变更记录：

序号	变更原因	变更内容	编制（变更）人/时间	批准人/时间	备注
1	新建	全部，版本A/0	葛方隽/2021.3	吕萍/2021.3	

移动互联安全拓展要求（S3A3G3）作业指导书					
控制点	**安全要求**	**要求解读**	**测评方法**	**预期结果或主要证据**	**符合情况**
无线接入点的物理位置	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	无线接入设备的安装位置选择不当，易被攻击者利用，特别是通过无线信号过度覆盖的弱点进行无线渗透攻击， 因此要选择合理的位置安装无线接入设备	1)核查无线接入设备的物理位置、确定无线信号的覆盖范围 2)测试无线信号的覆盖范围，测试在一定范围内是否可以进行渗透攻击与电磁干扰等	1)无线接入设备的部署方案 2)无线接入设备的物理部署位置合理 3)无线接入信号覆盖范围在合理范围内，未出现过度覆盖或被电磁干扰	符合情况：无线接入设备部署于XXX，各无线接入设备之间相隔一定距离，可避免过度覆盖及电磁干扰。 部分符合情况：无 不符合情况：无线接入设备部署于XXX，部署区域比较密集。
边界防护	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	保证无线网络与有线网络之间的网络边界隔离与安全访问控制，要求在有线网络与无线网络边界之间的和数访问和数据流通过无线接入网关设备，防止无线安全防护边界缺失	1)查阅网络拓扑结构图（含有线网络、无线网络，是否有明确边界划分，是否通过接入网关设备互联； 2）实地核查接入网关设备部署方式和位置。	1)在有线网络与无线网络边界之间部署无线接入网关设备	符合情况：有线网络与无线网络边界之间部署有无线接入网关设备，有线网络与无线网络边界之间的访问和数据流须通过无线接入网关设备。 部分符合情况：有线网络与无线网络边界之间部署有无线接入网关设备，无线网关设备策略不严谨。 不符合情况：有线网络与无线网络边界之间无无线接入网关设备。
访问控制	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模块进行认证	为保证无线接入终端的安全接入，可在无线接入设备上开启认证功能，部署认证服务器对无线接入终端认证，也可以采用国家密码管理机构批准的密码模块的认证	核查是否开启接入认证功能，是否采用认证服务器或国家密码管理机构批准的密码模块进行认证	1)无线接入设备开启接入认证功能，移动终端接入需要进行认证； 2)采用认证服务器或国家密码管理机构批准的密码模块进行认证。	符合情况：1.无线接入设备已开启接入认证功能，已禁止使用WEP方式，使用了【WPA-PSK/WPA2-PSK】认证方式，口令长度8位以上。2.无线接入设备已开启接入认证功能，采用认证服务器/国家密码管理机构批准的密码模块进行认证。 部分符合情况：无线接入设备具有认证功能，未采用符合国家密码管理机构批准的密码模块。 不符合情况：无线接入设备无接入认证功能。

入侵防范	a)应能检测到非授权的无线接入设备和非授权的移动终端的接入行为	保证接入到无线网络中的无线设备均为已授权的无线设备，防止私搭乱建无线网络所带来的安全隐患，比如网络中用户自己搭建的非法wifi,，或恶意搭建的wifi钓鱼等	1)核查是否能够检测到非授权的无线接入设备和非授权的移动终端的接入行为 2)测试验证是否能够检测非授权的无线接入设备和非授权的移动终端的接入行为	1)通过无线入侵检测/防范系统(WIDS/WIPS)能够检测到非授权无线接入设备和移动终端的接入行为 2)具有非授权无线接入设备和移动终端接入的检测日志	符合情况：通过无线入侵检测/防范系统(WIDS/WIPS)能够检测到非授权无线接入设备和移动终端的接入行为，具有非授权无线接入设备和移动终端接入的检测日志。 部分符合情况：无 不符合情况：未采取措施对非授权无线接入设备和移动终端接入网络进行检测。
	b)应能够检测到针对无线接入设备的网络扫描、DDoS攻击、密钥破解、中间人攻击和欺骗攻击等行为	为保证无线接入设备的安全性，防止被攻击者采用技术手段进行攻击，要求能够对无线网络攻击进行检测与记录	1)核查是否能够对网络扫描、DDoS攻击、密钥破解、中间人攻击和欺骗攻击等行为进行检测 2)核查规则库版本是否及时更新	1)通过无线入侵检测/防范系统(WIDS/WIPS)能够检测到对无线网络的扫描和攻击行为; 2)具有无线网络攻击行为的检测日志; 3)无线入侵检测/防范(WIDS/WIPS)的规则库及时更新。	符合情况：部署有抗APT攻击系统/网络回溯系统/威胁情报检测系统/抗DDoS攻击系统/入侵保护系统，设备规则库已更新至最新，可对网络扫描、DDoS攻击、密钥破解、中间人攻击和欺骗攻击等行为进行检测。 部分符合情况：部署有抗APT攻击系统/网络回溯系统/威胁情报检测系统/抗DDoS，规则库未进行定期更新。 不符合情况：未采取措施对网络扫描、DDoS攻击、密钥破解、中间人攻击和欺骗攻击等行为进行检测。
	c)应能够检测到无线设备的SSID广播、WPS等高风险功能的开启状态	为保证无线接入设备的安全性，应检测内部无线网络接入设备的SSID广播、WPS等高风险功能的是否已关闭，如发现未关闭时应及时关闭相关高风险功能	1）核查是否能够检测 无线网络接入设备的SSID广播、WPS等高风险功能的开启状态; 2）检查无线网络接入设备的SSID广播、WPS功能是否关闭。	1)具有无线接入设备的SSID广播、WPS等高风险功能开启状态的检测日志; 2)无线接入设备的SSID广播、WPS功能已关闭。	符合情况：部署有XXX设备，能够检测无线接入设备的SSID广播、WPS等高风险功能的开启状态。 部分符合情况：无 不符合情况;无线接入设备和无线接入网关未禁用SSID广播及WEP认证功能。

	d)应禁止多个AP使用同一个鉴别密钥	为保证无线AP的安全，禁止多个AP使用同一个鉴别密钥。比如：使用同一个认证密钥一旦被破解则使用相同密钥的AP都面临相同风险	1）查看无线AP的管理员登录口令设置，核查是否分别使用了不同的鉴别密钥	1)不同的无线AP的管理员登录口令不同	符合情况：无线接入网关与各个AP之间使用了不同的认证密钥，不同的无线AP的管理员登录口令不同。 部分符合情况：无 不符合情况：无线接入网关与各个AP之间使用了相同的认证密钥。
	e)应能够阻断非授权无线接入设备或非授权移动终端	为保证接入无线网络中的设备和终端均为授权终端，要求定位和阻断非授权无线接入设备或非授权移动终端。比如：发现非授权无线接入设备，采用地址冲突等方式进行阻断	1)应核查是否能够阻断非授权无线接入设备或非授权移动终端接入 2)应测试验证是否能够阻断非授权无线接入设备或非授权移动终端接入	1)部署无线防范系统(WIPS)，设置了阻断策略，并具有阻断日志； 2)经测试非授权无线接入设备或非授权移动终端不能接入。	符合情况：部署有终端准入控制系统/移动终端管理系统，可对非授权的无线接入设备及移动终端进行检测阻断，保留有阻断日志。 部分符合情况：部署有终端准入控制系统/移动终端管理系统，对非授权的无线接入设备及移动终端进行检测阻断，无相关的日志信息。 不符合情况：未部署移动终端管理系统，无法对无线接入设备或移动终端进行控制管理。
移动终端管控	a)应保证移动终端安装、注册并运行终端管理客户端软件	为保证移动终端的安全性，应按照统一的生命周期管理对移动终端管理，移动终端应安装、注册并并运行终端管理客户端软件	应核查移动终端是否安装、注册并运行终端管理客户端软件	1)移动终端安装，注册并运行了客户端软件 2)移动终端管理软件服务端相关客户端的记录	符合情况：移动终端安装，注册并运行了客户端软件，移动终端管理软件服务端具备相关客户端的记录。 部分符合情况：移动终端安装，注册并运行了客户端软件，移动终端管理软件服务端无相关客户端的记录。 不符合情况：移动终端未安装有终端管理软件。

	b)移动终端应接受移动终端管理服务端的设备命周期管理、设备远程控制，如：远程锁定、远程擦除等	为保证移动终端的远程可管可控，防止设备丢失造成的数据泄漏等安全风险，要求移动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。比如：远程移动端数据擦除	1)应核查移动终端管理系统是否设置了对移动终端进行设备远程控制及设备生命周期管理等安全策略 2)应测试验证是否能够对移动终端进行远程锁定和远程擦除等	1)移动终端管理服务端设置安全策略，能够对移动终端设备远程控制 2)移动终端管理服务端安全策略配置	符合情况：移动终端通过移动管理服务端管理控制，通过策略下发，管理端可以对移动终端进行远程控制，如软件安装、终端锁定、设备擦除等。 部分符合情况：无 不符合情况：无移动管理服务端对移动终端进行管控。
移动应用管控	a)应具有选择应用软件安装、运行的功能	为保证移动终端应用软件安装与运行的可管可控 要求对移动终端管理客户端的应用软件安装与运行的功能进行管理，以选择是否安装应用软件，运行哪些功能等	应核查是否具有应用软件安装、运行的功能	1)移动终端管理服务端设置的安全策略，能够对移动终端的应用软件安装进行控制 2)移动终端管理服务端设置的安全策略	符合情况：通过管理端控制移动终端安装、运行的移动应用软件。 部分符合情况：无 不符合情况：无移动管理端，移动终端可以随意安装运行移动应用软件。
	b)应只允许指定证书签名的应用软件安装和运行	为保证移动终端应用安装的可管可控，要求对移动应用软件使用指定的证书进行签名，保证安装文件的完整性，防止被恶意用户篡改	应核查移动应用是否由指定证书签名	1)移动应用使用了指定证书进行签名 2)使用的证书以及证书签发机构	符合情况：移动应用由指定证书签名，从可信任应用市场下载或具备可信任证书签名。 部分符合情况：无 不符合情况：移动应用未通过指定证书签名。
	c)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	为保证移动终端应用安装的可管可控，在移动终端管理系统中加入白名单，控制移动终端软件的应用安装范围，仅允许白名单内的移动应用进行安装、运行。比如:设置白名单仅允许安装企业建设的移动应用商店内的移动应用	1)应核查是否具有软件白名单功能 2)应测试验证白名单功能是否能够控制应用软件安装、运行	1)移动终端管理服务端设置白名单，能够对移动终端的应用软件安装进行控制 2)移动终端管理服务端设置的白名单	符合情况：移动应用软件通过管理服务端设置白名单进行管理控制，管理端专人管理。 部分符合情况：移动管理服务端能够通过白名单控制应用软件的安装和运行，但无专人管理服务端。 不符合情况：无移动管理服务端，无法控制应用软件安装和运行。

移动应用软件采购	a)应保证移动终端安装、运行的应用软件来自可靠分发渠道或使用可靠证书签名	要求移动终端安装、运行的应用软件应采用证书进行签名，保证应用软件的完整性，或者要求使用可靠的移动应用软件的分发渠道，降低移动应用软件安装带来的风险	应核查移动应用软件是否来自可靠分发渠道或使用可靠证书签名	1)移动应用软件下载使用来自于官网或内部应用商店等可靠渠道 2)移动应用软件采用签名证书	符合情况：移动应用软件可通过官网二维码、应用商店、百度等正规渠道下载安装，并且移动应用软件采用可靠的签名证书。 部分符合情况：移动应用软件通过公司内部提供地址下载安装，未采用可靠的签名证书。 不符合情况：移动应用软件未采用证书进行签名，未通过正规渠道下载安装。
	b)应保证移动终端安装、运行的应用软件由指定的开发者开发	为保证移动终端安装的移动应用软件件的安全性，要求安装使用的移动应用软件需要由指定的开发者开发，比如：移动终端安装、运行的移动终端管理软件应明确开发单位/开发者等	应核查移动应用否由指定的开发者开发	1)移动应用软件由指定的开发者开发 2)移动应用软件开发者单位及开发者相关信息	符合情况：移动应用软件由公司研发组正式员工开发，并签署有相关保密协议。 部分符合情况：移动应用软件由公司研发组正式员工开发，未签署有相关保密协议。 不符合情况：移动应用软件由外包单位或其他非正式员工开发，开发者与公司也未签订相关保密协议。
移动应用软件开发	a)应对移动业务应用软件开发者进行资格审查	为保证移动业务应用软件的安全性，要求对开发者进行基本的资格审查。比如：工作简历、技术能力、资格证书、项目实施情况等	应访谈系统建设负责人，是否对开发者进行资格审查	1)移动应用开发者的资格符合要求 2)移动应用开发者资格审查记录或相关资质材料	符合情况：所有移动应用开发者为单位正式员工，签订有保密协议，每年会进行技术考核，持证上岗，具备考核记录。 部分符合情况：所有移动应用开发者为单位正式员工，签订有保密协议，未进行资质审查和考核。 不符合情况：所有移动应用开发者非单位正式员工，也未进行能力考核和资质审查。

	b)应保证开发移动业务应用软件的签名证书合法性	为保证移动业务应用软件所采用的证书的合法性，要求采用国家移动业务应用软件的签名证书是否具有合法性	应核查开发移动业务应用软件的签名证书是否具有合法性	1)移动业务应用软件的签名证书具有合法性 2)签名证书的签发机构	符合情况：移动业务应用软件的签名证书由合法的认证机构颁发，具备合法性。 部分符合情况：移动业务应用软件的签名证书未经过认证。 不符合情况：移动业务应用软件的签名证书未经过合法认证。
配置管理	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	为保证无线接入设备和移动终端的安全接入，要求对无线接入设备和移动终端的设备情况进行登记和记录，形成合法设备配置库、当设备接入无线网络时进行比对，如不在配置库内则认为非法设备，不允许接入	应核查是否建立无线接入设备和合法移动终端配置库，并通过配置库识别非法设备	1)建立无线接入设备和合法移动终端配置库，并可以进行比对识别 2)无线接入设备和合法移动终端配置库信息	符合情况：将所有合法无线接入设备和合法移动终端ID信息纳入现有配置库，可对非法设备识别、阻断。 部分符合情况：无 不符合情况：未建立无线接入设备、移动终端配置管理库，未对无线接入设备和移动终端进行识别、控制。