**警惕！服务外包的失泄密大坑**

原创 石涛 [保密观](javascript:void(0);) 2022-04-01 06:45



服务外包，即机关单位把部分后勤服务、技术服务及公共服务，比如餐饮、保洁、信息化运维等，承包给有关市场主体、社会组织承担或者协助开展。

随着经济社会的发展，服务外包在机关单位日常运转中发挥的作用越来越重要。然而，由于服务外包的“整体打包”特点，发包方往往疏于对承包方的保密监管，由此引发的失泄密案件屡见不鲜。

**典型案例**

**案例1：**服务人员成“盲区”，不察不周酿大案  
 2016年8月，某涉密单位发生重大失泄密案件。经查，该单位长期将办公大楼物业管理外包给某物业服务公司运营，该公司保洁人员段某主动联系境外情报机构，利用工作之便盗取、偷拍文件资料，先后为境外提供1项机密级、2项秘密级国家秘密及其他6项情报。案件发生后，段某被依法追究刑事责任，所在物业服务公司承包合同被终止，该单位有关领导责任人员、监管责任人员被依纪依法给予党纪政务处分。



**案例2：**保密审查不严格，泄密风险别小觑

2018年6月，有关部门在工作中发现，有人在文库类网站出售涉密文件。经查，这些文件均出自某公司。该公司虽不具备有关资质，但通过骗取信任的方式，承包了某区多家机关单位档案资料数字化业务。在此期间，公司员工蒋某利用工作便利，窃取、复制39份涉密文件，将其中5份放在互联网上出售。案件发生后，蒋某及其所在公司实际控制人方某被依法追究刑事责任，涉案机关单位相关责任人员均被依纪依法给予党纪政务处分。



**案例3：**日常监管不到位，隐患长留生事端

2019年3月，某资质企业向公安机关报案，称员工孙某丢失1台涉密笔记本电脑。经查，该企业承包某省多家单位的涉密信息系统运维服务，其中孙某长期在某机关驻场服务，并被确定为涉密人员。然而据其同事介绍，孙某经常将机关配发的涉密设备带回家中。事发当日，孙某携带涉密笔记本电脑在某餐厅用餐，中途外出接打电话，遗留在座位上的装有涉密笔记本电脑的背包被社会人员金某盗走。事后，金某被迅速抓捕归案，孙某被其所在单位辞退。



**案例4：**涉密文件也“打包”，舍本逐末酿祸端

2020年11月，有关部门在工作中发现，有人在微信群中传播涉密文件。原来，系某区属单位负责人蒋某，为总结工作成果，将2份秘密级文件违规复印后，交给相关服务外包的某社会组织负责人谢某参考，谢某又将文件转交工作人员程某，程某为收集情况，用手机对2份文件拍照并发送至微信群中，后被群成员转发至其他3个群，造成泄密。案件发生后，蒋某受到党纪政务处分，该社会组织有关合作协议被终止。

**应对之策**

从以上4起案例不难看出，无论是涉密工作还是非涉密工作“外包”，也无论哪类服务的“外包”，都存在一定的失泄密风险。因此，机关单位必须采取更有力措施，有针对性地强化服务外包中的保密管理，尤其须加强以下三方面工作。

**一是提高认识，高度重视。**服务外包虽是一种委托、放权行为，但委托不等同于卸责，放权更不等同于放任，服务外包具有风险“放大器”效应，保密管理必须及时跟进、主体责任必须落实到位，委托服务外包的机关单位更要有如履薄冰、如临深渊的责任意识，有针对性地加强监督，确保保密监督管理覆盖到位、不出纰漏。

**二是明确义务，夯实责任。**机关单位应当在外包协议中明确自身的保密监管权力和承包方的保密管理义务，经常性督促承包方加强对服务人员的保密管理，落实上岗审查，关注思想动态，做好保密提醒；机关单位内部要进一步夯实保密管理主体责任，明确“发包”部门的监管责任，做好对承包方和服务人员的管理，特别是购买服务涉及国家秘密的，应当把好资质关口、签订保密协议、提出保密要求，随时关注承包方内部管理情况，并做好对内部人员的监督提醒。

**三是加强教育，普及“两识”。**服务人员保密“两识”不足，是当前案件高发的主要原因。要结合外包服务的工作特点，以生动、典型的服务人员失泄密案例为教育内容，向其普及保密“两识”。涉密工作外包的机关单位和涉密程度高的“发包”单位，除了将服务人员纳入日常保密培训外，还应当适时“开小灶”，帮助他们增强反窃密、防泄密的意识和本领，杜绝违法犯罪行为发生。