ICS 35.240.99
CCS A 90

GA

# 中华人民共和国公共安全行业标准

GA/T 1987—2022

# 执法记录仪接入移动警务系统技术要求

**Technical requirements for portable recording equipment for law enforcement accessing the mobile police information system**

2022-05-26 发布　　2022-07-01 实施

中华人民共和国公安部　发布

# 目　　次

# 前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由公安部科技信息化局提出。

本文件由公安部通信标准化技术委员会归口。

本文件起草单位：公安部科技信息化局、甘肃省公安厅、公安部第一研究所、公安部特种警用装备质量监督检验中心、成都鼎桥通信技术有限公司、深圳警翼软件技术有限公司、北京迅安网络系统有限责任公司、苏州科达科技股份有限公司、杭州海康威视数字技术股份有限公司。

本文件主要起草人：康鹏、陈妍、谢峰、袁艺芳、卢煜、邹慧莹、支文强、欧阳甸、卢玉华、张双双、苏智睿、苑雪、张江涛、王璐、徐艺谋、于炳虎、贺晓巍、王晋波。

# 执法记录仪接入移动警务系统 技术要求

## 1 范围

本文件规定了执法记录仪接入移动警务系统的通用技术要求、安全技术要求、安全监控组件技术要求和检测方法。

本文件适用于接入移动警务系统的执法记录仪的设计、研制和检测等。

## 2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GA/T 947(所有部分) 单警执法视音频记录系统

GA/T 1466.1—2018 智能手机型移动警务终端 第1部分：技术要求

GA/T 1466.2—2018 智能手机型移动警务终端 第2部分：安全监控组件技术规范

GA/T 1561—2019 移动警务系统 总体技术要求

GA/T 1720 移动警务 数字证书格式技术要求

GA/T 1737—2020 公安移动信息网技术要求

GA/T 1768 移动警务 身份认证技术要求

## 3 术语和定义、缩略语

### 3.1 术语和定义

GA/T 1466.1—2018、GA/T 1466.2—2018、GA/T 1561—2019、GA/T 1737—2020 界定的术语和定义适用于本文件。

3.1.1

**移动警务系统 mobile police information system**

利用移动终端通过无线网络处理警务信息的系统。

[来源：GA/T 1561—2019，3.1.1]

3.1.2

**移动警务终端 mobile police terminal**

在移动警务系统中处理移动警务信息的无线终端设备。

[来源：GA/T 1561—2019，3.1.3]

3.1.3

**静态可信度量 trusted static measurement**

针对系统镜像、内核驱动、服务、应用进行的启动前完整性检查和合法性判断。移动警务终端处于出厂状态第一次引导时或系统镜像更新后第一次引导时自动采集生成静态可信度量基准值，并在合法

的应用安装时自动更新。

[来源:GA/T 1466.1—2018,3.1.6]

3.1.4

**基准值 base value**

用于判断度量目标完整性和合法性的依据。

[来源:GA/T 1466.1—2018,3.1.5]

3.1.5

**无线专用传输链路 wireless private transmission link**

在公众和专用等无线通信网络上,专用于承载移动警务系统接入的 APN 或 VPDN 传输链路。

[来源:GA/T 1466.1—2018,3.1.1]

3.1.6

**公安移动信息网 police mobile information network**

移动警务系统联网服务子平台(Ⅱ类区域)的网络基础设施。

[来源:GA/T 1737—2020,3.1.2]

3.1.7

**安全监控组件 security monitoring and controlling plugin**

运行于移动警务终端,具有终端注册、终端登录、管控策略解析执行及结果上报、终端信息采集上报、安全事件监测上报等安全监控功能的软件。

[来源:GA/T 1466.2—2018,3.1.1]

## 3.2 缩略语

下列缩略语适用于本文件。

APN:接入点名称(Access Point Name)

CN:数字证书主体通用名称(Common Name)

CPU:中央处理器(Central Processing Unit)

ICCID:集成电路卡识别码(Integrate Circuit Card Identity)

IMEI:国际移动设备身份码(International Mobile Equipment Identity)

IP:网际协议(Internet Protocol)

MAC:介质访问控制(Media Access Control)

MEID:移动设备识别码(Mobile Equipment IDentifier)

MTP:媒体传输协议(Media Transfer Protocol)

NFC:近场通信(Near Field Communication)

PKI:公钥基础设施(Public Key Infrastructure)

PTP:图片传输协议(Picture Transfer Protocol)

PWL:警用无线局域网(Police Wireless LAN)

SIM:客户识别模块(Subscriber Identity Module)

SSO:单点登录(Single Sign On)

USB:通用串行总线(Universal Serial Bus)

VPDN:虚拟专用拨号网(Virtual Private Dial-up Network)

WLAN:无线局域网(Wireless Local Area Network)

# 4 通用技术要求

接入移动警务系统的执法记录仪应符合如下技术要求:

a) 符合 GA/T 1561—2019 中 5.1.2 的要求；
b) 符合 GA/T 947.2 的要求；
c) 具有标识硬件唯一性的 IMEI 号，且不应被更改；
d) 具备无线电发射能力的执法记录仪，具有无线电发射设备型号核准证；
e) 具备公用电信网接入能力的执法记录仪，具有电信设备进网许可证。

## 5 安全技术要求

### 5.1 安全体系

安全体系主要包括五部分：操作系统安全、应用层安全、网络连接安全、外围接口安全和用户数据安全。网络连接安全和外围接口安全涉及操作系统安全，用户数据安全涉及操作系统安全和应用层安全，如图 1 所示。

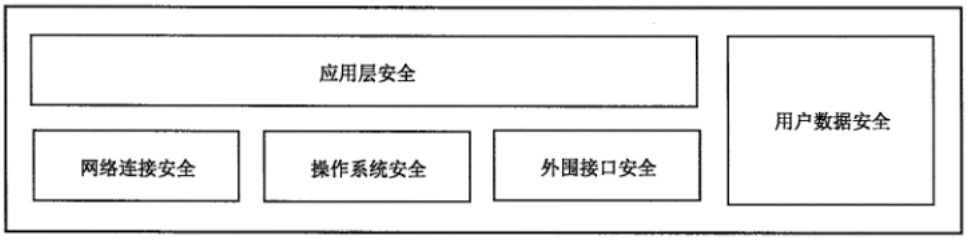


图 1 安全体系

### 5.2 操作系统

操作系统安全性应符合如下技术要求：

a) 防止非法获取系统的超级管理员权限；
b) 不存在已知严重和高危系统漏洞；
c) 在未获得用户确认的情况下，不主动向未知和未授权服务器发送个人信息，包括但不限于键盘或手写输入信息、用户位置信息、MAC 或 IP 地址、硬件标识信息；
d) 提示网络连接状态，在界面上给出相应的状态提示；
e) 提示网络数据传送状态，在界面上给出相应的状态提示；
f) 不以明文的方式保存和传送口令，输入口令时不明文回显；
g) 支持离线/在线方式升级更新，且只使用授权的升级包进行升级；
h) 不准许用户通过系统菜单进行恢复出厂操作。

### 5.3 应用层

应用层安全性应符合如下技术要求。

a) 安装安全监控组件。
b) 对支持安装第三方应用的执法记录仪，采用国产商用密码算法对应用进行安全认证，利用移动警务应用签名证书对应用安装包或更新包进行来源检查和完整性检查，只安装验签成功的应用。
c) 对应用进行静态可信度量。在应用启动时按基准值检查其完整性，若应用的完整性被破坏，则阻止其运行。
d) 对支持安装第三方应用的执法记录仪，具备浏览和配置应用开机自启动的功能。

### 5.4 网络连接

网络连接安全性符合如下技术要求。

a) 应通过预置网络连接参数或管控接口配置，只准许通过无线专用传输链路接入公安移动信息网，不应与互联网连接。

b) 应采用基于移动警务 PKI 数字证书的身份认证接入公安移动信息网，身份认证应符合 GA/T 1768的规定，证书格式应符合 GA/T 1720 的规定；宜通过数字证书、口令、生物标识、设备标识等方式进行用户和设备的自动关联。

c) 应通过预置 WLAN 功能策略或管控接口配置，不准许开启热点，并限制 PWL 之外的无线局域网只用于采集热点信息。

d) 当执法记录仪通过 USB 接口连接执法数据采集设备时，不应使用无线连接，包括但不限于移动网络、WLAN、蓝牙、NFC 等。

### 5.5 外围接口

外围接口安全性应符合如下技术要求：

a) NFC 支持通过管控接口配置是否开启，并给出相应的状态提示；

b) 通过预置蓝牙连接策略或管控接口配置，限制蓝牙只准许连接指定设备，并给出相应的状态提示；

c) 通过预置 USB 接口策略或管控接口配置，只准许符合 GA/T 947(所有部分)规定的执法数据采集设备通过 USB 接口从执法记录仪采集数据或者配置参数，其他场景下限制 USB 接口只用于充电，并给出相应的状态提示。

### 5.6 用户数据

用户数据安全性应符合如下技术要求：

a) 保证用户数据不被未授权用户查询、删除和修改；

b) 支持远程锁定执法记录仪；

c) 远程控制不应具有数据擦除、恢复出厂以及存储格式化的功能。

## 6 安全监控组件技术要求

### 6.1 运行环境

安全监控组件的运行环境应符合 GA/T 1466.2—2018 第 4 章的要求。

### 6.2 一般要求

安全监控组件的一般要求应符合 GA/T 1466.2—2018 第 5 章的要求。

### 6.3 功能要求

#### 6.3.1 参数设置

安全监控组件的参数设置应符合 GA/T 1466.2—2018 中 6.1 的要求。

#### 6.3.2 注册

安全监控组件的注册应符合 GA/T 1466.2—2018 中 6.2 的要求。

#### 6.3.3 登录

安全监控组件的登录应符合 GA/T 1466.2—2018 中 6.3 的要求。

#### 6.3.4 策略更新

安全监控组件的策略更新应符合 GA/T 1466.2—2018 中 6.4 的要求。

#### 6.3.5 策略解析及执行

安全监控组件应按照 GA/T 1466.2—2018 附录 A 解析管控策略，调用 GA/T 1466.2—2018 中 B.2 实现管控能力，应包括但不限于 6.3.7 规定的管控能力。当不具备所依赖的硬件或系统模块时，对应的管控能力可不予以实现。

#### 6.3.6 执行结果反馈

安全监控组件的执行结果反馈应符合 GA/T 1466.2—2018 中 6.6 的要求。

#### 6.3.7 管控能力

##### 6.3.7.1 硬件模块管控

硬件模块管控除符合 GA/T 1466.2—2018 中 6.7.1.1～6.7.1.7、6.7.1.14 的要求外，还应符合如下要求。

a) WLAN 控制应支持以下方式：
   ——禁止使用：不准许使用 WLAN 功能；
   ——仅 PWL 或指纹扫描：只准许接入 PWL 网络或扫描 WLAN 指纹，无法接入 PWL 之外的其他 WLAN 无线网络。
b) USB 工作模式控制应支持以下方式：
   ——仅充电和采集：对于连接执法数据采集设备的场景，只准许充电、采集数据或配置参数，其他场景下只准许充电；
   ——不管控：可使用所有 USB 工作模式，如 MTP 模式、PTP 模式、主机模式等。

##### 6.3.7.2 基本功能管控

基本功能管控除符合 GA/T 1466.2—2018 中 6.7.2.1～6.7.2.6、6.7.2.12、6.7.2.13 的要求外，还应符合如下要求。

a) 开发调试模式控制应支持以下方式：
   ——禁止使用：不准许使用开发调试模式；
   ——不管控：可使用开发调试模式。
b) 开发调试模式应用安装/卸载功能控制应支持以下方式：
   ——禁止使用：不准许使用开发调试模式安装/卸载应用；
   ——不管控：可使用开发调试模式安装/卸载应用。

##### 6.3.7.3 应用管控

应用管控应符合 GA/T 1466.2—2018 中 6.7.3 的要求。

##### 6.3.7.4 监测采集管控

监测采集管控应符合 GA/T 1466.2—2018 中 6.7.4 的要求。

#### 6.3.7.5 管控策略围栏

管控策略围栏应符合 GA/T 1466.2—2018 中 6.7.6 的要求。

#### 6.3.7.6 远程控制和配置

远程控制和配置应符合 GA/T 1466.2—2018 中 6.7.7.1、6.7.7.3～6.7.7.7、6.7.7.9～6.7.7.11 的要求。

### 6.3.8 升级

安全监控组件的升级应符合 GA/T 1466.2—2018 中 6.8 的要求。

## 6.4 性能要求

安全监控组件的性能要求应符合 GA/T 1466.2—2018 第 7 章的要求。

## 6.5 接口要求

### 6.5.1 应用服务类接口

安全监控组件的应用服务类接口应符合 GA/T 1466.2—2018 中 8.2.1～8.2.3 的要求。

### 6.5.2 管控类接口

#### 6.5.2.1 总体要求

安全监控组件的管控类接口应满足以下要求：

a) 接口由“ga.mdm.PolicyManager”定义；

b) 调用权限受操作系统控制，方式包括但不限于只准许指定应用访问、不限制调用。

#### 6.5.2.2 硬件模块管控接口

硬件模块管控接口应符合 6.3.7.1 的要求，接口定义详见 GA/T 1466.2—2018 中 B.2.1。

a) WLAN 管控接口的参数 mode 取值的含义为：

——mode=0：禁止使用无线网络；

——mode=1：只准许接入 PWL 网络或进行无线网络指纹扫描。

b) USB 工作模式控制接口的参数 mode 取值的含义为：

——mode=0：对于连接执法数据采集设备的场景，只准许充电、采集数据或配置参数，其他场景下只准许充电；

——mode=1：可使用所有 USB 工作模式。

#### 6.5.2.3 基本功能管控接口

基本功能管控接口应符合 6.3.7.2 的要求，接口定义详见 GA/T 1466.2—2018 中 B.2.2。

a) 开发调试模式控制接口的参数 mode 取值的含义为：

——mode=0：不准许使用开发调试模式；

——mode=1：可使用开发调试模式。

b) 开发调试模式应用安装/卸载功能控制接口应按照 GA/T 1466.2—2018 中 B.2.2 的应用 ADB 方式安装/卸载功能控制接口定义。其中，参数 mode 取值的含义应为：

——mode=0：不准许使用开发调试模式安装/卸载应用；

——mode=1：可使用开发调试模式安装/卸载应用。

#### 6.5.2.4 应用管控接口

应用管控接口应符合 6.3.7.3 的要求，接口定义详见 GA/T 1466.2—2018 中 B.2.3。

#### 6.5.2.5 监测采集管控接口

监测采集管控接口应符合 6.3.7.4 的要求，接口定义详见 GA/T 1466.2—2018 中 B.2.4。

#### 6.5.2.6 远程控制和配置接口

远程控制和配置接口应符合 6.3.7.6 的要求，接口定义详见 GA/T 1466.2—2018 中 B.2.6。

## 7 检测方法

### 7.1 通用技术要求检测

通用技术要求检测方法如下：

a) 核查执法记录仪是否具有按照 GA/T 947.2 检测出具的检测报告；
b) 进入操作界面，手动检查执法记录仪 IMEI 码，检查所有菜单是否有可供修改 IMEI 码的功能项或入口，判定结果是否符合第 4 章 c)的要求；
c) 检查执法记录仪是否具备无线电发射能力，对于具备无线电发射能力的执法记录仪，核查厂家提供的无线电发射设备型号核准证书；
d) 检查执法记录仪是否具备公用电信网接入能力，对于具备接入公用电信网的执法记录仪，核查厂家提供的电信设备进网许可证书。

### 7.2 安全技术要求检测

#### 7.2.1 操作系统安全性检测方法

操作系统安全性检测方法如下。

a) 防止非法获取系统的超级管理员权限检测方法：
   1) 对执法记录仪进行获取 ROOT 权限操作；
   2) 检查执法记录仪的用户权限；
   3) 判定结果是否符合 5.2 a)的要求。
b) 严重和高危系统漏洞检测方法：
   1) 保证执法记录仪网络通信功能正常；
   2) 对执法记录仪进行系统漏洞检测，观察检测结果；
   3) 检查执法记录仪防病毒软件库或补丁是否覆盖自送检日前 3 个月官方权威发布的系统严重和高危等级漏洞；
   4) 判定结果是否符合 5.2 b)的要求。
c) 不主动向未知和未授权服务器发送个人信息检测方法：
   1) 保证执法记录仪网络通信功能正常；
   2) 使用移动网络报文抓取工具抓取执法记录仪通信数据报文，分析抓取的通信数据报文；
   3) 判定结果是否符合 5.2 c)的要求。
d) 网络连接状态检测方法：
   1) 保证执法记录仪网络通信功能正常；

2) 执法记录仪连接移动通信网络，检查是否具有网络连接状态提示；
3) 判定结果是否符合 5.2 d)的要求。

e) 网络数据传送状态检测方法：
1) 保证执法记录仪网络通信功能正常；
2) 执法记录仪通过移动通信网络传送数据，检查是否具有数据传送状态提示；
3) 判定结果是否符合 5.2 e)的要求。

f) 保存和传送口令方式检测方法：
1) 保证执法记录仪网络通信功能正常；
2) 使用厂商提供的获取日志方案，查看保存和传送方式是否为明文；
3) 判定结果是否符合 5.2 f)的要求。

g) 操作系统升级检测方法。
1) 保证执法记录仪网络通信功能正常。
2) 通过在线方式验证授权升级包，执法记录仪应能执行授权升级包的升级操作；通过在线方式验证非授权升级包，执法记录仪应能识别非授权升级包并拒绝升级操作，同时给出相应提示。
3) 通过离线方式验证授权升级包，执法记录仪应能执行授权升级包的升级操作；通过离线方式验证非授权升级包，执法记录仪应能识别非授权升级包并拒绝升级操作，同时给出相应提示。
4) 判定结果是否符合 5.2 g)的要求。

h) 不准许用户通过系统菜单进行恢复出厂操作检测方法：
1) 进入系统菜单界面，检查执法记录仪是否有恢复出厂设置选项；
2) 判定结果是否符合 5.2 h)的要求。

#### 7.2.2 应用层安全性检测方法

应用层安全性检测方法如下。

a) 移动警务应用认证检测方法：
1) 在执法记录仪上安装经过移动警务应用签名证书正确签名的应用，查看是否能成功安装此应用；
2) 在执法记录仪上分别安装未经过移动警务应用签名证书签名的以及经移动警务应用签名证书签名后二次篡改的、签名信息来源非法的、签名证书有效期失效的应用，查看是否能阻止以上应用安装并给出提示；
3) 判定结果是否符合 5.3 b)的要求。

b) 应用程序静态可信度量检测方法：
1) 篡改执法记录仪中已安装的应用文件，即破坏应用的完整性，当再次启动该应用时，查看执法记录仪是否能阻止该应用启动并给出提示；
2) 判定结果是否符合 5.3 c)的要求。

c) 第三方应用开机自启动程序监控检测方法：
1) 审查执法记录仪开机自启动程序监控及使用说明；
2) 查看执法记录仪是否能监控第三方应用开机自启动，并进行配置是否允许第三方应用开机自启动操作；
3) 判定结果是否符合 5.3 d)的要求。

#### 7.2.3 网络连接安全性检测方法

网络连接安全性检测方法如下。

a) 连接无线专用传输链路检测方法。
   1) 在执法记录仪中安装支持无线专用传输链路的 SIM 卡，连接无线专用传输链路，查看执法记录仪是否能正常连接无线专用传输链路。
   2) 在执法记录仪中安装支持无线专用传输链路的 SIM 卡，连接互联网，查看执法记录仪是否能连接互联网；在执法记录仪中安装不支持无线专用传输链路的 SIM 卡，连接互联网，查看执法记录仪是否能连接互联网。
   3) 判定结果是否符合 5.4 a)的要求。
b) 移动警务 PKI 数字证书认证检测方法：
   1) 审查身份认证是否符合 GA/T 1768 和 GA/T 1720 的要求；
   2) 检查用户和设备自动关联方式；
   3) 判定结果是否符合 5.4 b)的要求。
c) WLAN 连接安全性检测方法：
   1) 使用 WLAN 连接非 PWL 的无线网络，查看执法记录仪是否能采集热点信息，查看执法记录仪是否能连接无线网络；
   2) 对执法记录仪进行开启热点操作，查看是否可以作为 WLAN 热点；
   3) 对执法记录仪进行开启直连操作，查看是否可以开启直连、与其他终端进行直连；
   4) 使用 WLAN 连接 PWL 无线网络，重复上述操作；
   5) 判定结果是否符合 5.4 c)的要求。
d) 连接执法数据采集设备时禁用无线连接检测方法：
   1) 将执法记录仪与执法数据采集设备相连接；
   2) 检查执法记录仪的移动网络、WLAN、蓝牙、NFC 等无线连接功能是否禁止；
   3) 判定结果是否符合 5.4 d)的要求。

#### 7.2.4 外围接口安全性检测方法

外围接口安全性检测方法如下。

a) NFC 通信管控安全检测方法：
   1) 基于执法记录仪厂商提供相关 NFC 通信管控操作说明，对执法记录仪的 NFC 功能进行启动和禁用操作；
   2) 启用后，应具有 NFC 通信状态提示信息并可通过 NFC 正常通信；
   3) 禁用后，执法记录仪应无法通过 NFC 与其他终端进行通信；
   4) 判定结果是否符合 5.5 a)的要求。
b) 蓝牙通信管控安全检测方法：
   1) 基于执法记录仪厂商提供的蓝牙通信管控说明，设置白名单设备；
   2) 使用白名单中的设备与执法记录仪进行蓝牙通信，应能正常通信，查看是否具有状态提示；
   3) 使用非白名单中的设备与执法记录仪进行蓝牙通信，应无法通信；
   4) 判定结果是否符合 5.5 b)的要求。
c) USB 接口和隐藏调试端口安全检测方法：
   1) 审查执法记录仪厂商提供的 USB 接口说明；
   2) 用 USB 数据线连接符合 GA/T 947(所有部分)规定的执法数据采集设备，查看执法记录仪是否可与对应的执法数据采集设备进行数据采集或参数配置；
   3) 用 USB 数据线连接非 GA/T 947(所有部分)规定的其他设备，查看执法记录仪是否能进行数据采集或参数配置，是否只能进行充电使用并给出相应提示；

4） 判定结果是否符合5.5 c)的要求。

#### 7.2.5 用户数据安全性检测方法

用户数据安全性检测方法如下。

a） 用户数据非授权访问防护检测：

1） 基于厂商提供的操作说明及授权说明对执法记录仪摄录数据进行查询操作，对第三方应用进行下载、安装和运行操作，查看系统提示；

2） 使用非授权用户访问执法记录仪，查看执法记录仪是否拒绝非授权用户对用户数据进行查询操作；

3） 判定结果是否符合5.6 a)的要求。

b） 远程锁定检测：

1） 使用移动警务终端安全管理子系统，登录测试账号，对执法记录仪执行远程锁定操作，查看结果；

2） 判定结果是否符合5.6 b)的要求。

c） 用户数据远程保护检测：

1） 使用移动警务终端安全管理子系统，登录测试账号，查看执法记录仪是否拒绝执行远程擦除或远程数据销毁命令，用户数据包括用户应用产生的操作与业务数据、用户操作日志数据和个人定制化数据等；

2） 对执法记录仪执行远程恢复出厂操作以及存储格式化操作，查看结果；

3） 判定结果是否符合5.6 c)的要求。

### 7.3 安全监控组件检测

#### 7.3.1 安全监控组件功能检测方法

##### 7.3.1.1 参数设置检测方法

参数设置检测方法如下：

a） 通过预置、短信、二维码或特定指令方式进行安全监控组件参数设置；

b） 判定结果：参数设置成功后可与对应的移动警务终端安全管理子系统进行通信。

##### 7.3.1.2 注册检测方法

注册检测方法如下：

a） 受测安全监控组件采集执法记录仪软硬件信息，包含但不限于厂商、品牌、型号、硬件标识(IMEI号或MEID号列表)、CPU型号、运行内存容量、内部存储容量、外部存储容量、操作系统版本、组件版本、SIM卡标识(ICCID号)、密码模块编号、数字证书序列号(十六进制)、用户标识(CN项)等，提交至移动警务终端安全管理子系统验证执法记录仪合法性；

b） 移动警务终端安全管理子系统验证执法记录仪合法，返回授权信息；

c） 受测安全监控组件校验授权信息；

d） 判定结果：注册成功，受测安全监控组件可登录移动警务终端安全管理子系统；注册失败，受测安全监控组件显示失败原因，并将执法记录仪恢复至注册开始前的状态。

##### 7.3.1.3 登录检测方法

登录检测方法如下：

a） 受测安全监控组件采集登录信息，包括但不限于硬件标识(IMEI号或MEID号列表)、密码模

块编号、数字证书用户标识(CN 项)、SIM 卡标识(ICCID 号),提交至移动警务终端安全管理子系统进行校验;

b) 移动警务终端安全管理子系统返回登录校验结果;

c) 判定结果:登录成功,移动警务终端安全管理子系统可通过安全监控组件控制执法记录仪。

#### 7.3.1.4 策略更新检测方法

受测安全监控组件接收移动警务终端安全管理子系统以全量或增量方式下发的管控策略,对管控策略完整性进行校验,在执法记录仪上查验管控策略更新是否执行。

#### 7.3.1.5 策略解析及执行检测方法

受测安全监控组件解析移动警务终端安全管理子系统下发的管控策略,包含但不限于 6.3.7 规定的管控能力,在执法记录仪上查验管控策略是否执行。

#### 7.3.1.6 执行结果反馈检测方法

查验移动警务终端安全管理子系统是否接收到安全监控组件上报的管控策略执行结果。

#### 7.3.1.7 管控能力检测方法

管控能力检测方法如下。

a) 按照 7.3.1.4 的检测方法向受测安全监控组件下发管控策略,包括:

1) 硬件模块管控:WLAN、移动数据网络、蓝牙、NFC、红外、生物特征识别模块、定位服务、USB 工作模式、扩展外设控制;

2) 基本功能控制:通话功能、短信功能、截屏功能、网络共享功能、APN 管理功能、网络访问规则、开发调试模式、应用交互安装/卸载接口、应用静默安装/卸载接口、开发调试模式应用安装/卸载功能控制;

3) 应用管控:应用安装、应用运行、应用更新、应用卸载、应用权限控制;

4) 监控采集管控:应用流量上报、应用耗电量上报、应用运行时长上报、应用运行异常上报、硬件信息上报、软件安装信息上报、ROOT 状态上报、系统完整性监测、硬件合规监测、应用合规监测、登录失败监测、互联网联通监测、终端失联监测、可信检测结果监测控制;

5) 管控策略围栏:时间围栏、地理围栏、WLAN 围栏、默认围栏;

6) 远程控制和配置:终端锁定/解锁、终端重启、终端关机、运行状态上报、定位信息上报、WLAN 配置推送、APN 配置推送、SSO 配置推送、验证证书推送。

b) 判定结果:在执法记录仪或移动警务终端安全管理子系统上查验管控策略是否有效执行。

#### 7.3.1.8 升级检测方法

通过移动警务终端安全管理子系统对安全监控组件强制升级,比对执法记录仪上安全监控组件升级前后的版本信息,查验安全监控组件是否升级成功。

### 7.3.2 安全监控组件性能检测方法

#### 7.3.2.1 策略执行影响检测方法

按 7.3.1.7 的要求检验过程中,观测执法记录仪操作系统、应用是否非正常运行,非正常状态包括但不限于操作系统崩溃、应用程序异常等。

#### 7.3.2.2 CPU 使用率检测方法

CPU 使用率检测方法如下：

a) 执法记录仪充电 100%后进行使用；
b) 使用厂家提供的执法记录仪 CPU 使用率查看方法，查看执法记录仪进程 CPU 使用率；
c) 查看受测安全监控组件对应应用在完整放电周期内的 CPU 使用率；
d) 判定结果：受测安全监控组件 CPU 使用率应低于 1%。

#### 7.3.2.3 运行内存占用量检测方法

运行内存占用量检测方法如下：

a) 执法记录仪充电 100%后进行使用；
b) 使用厂家提供的执法记录仪内存占用量查看方法，查看受测安全监控组件对应应用内存占用信息；
c) 判定结果：受测安全监控组件运行内存占用量应低于 100 MB。

#### 7.3.2.4 网络带宽占用量检测方法

网络带宽占用量检测方法如下：

a) 对执法记录仪进行安全监控组件注册、登录操作及策略更新操作；
b) 向执法记录仪下发应用流量上报控制策略(GA/T 1466.2—2018 中 6.7.4.1 的规定)，查看受测安全监控组件对应的网络流量消耗量，计算安全监控组件注册、登录及策略更新操作过程中网络带宽占用量；
c) 保持执法记录仪在线，查看完整放电周期受测安全监控组件对应的网络流量消耗量，计算平均网络带宽占用量；
d) 判定结果：受测安全监控组件注册、登录、策略更新过程平均网络带宽占用量应低于 100 kb/s，在线状态下平均网络带宽占用量应低于 1 kb/s。

#### 7.3.2.5 耗电量检测方法

耗电量检测方法如下：

a) 执法记录仪充电 100%后进行使用；
b) 在执法记录仪系统设置中查看完整放电周期内受测安全监控组件消耗电量；
c) 判定结果：受测安全监控组件耗电量应低于执法记录仪实际总耗电量的 5%。

#### 7.3.2.6 策略执行时延方法

策略执行时延检测方法如下：

a) 使用厂家提供的方法启动日志记录；
b) 通过移动警务终端安全管理子系统向受测安全监控组件下发对应管控策略，如 WLAN 禁止使用等；
c) 打开日志文件，查找对应管控策略执行记录，计算接受策略到执行策略的时间间隔；
d) 判定结果：策略执行时延应不超过 1 s。

### 7.3.3 安全监控组件交互接口检测方法

安全监控组件交互接口检测方法如下。

a) 在执法记录仪上安装安全监控组件交互接口检测工具，运行、调用以下接口：

1) 应用服务类接口：终端信息查询接口(GA/T 1466.2—2018 中 B.1.1 的规定)、密码模块查询接口(GA/T 1466.2—2018 中 B.1.2 的规定)、应用静默安装/卸载接口(GA/T 1466.2—2018 中 B.1.3 的规定)；
2) 管控类接口：硬件模块管控接口(GA/T 1466.2—2018 中 B.2.1 的规定)、基本功能管控接口(GA/T 1466.2—2018 中 B.2.2 的规定)、应用管控接口(GA/T 1466.2—2018 中 B.2.3 的规定)、监测采集管控接口(GA/T 1466.2—2018 中 B.2.4 的规定)、远程控制和配置接口(GA/T 1466.2—2018 中 B.2.6 的规定)。

b) 判定结果：通过接口返回值，判断交互接口是否正确。