面向国家重要信息系统的载体全生命周期管控研究及实践

汇报人：张军锋

汇报单位：航天科工三院三〇四所

汇报提纲

1 载体管控背景与需求

2 载体全生命周期管控解决方案

3 载体全生命周期管控建设效果

背景

随着信息化的发展，信息技术在国家重要信息系统内广泛应用的同时，也给信息的保密管理工作带来了严峻的挑战。信息载体的使用、存放、传递和处理已经贯穿日常生产、工作的各个环节，但由于缺乏有效的技术监管手段，对载体无法实现全生命周期的管控，从而导致涉密载体乱放、乱带、非法使用等现象时有发生，由此引发的失泄密事件日益增多，直接危害国家与军队的安全。

标准要求

国家保密法中对载体管控的相关规定：

1.8　制作、收发、传递、使用、复制、保存、维修和销毁国家秘密载体（含纸介质、磁介质、和光盘等各类物品）及其过程文件资料，应当符合国家有关保密管理规定。

分级保护技术要求中对信息输入输出、载体管控提出明确要求：

8.1.3.3制作涉密载体，应标明密级和保密期限，注明发放范围、制作数量级编号；

7.1.3.2收发涉密载体，应当履行清点、登记、编号、签收手续。

现状分析

航天科工集团第三研究院信息化工作起步时间早、发展速度快，信息化水平达到国资委A级评价水平，属于国防工业科研类单位。在**网络建设**方面，航天三院已经建成了以院主干网为中心、覆盖全国所属数17家单位的大型广域网络，联网涉密终端达到1万余台，初步具备了基于网络的语音、视频、图文档信息互联互通能力。

现状分析

在**信息安全**方面，航天三院涉密信息系统基本满足BMB17-2006、BMB20-2007、BMB22－2007标准中机密增强型防护要求，解决了航天三院涉密信息系统在环境安全、介质安全、备份与恢复、电磁泄漏发射防护、安全域边界防护、系统安全性能检测等方面的安全问题。

现状分析

航天三院**载体管控**主要分为两类：**纸质载体**和**存储类载体**。其中**纸质载体**包括通过内网打印的各类文件、通过复印产生的各类文件、外来的各类文件；**存储类载体**主要是指光盘介质和移动存储介质。

目前航天三院每年产生的内部打印文件200余万份，其中涉密文件8万余份；产生的光盘近10万张，其中涉密光盘近万张。

航天三院共有在职员工上万余人，涉密人员超过一半以上，每日产生的涉密文件打印、复印数量大，管理介质数目多，管控复杂。

现状与问题

载体输入管理方面

现状

用户可直接通过光盘将电子类文件导入到信息系统内部。
外来纸质文件个人登记留存。

安全隐患

纸质文件及光盘介质文件，无统一、唯一的身份标识，在信息系统内缺少规范化管理流程；
外来电子文件导入时，无杀毒措施，存在木马、病毒等安全隐患。

现状与问题

载体产生与制作管理方面--纸质载体的管理

现状

打印申请人员直接在单位集中打印控制点或本地进行打、复印输出。

安全隐患

缺乏对用户打印行为的有效控制；
由于采用集中打印输出管理，管理员权限过大，易造成泄密事件；
复印登记为操作人员自行进行，不利于有效管控；
打、复印件缺乏统一的标识，不利于对纸质载体的全生命周期管控。

现状与问题

载体产生与制作管理方面--存储类载体的管理

现状

刻录申请人员直接到集中刻录点或本地刻录输出，由刻录人员自行在光盘上填写编号和密级。

安全隐患

缺少对终端刻录的安全管控，无法完全杜绝涉密终端自行刻录的行为；

由于采用集中刻录管理，管理员权限过大，易造成泄密事件；

光盘编码和密级为刻录人员自行填写，并与刻录过程分两步进行，易造成光盘与标签不一致的问题 。

现状与问题

载体的流转与监控方面

现状

通过纸质文件记录载体的流转、传递与收发过程，通常由专人管理，需要单独建立纸质台帐。缺少载体边界防护与检测管理措施，对于涉密载体的非法带出、乱带乱放无法监控。

安全隐患

载体的管控人员权限过大，存在载体非法使用等安全隐患；载体流转环节缺少必要的技术管控手段，易造成载体丢失、非法带出等泄密事件。

现状与问题

载体的回收与销毁管理方面

现状

销毁载体需要工作人员主动完成，当回收时间到时，统一到集中销毁点，由专人完成载体的回收与销毁。

安全隐患

载体未及时闭环，难以追踪载体使用状态，工作人员缺少按时回收载体的意识；
载体台帐记录不完整；
无法根据载体密级设置不同的闭环管理流程，达不到精细化的回收管理要求。

载体管控需求

（1）**载体输入管理方面**

- 电子载体输入需要登记、编号；
- 电子载体输入需要负责人审批。

（2）**载体产生与制作方管理方面**

- 电子载体的输出（包括 打印、 复印、刻盘、移动存储设备输出）负责人审批及形成台账，输出形成的涉密载体（介质）可追溯、可管控、可回收。

（3）**载体流转与监控管理方面**

- 电子载体在流传过程中要能够控制知悉范围；
- 载体的借入借出及使用需要履行清点、登记、编号、分发和签收等手续，建立完备台账，严格履行审批手续；
- 载体的流转需要签收确认。

（4）**载体回收与销毁管理方面**

- 载体要及时回收闭环；
- 载体的销毁需要负责人审批及形成台账。

汇报提纲

1 载体管控背景与需求

2 载体全生命周期管控解决方案

3 载体全生命周期管控建设效果

建设目标

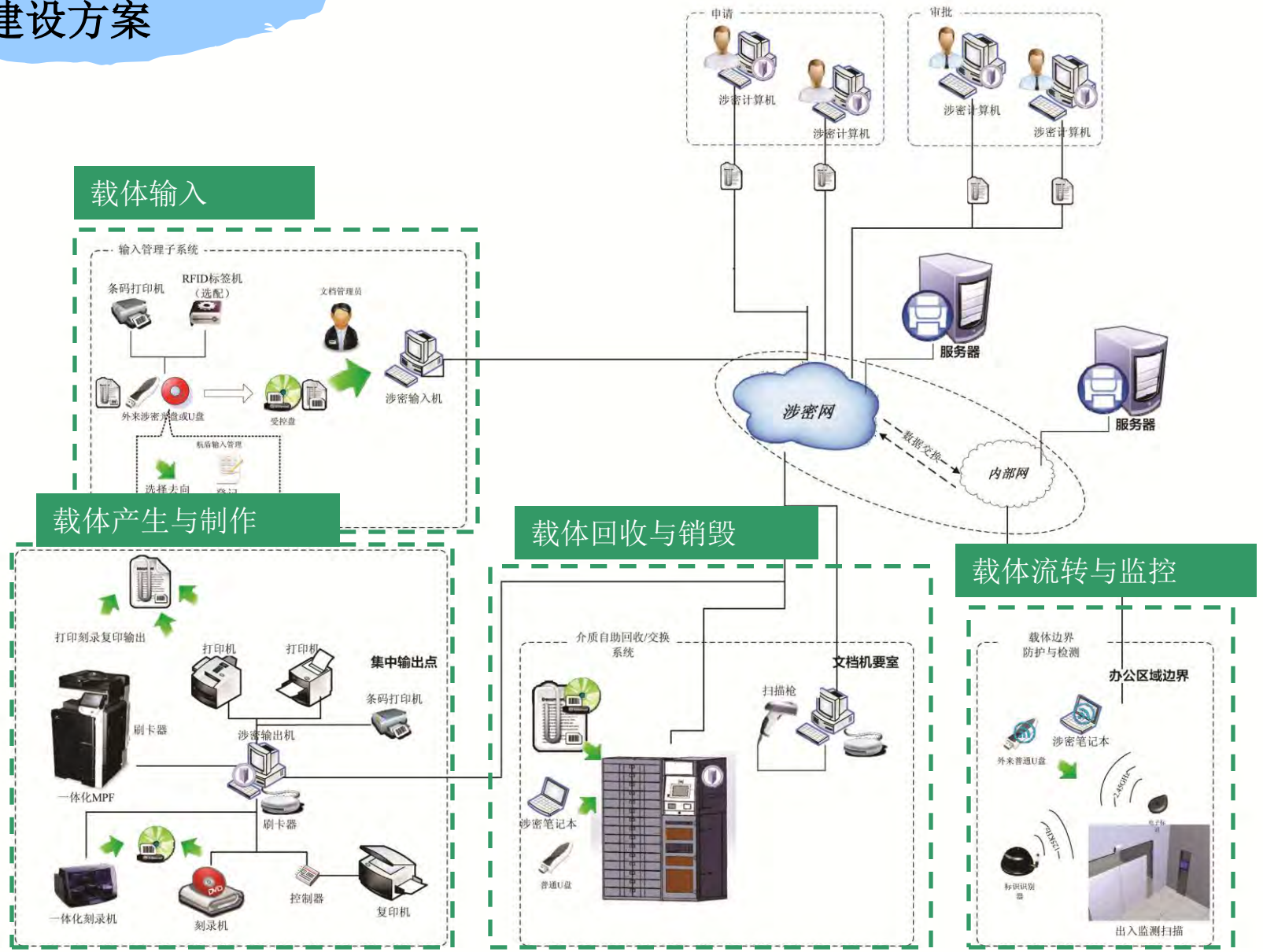
载体全生命周期管控解决方案

建设目标：实现对航天三院办公环境中使用的所有纸质介质、光盘介质、移动存储介质进行全对象、全生命周期的管控，采用技术手段对载体从产生、流转、使用到销毁几个阶段进行全程追踪及管控，最终实现对信息载体管理的流程智能化、过程自动化、控制技术化。

建设方案

项目在航天三院所有涉密单位实施，建设内容主要由**打复印安全监控与审计系统、光盘刻录监控与审计系统、基于RFID的涉密载体监控与管理系统、载体自助回收柜**组成，形成对纸质介质、光盘介质、移动存储介质的全对象、全生命周期管控。

建设方案


申请
涉密计算机
涉密计算机
审批
涉密计算机
涉密计算机
载体输入
输入管理子系统
条码打印机
RFID标签机
（选配）
文档管理员
外来涉密光盘或U盘
受控盘
涉密输入机
载体输入管理
选择去向
登记
服务器
涉密网
数据交换
内部网
服务器
载体产生与制作
打印刻录复印输出
打印机
打印机
集中输出点
条码打印机
刷卡器
涉密输出机
一体化MPF
刷卡器
一体化刻录机
刻录机
控制器
复印机
载体回收与销毁
介质自助回收/交换系统
文档机要室
扫描枪
涉密笔记本
普通U盘
载体流转与监控
载体边界防护与检测
办公区域边界
涉密笔记本
外来普通U盘
标识识别器
出入监测扫描

业务范围

载体全生命周期
管控解决方案

载体输入管理

实现对外来纸质文件、外来光盘的录入安全管控，达到对输入渠道进行严格安全监管的目的。

载体产生与制作管理

实现对信息输出打印、复印、光盘刻录环节的监控与审计，达到对输出渠道进行严格安全监管的目的。

载体流转和监控管理

实现对载体流转、传递环节的安全管控，实时监控载体的带入带入行为，达到防止涉密介质的非法使用和非法流出的目的。

载体回收与销毁管理

实现对载体回收、销毁环节的安全管控，完成对载体全生命周期的闭环管理。

管控对象

1、载体输入管理

载体的输入管理主要包括两方面的内容：

（1）外来纸质文件的管理

（2）外来光盘介质的管理

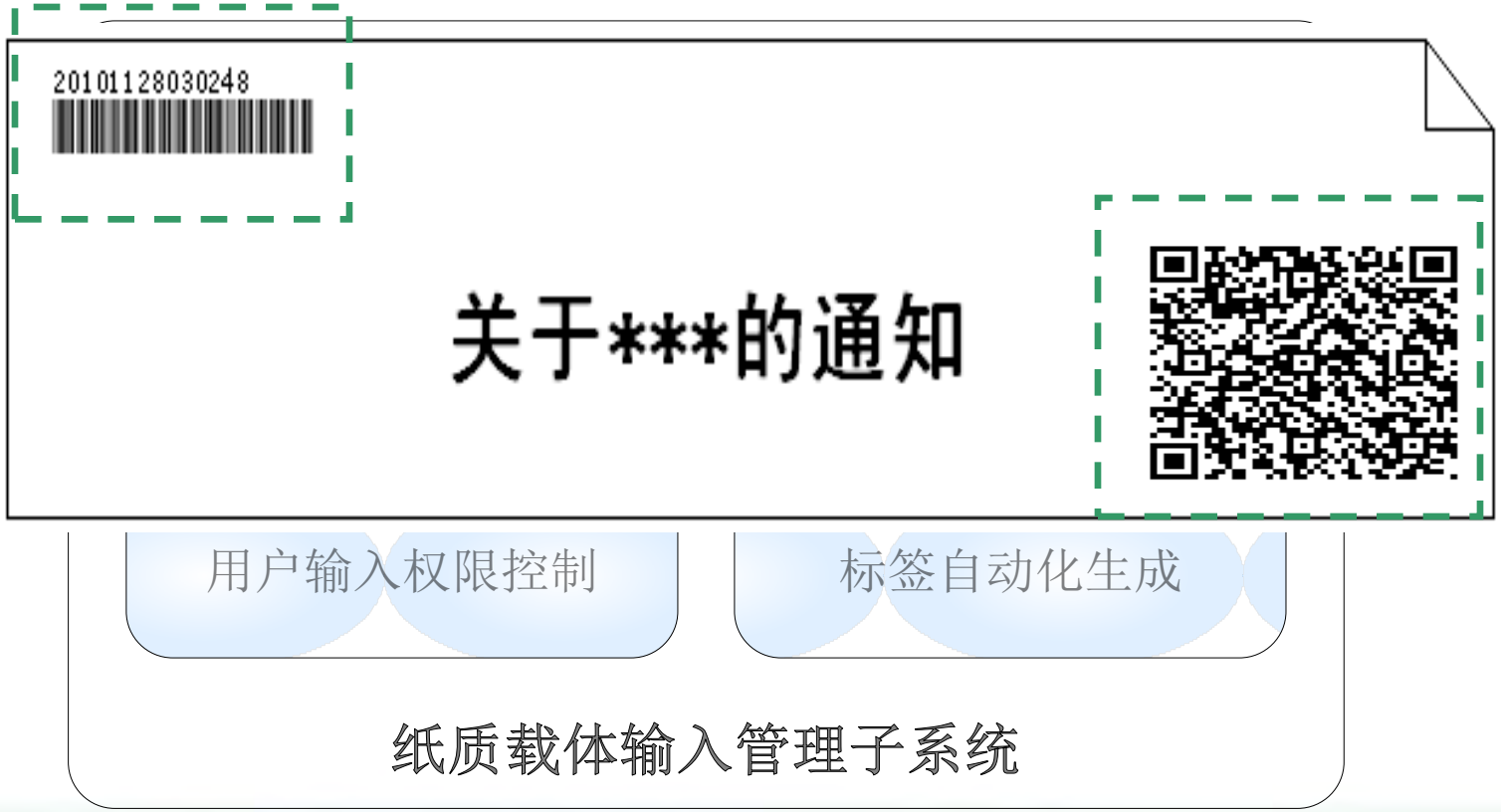
管控流程

外来文件的管理采用**文件录入管理模块、复印管理模块**，其管理流程包括外来文件的复印、留用、流转、归档、销毁过程，统一采用系统内派发的唯一性条码进行管理

外来光盘的管理使用**光盘录入管理模块**，其管理流程包括外来光盘留用、流转、归档及销毁全生命周期流程。

建设要点

载体输入管理 -- 纸质文件输入管理模块



建设要点

载体输入管理 -- 外来光盘输入模块

用户身份认证

中间机接口设备控制
（USB及光驱控制）

码

内

绘

去

杀

外
记录

涉密单机的介质台帐
及日志导入

标签生成

外来光盘输入管理

管控对象

2、载体产生与制作管理

涉密载体的产生与制作管理主要包括四方面内容：

（1）打印文件管理

（2）复印文件管理

（3）光盘刻录管理

管控流程

内网打印文件的管理使用**打印安全监控与审计**模块。
打印文件的管理流程包括外发、留用、流转、归档及销毁全生命周期流程。

内网复印文件的管理使用**复印安全监控与审计**模块。
复印文件的管理流程包括复印文件外发、留用、流转、归档及销毁全生命周期流程。

内网光盘的管理使用**光盘刻录监控与审计**模块。光盘介质的管理流程包括光盘外发、留用、流转、归档及销毁全生命周期流程。

建设要点

载体产生与制作管理 -- 打印模块

建设要点

载体产生与制作管理 -- 复印管理子模块

复印申请电子化审批

复印权限严格控制

二维条码自动生成

复印使用日志完备、规范

复印管理子系统

建设要点

载体产生与制作管理 -- 光盘刻录管理子模块

对刻录输出的光盘介质采取**自动喷绘条码**的方式进行载体可视化标记，实现光盘介质载体的有效管理，对涉密光盘介质进行全生命周期管理。

管控对象

3、载体流转与监控管理

载体流转与监控管理主要包括两方面的内容：

（1）载体（光盘、纸介质）的自动化流转管理

（2）基于RFID的载体的边界防护与检测管理

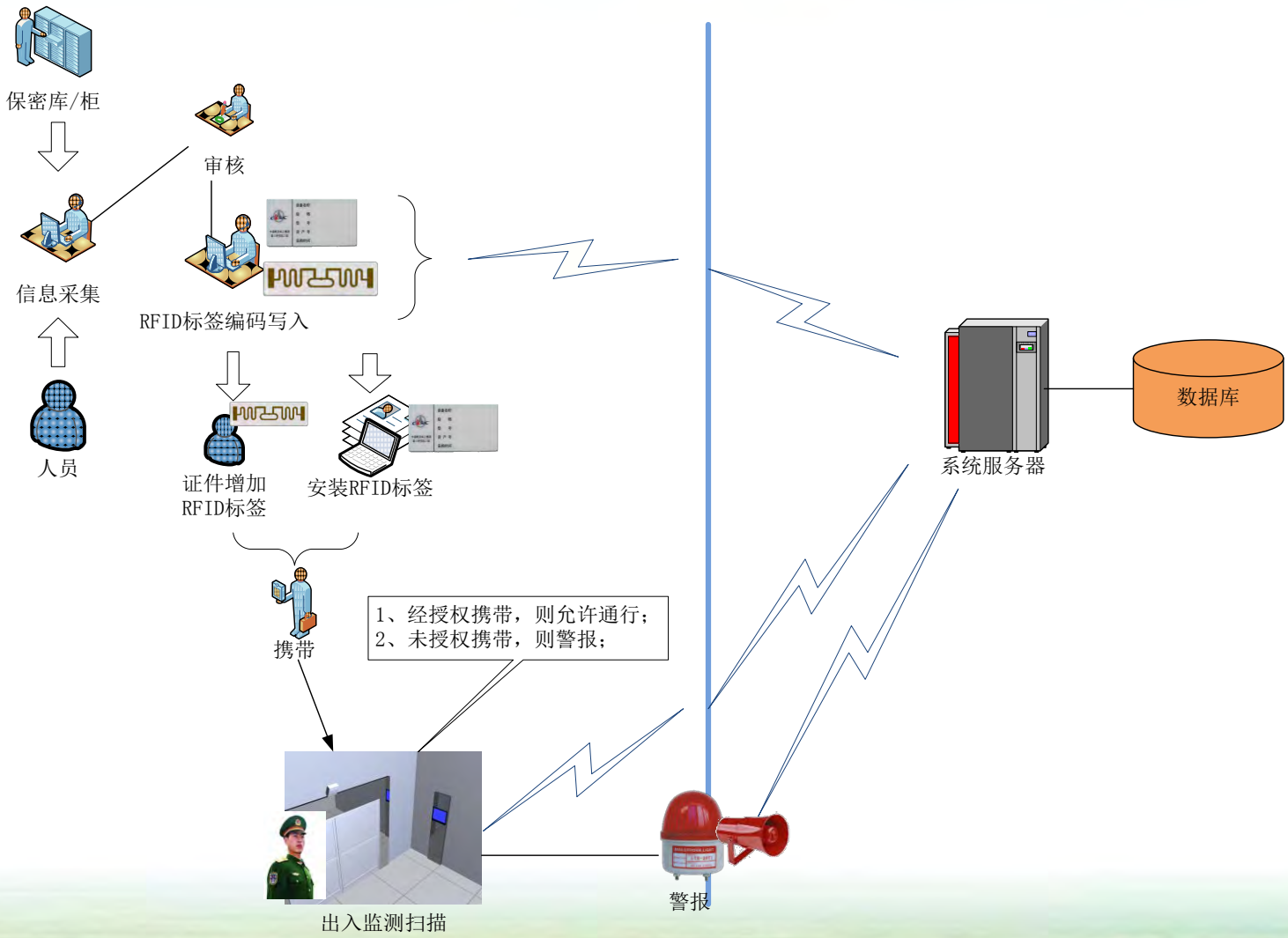
建设要点

载体流转与监控管理--自动化流转模块

建设要点

基于RFID的载体边界防护与检测管理

建设要点


保密库/柜
信息采集
人员
审核
RFID标签编码写入
证件增加
RFID标签
安装RFID标签
携带
1、经授权携带，则允许通行；
2、未授权携带，则警报；
出入监测扫描
警报
系统服务器
数据库

管控对象

4、载体的回收与销毁管理

载体回收与销毁管理主要包括两方面的内容：

（1）纸质载体的回收与销毁管理

（2）光盘载体的回收与销毁管理

建设要点

载体的回收与销毁管理

- 纸质文件闭环管理
- 文件回收提醒
- 光盘介质闭环管理
- 文件超期提醒
- 载体条码统一管控
- 载体台帐清晰、完整

载体回收与销毁管理模块

汇报提纲

1 涉密载体的管控现状与需求

2 涉密载体全生命周期管控解决方案

3 涉密载体全生命周期管控建设效果

项目实施效果

1 提高涉密载体管理水平	●提高航天三院涉密信息系统信息安全防护水平和能力，适应涉密信息系统信息安全的精细化、信息化管理的要求。 ●实现“底数清、账务符、流程明”的建设效果。
2 探究载体管理新模式	●利用智能化设备提高涉密信息系统的监管力度和执行效率，探索涉密载体保密管理的新方式。 ●提高航天三院保密管理水平，促进单位管理变革。
3 制定合理的信息资源规划	●制定适合企业运营发展的信息资源规划，有助于提高企业的信息管理水平，降低运营成本。
4 行业最佳实践	●基于全对象、全流程、全生命周期的信息化管理，成为军工、政府、军队行业的最佳实践。

项目创新性

技术创新 行业领先	实现对工程制图、财务软件等多种应用场景的支持，可支持隐形水印技术，形成责任追溯的管控功能。
涉密载体 统一编码标识	**涉密载体统一编码管理，做到载体底数清晰、动态一体化管理，并验证RFID物联网技术在涉密载体监测管理方面的实际效果。**
智能化、自动化的控制设备	采用智能保密柜设备，以新的应用思路解决常规操作人员占用、过程审批繁琐、审计日志分析困难等问题，探索新的涉密载体管理模式。

项目示范作用

2015年，该项目获得国家发改委信息安全专项保密试点示范项目资金支撑，也是军工集团内唯一试点示范项目，成为国内重要信息系统载体安全防护的应用典范。

谢　谢！