组件版本、移动终端各种设备或软件组件的配置参数等；

b） 应将移动终端基本配置信息改变纳入系统变更范畴，实施对配置信息改变控制，并及时更新基本配置信息库；

c） 应建立合法无线接入设备和合法移动终端配置库，用于对非法无线接入设备和非法移动终端的识别。

8.2.4.7 监控和审计管理

本项要求包括：

a) 移动终端管理服务端对移动终端状态、资源使用、软件运行等应进行监控和审计；

b) 应对上线后的业务移动应用软件进行监测。

8.2.4.8 备份与恢复管理

本项要求包括：

a) 应识别需要定期备份的移动终端中的重要业务信息、系统数据及软件系统等；

b) 应规定备份信息的备份方式、备份频度、存储介质、保存期等；

c) 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。

8.2.4.9 安全事件处置

本项要求包括：

a) 应报告所发现的移动互联安全弱点和可疑事件；

b) 应明确安全事件的报告和处置流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责；

c) **应针对移动互联系统发生的安全事件制定应急处置预案。**

9 第四级安全要求

9.1 技术要求

9.1.1 物理和环境安全

应为无线接入设备的安装选择合理位置，避免过度覆盖和电磁干扰。

9.1.2 网络和通信安全

9.1.2.1 网络架构

本项要求包括：

a) 无线接入网关的处理能力应满足业务高峰期需要；

b) 无线接入设备的带宽应满足业务高峰期需要；

c) 无线接入设备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算法进行加密。

9.1.2.2 边界防护

有线网络与无线网络边界之间的访问和数据流应通过无线接入网关设备。

9.1.2.3 访问控制

本项要求包括：

a) 应在有线网络与无线网络边界根据访问控制策略设置访问控制规则，默认情况下，除允许通信外，受控接口拒绝所有通信；
b) 应对来自移动终端的数据流量、数据包和协议等进行检查，以允许/拒绝数据包通过；
c) 应在无线接入网关上对进出无线网络的数据进行内容过滤；
d) 应设置访问控制规则限制移动终端可访问的等级保护对象资源。

9.1.2.4 入侵防范

本项要求包括：

a) 应能够检测、记录、定位非授权无线接入设备；
b) 应能够对非授权移动终端接入的行为进行检测、记录、定位**并阻断**；
c) 应具备对针对无线接入设备的网络扫描、DoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为进行检测、记录、分析定位；
d) 应能够检测到无线接入设备的 SSID 广播、WPS 等高风险功能的开启状态。

9.1.2.5 通信传输

本项要求包括：

a) 应采用国家密码管理主管部门批准使用的密码算法保证无线通信过程中数据的完整性；
b) 应采用国家密码管理主管部门批准使用的密码算法保证无线通信过程中敏感信息字段或整个报文的保密性。

9.1.2.6 安全审计

本项要求包括：

a) 应启用设备安全审计功能，审计覆盖到每个移动终端，对**所有终端行为和所有安全事件**进行审计；
b) 应能对移动终端接入的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。

9.1.2.7 网络设备防护

本项要求包括：

a) 应能发现系统移动终端、无线接入设备、无线接入网关设备可能存在的漏洞，并在经过充分测试评估后，及时修补漏洞；
b) 应禁用无线接入设备和无线接入网关存在风险的功能，如：SSID广播、WEP认证等；
c) 应禁止多个AP使用同一个鉴别密钥。

9.1.3 设备和计算安全

9.1.3.1 身份鉴别

本项要求包括：

a) 应对移动终端用户登录、移动终端管理系统登录及其他系统级应用登录进行身份鉴别；
b) 移动终端应具有登录失败处理功能，应配置并启用限制非法登录次数等措施。

9.1.3.2 移动终端管控

移动终端本项要求包括：

a) 应只用于处理与等级保护对象相关业务；

b) 应安装、注册并运行终端管理客户端软件；

c) 应接受等级保护对象移动终端管理服务端的设备生命周期管理、设备远程控制、设备安全管控。

9.1.3.3 应用管控

移动终端管理客户端本项要求包括：

a) 应具有软件白名单功能，应能根据白名单控制应用软件安装、运行；

b) 应具有应用软件权限控制功能，应能控制应用软件对移动终端中资源的访问；

c) 应只允许等级保护对象管理者指定证书签名的应用软件安装和运行；

d) 应具有接受移动终端管理服务端推送的移动应用软件管理策略，并根据该策略对软件实施管控的能力。

9.1.3.4 安全审计

本项要求包括：

a) 应启用移动终端安全审计功能，对终端用户**所有**操作及软件行为进行审计；

b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。

9.1.3.5 入侵防范

移动终端本项要求包括：

a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；

b) 应能发现可能存在的漏洞，并在经过充分测试评估后，及时修补漏洞；

c) 应关闭不需要的系统服务、默认共享和**不需要的**端口；

d) 应能够发现**并阻止**用户权限异常改变的情况。

9.1.3.6 恶意代码防范

移动终端本项要求包括：

a) 应安装防恶意代码软件，并定期进行恶意代码扫描，及时更新防恶意代码软件版本和恶意代码库；

b) 应支持移动业务应用软件仅运行在安全容器内，防止被恶意代码攻击。

9.1.3.7 资源控制

本项要求包括：

a) 应禁止同一移动终端处理访问不同等级保护对象的运行环境；

b) 应禁止同一移动终端处理访问等级保护对象与非等级保护对象的运行环境；

c) 应**禁止**用户或进程对移动终端系统资源的最大使用限度，防止移动终端被提权。

9.1.4 应用和数据安全

9.1.4.1 身份鉴别

本项要求包括：

a) 使用口令登录时，应强制用户首次登录时修改初始口令，对用户的鉴别信息进行复杂度检查；
b) 用户身份鉴别信息丢失或失效时，应采用鉴别信息重置或其他技术措施保证系统安全；
c) 移动应用软件应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，鉴别信息具有复杂度要求；
d) 移动应用软件应提供并启用登录失败处理功能，多次登录失败后应采取必要的保护措施；
e) 应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别。

9.1.4.2 软件审核与检测

等级保护对象业务移动应用软件开发后、上线前应经专业测评机构安全检测。

9.1.4.3 数据完整性

移动应用软件本项要求包括：

a） 应采用**国家密码管理主管部门批准使用的密码算法**保证通信过程中数据的完整性；
b） 应采用校验技术或密码技术保证重要数据存储时的完整性，并在检测到完整性错误时采取必要的恢复措施；
c） 应采用校验技术保证代码的完整性。

9.1.4.4 数据保密性

移动应用软件本项要求包括：

a） 应采用**国家密码管理主管部门批准使用的密码算法**保证重要数据在本地存储时的保密性；
b） 移动应用软件之间的重要数据应不能被互操作；
c） 移动应用软件数据文件所在的存储空间，被释放或重新分配前应得到完全清除；
d） 应对通信过程中的敏感信息字段或整个报文进行加密。

9.1.4.5 数据备份恢复

移动应用软件本项要求包括：

a) 应提供移动终端重要数据备份与恢复功能；
b) 应将重要数据定时批量传送至备用位置。

9.2 管理要求

9.2.1 安全策略和管理制度

本项要求包括：

a） 应建立等级保护对象移动互联安全管理制度，并纳入等级保护对象管理安全制度；
b） 应对管理人员或移动终端操作人员执行的日常管理操作建立操作规程；
c） 应在等级保护对象管理制度中建立移动终端管理服务端操作使用管理规定。

9.2.2 安全管理机构和人员

9.2.2.1 岗位设置

本项要求包括：

a) 应将移动互联管理纳入等级保护对象管理员职责；

b) 应设立移动互联信息安全管理工作的职能部门，并制定各负责人的职责；

c) 应为移动终端管理服务端设置专职管理员、操作员，并纳入职能部门职责。

9.2.2.2 人员配备

移动终端管理服务端应配备专职管理员、操作员和审计员。

9.2.2.3 授权和审批

本项要求包括：

a) 应根据各个部门和岗位的职责明确移动互联管理授权审批事项、审批部门和批准人；

b) 应针对移动互联系统变更、重要操作、物理访问和系统接入等事项执行审批过程；

c) 移动终端管理服务端设置专职管理员、操作员权限应由审批部门或批准人批准。

9.2.2.4 安全意识教育和培训

本项要求包括：

a) 应对各类人员进行移动互联管理安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施；

b) 应对移动终端管理服务端设置专职管理员、操作员进行专项安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。

9.2.3 安全建设管理

9.2.3.1 安全方案设计

本项要求包括：

a) 应根据等级保护对象的安全保护等级选择移动互联基本安全措施，依据风险分析的结果补充和调整安全措施；

b) 应根据等级保护对象的安全保护等级进行移动互联安全方案设计，并纳入系统总体方案设计；

c) 应组织相关部门和安全专家对系统移动互联安全方案设计进行论证和审定，经过批准后才能正式实施。

9.2.3.2 产品采购和使用

a) 移动互联信息安全产品采购和使用应符合国家的有关规定；

b) 密码产品与服务的采购和使用应符合国家密码管理主管部门的要求。

9.2.3.3 移动应用软件开发

本项要求包括：

a) 应对移动业务应用软件开发者进行资格审查；

b) 应要求开发移动业务应用软件的签名证书合法性；

c） 应要求移动应用软件开发完提供软件设计文档、使用指南；

d） 应要求应用软件开发使用的工具来源可靠；

e） 自行开发移动应用软件,开发环境与实际运行环境应物理分开,测试数据和测试结果受到控制；

f） 自行开发移动应用软件,应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；

g） 自行开发移动应用软件,应具备软件设计的相关文档和使用指南，并对文档使用进行控制；

h） 自行开发移动应用软件,对程序资源库的修改、更新、发布应进行授权和批准，并严格进行版本控制。

9.2.3.4 工程实施

应指定或授权专门的部门或人员负责系统移动互联工程实施过程的管理。

9.2.3.5 测试验收

应对系统的移动互联部分进行安全性测试验收。

9.2.3.6 系统交付

本项要求包括：

a） 应根据交付清单对所交接的移动互联设备、移动应用软件和文档等进行清点；

b） 应对负责系统移动互联运行维护的技术人员进行相应的技能培训；

c） 应提供移动互联建设过程中的文档和指导用户进行系统运行维护的文档；

d） 应提供移动终端管理服务端建设过程中的文档和指导用户进行系统运行维护的文档。

9.2.3.7 服务供应商选择

本项要求包括：

a） 移动互联安全服务商的选择应符合国家的有关规定；

b） 应与选定的移动互联安全服务商签订与安全相关的协议，明确约定相关责任；

c） 应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的信息安全相关义务；

d） 应选择安全可靠应用软件分发运营商。

9.2.4 安全运维管理

9.2.4.1 资产管理

本项要求包括：

a） 应编制并保存与等级保护对象相关的移动终端资产清单，包括资产责任部门、重要程度和使用人等内容；

b） 应根据资产的重要程度对移动终端进行标识管理，根据其价值选择相应的管理措施。

9.2.4.2 设备维护管理

本项要求包括：

a） 应对各种移动互联设备（包括无线接入设备及移动终端）维护纳入等级保护对象进行管理；

b） 移动终端在报废或重用前应进行完全清除或被安全覆盖，该设备上的敏感数据和授

权软件应无法被恢复重用；

c） 应在移动终端设备丢失后进行远程数据擦除。

9.2.4.3 漏洞和风险管理

应采取必要的措施识别移动互联安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。

9.2.4.4 应用软件来源管理

本项要求包括：

a） 移动终端安装、运行的应用软件应来自等级保护对象管理者指定证书签名或**指定**分发渠道；

b） 移动终端安装、运行的移动应用软件应由**等级保护对象管理者指定**的开发者开发。

9.2.4.5 恶意代码防范管理

本项要求包括：

a） 应对移动终端应用软件恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等；

b） 应对截获的恶意代码进行及时分析处理；

c） 移动终端管理服务端应将移动应用软件运行策略推送给移动终端。

9.2.4.6 配置管理

本项要求包括：

a） 移动终端管理服务端应记录和保存移动终端基本配置信息，包括操作系统、软件组件版本、移动终端各种设备或软件组件的配置参数等；

b） 移动终端管理服务端应将移动终端基本配置信息改变纳入系统变更范畴，实施对配置信息改变控制，并及时更新基本配置信息库；

c） 应建立合法无线接入设备和合法移动终端配置库，用于对非法无线接入设备和非法移动终端的识别。

9.2.4.7 监控和审计管理

本项要求包括：

a） 移动终端管理服务端对移动终端状态、资源使用、软件运行等应进行监控和审计；

b） 应对上线后的业务移动应用软件进行监测。

9.2.4.8 备份与恢复管理

本项要求包括：

a） 应识别需要定期备份的移动终端中的重要业务信息、系统数据及软件系统等；

b） 应规定备份信息的备份方式、备份频度、存储介质、保存期等；

c） 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。

9.2.4.9 安全事件处置

本项要求包括：

a） 应报告所发现的移动互联安全弱点和可疑事件；

b） 应明确安全事件的报告和处置流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责；

c） 应针对移动互联系统发生的安全事件制定应急处置预案。

10 第五级安全要求

（略）

参考文献

[1] GB/T18336-2015 信息技术 信息技术安全性评估准则
[2] GB/T19716-2005 信息技术 信息安全管理实用规则
[3] GB/T 20269-2006 信息安全技术 信息系统安全管理要求
[4] GB/T 20270-2006 信息安全技术 网络基础安全技术要求
[5] GB/T 20271-2006 信息安全技术 信息系统通用安全技术要求
[6] GB/T 20272-2006 信息安全技术 操作系统安全技术要求
[7] GB/T 20273-2006 信息安全技术 数据库管理系统安全技术要求
[8] GB/T 20282-2006 信息安全技术 信息系统安全工程管理要求
[9] NIST Special Publication 800-53 联邦信息系统推荐性安全控制措施
[10] DoD Directive & Instruction 8500-1，2 信息保障 & 信息保障实施
[11] ZISIA/EMCG 2014-001企业移动终端安全等级产品规范
[12] ZISIA/EMCG_2014-002-RFC-001 企业移动终端管理AIP规范
[13] ZISIA/EMCG 2014-003 企业移动智能终端应用开发、安装、运行管控机制（指南）