保密小常识

保密工作的方针

在不同历史时期，党和国家保密工作方针有所不同。2010年修订实施的保密法结合保密工作的特点和方法，在总结新时期党和国家保密工作实践经验的基础上，规定“保守国家秘密的工作，实行积极防范、突出重点、依法管理的方针，既确保国家秘密安全，又便利信息资源合理利用”。

积极防范

“积极防范”是保密工作实践经验和特点规律的科学总结。保密工作首先要以预防为主，做到未雨绸缪，防患未然。即以防止窃密泄密为出发点和着力点，积极主动、关口前移，构筑人防、物防、技防的综合防范体系，及时发现和消除泄密隐患，堵塞泄密漏洞，从源头上防止各类泄密窃密事件发生，确保国家秘密安全。

突出重点

“突出重点”是抓好保密工作的重要方法，也是保密工作的基本方针。保密工作涉及多部门、多行业、多领域、多学科，是一项复杂的系统工程。做好保密工作，必须处理好重点和一般的关系，抓好重点，确保核心。同时，“突出重点”不是“只要重点”，对非重点可以放任不管或是放松管理，而是建立在对国家秘密进行全面管理基础之上。国家秘密在任何一个地区、任何一个部门、任何一个环节、任何一种渠道泄露出去，都会危害国家安全和利益，都会影响保密工作的整体效能。

依法管理

“依法管理”是依法治国基本方略在保密工作中的运用和体现。一是有法可依，建立完备的保密法律制度，将保密工作的各个方面纳入法制轨道，不断提高立法质量，完善法律体系，增强保密法律体系的完整性、权威性、有效性；二是有法必依，机关单位严格按照有关法律法规管理涉密人员、涉密载体、涉密信息系统和涉密活动等；三是执法必严，保密行政管理部门按照有关法律法规，认真履行监督管理职责；四是违法必究，对违反保密法律法规的行为依法查处，严肃追究法律责任。

保放适度

“既确保国家秘密安全，又便利信息资源合理利用”，是保密工作遵循的一个重要准则。即在确保国家秘密安全的前提下，努力实现国家秘密保护和信息资源利用之间的平衡，做到依法保密、依法公开。因此，为处理好“信息保密”和“信息公开”的关系，依法保障公民的知情权、参与权和监督权，必须遵循“法律、行政法规规定公开的事项，应当依法公开”的原则，对于法律法规要求公开的事项，不得以保密为由不予公开或者拒绝公开，公开的事项不得泄露国家秘密，公开的程序和方式也必须符合法律规定。

责任编辑/徐 琛

国家秘密载体印制资质的申请条件

□秦 黎

申请人提出申请，是行政许可的前提条件，是申请人从事某种特定行为之前必须履行的法定义务。申请权是一种程序上的权利，不论申请人在实体法上是否符合获得许可的条件，申请人都有权通过合法的申请，要求行政机关作出合法的应答。但是，行政审批属于事前管理，既是一项权力，更是一种职责和义务，如果不符合行政许可条件，行政机关也不会作出审批。因此，从申请有效性上考虑，申请人应该依据行政许可的有关条件，认真准备，以利于行政审批事项的获得。

国家秘密载体印制资质作为行政审批事项也是如此，有关生产经营性企业事业单位申请该资质时必须符合一定的条件，能够确保党和国家秘密安全，才有可能获得该资质。按照有关规定，国家秘密载体印制资质申请单位应当具备以下基本条件：（1）在中华人民共和国境内注册的企业法人或者事业单位法人；（2）参与国家秘密载体印制业务的人员为中华人民共和国境内公民，国家另有规定的除外；（3）具有与所申请资质类别、等级相适应的固定生产经营场所和办公场所；（4）从事相应印制业务3年以上，具有良好的诚信记录，无违纪违法行为；（5）具备相应规模的印制设备和技术力量等生产经营条件；（6）生产经营和监督管理制度健全。

同时，按照有关规定，出于国家秘密安全的考虑，申请单位还应当具备一定的保密条件，具体包括：（1）保密制度完善；（2）保密组织健全，有专门的机构或者人员负责保密工作；（3）对涉密人员的审查、考核、登记手续完备，且涉密人员具备必要的保密知识和技能；（4）具备独立的保密室和涉密印制业务所必需的印制车间、成品库、废品库等功能场所；（5）用于涉密印制业务的场所、设施、设备符合国家保密规定和标准；（6）涉密计算机信息系统、涉密办公自动化设备防护和管理符合国家保密标准和管理规范；（7）厂房、生产车间周边环境安全保密。

需要注意的是，甲级资质申请单位，除具备以上条件外，还应当具备乙级资质，有3年以上国家秘密载体印制业务经验；国家秘密载体印制区域实行封闭式管理；设置专职保密总监，配备专门保密工作人员。同时，有关规定还明确，有境外（含香港、澳门、台湾）组织、机构、人员投资或者参与经营管理的，不得授予涉密文件资料、涉密光电磁介质印制资质；有境外（含香港、澳门、台湾）组织、机构、人员控股或者参与经营管理的，不得授予国家统一考试试卷、涉密防伪票据证书印制资质。

以上是申请国家秘密载体印制资质的基本条件和保密条件，是最基本的市场准入门槛。为了使这些条件更加具有可操作性和指导性，让申请单位更有针对性地进行资质申请前的准备，国家保密行政管理部门另行规定了翔实的国家秘密载体印制资质具体条件和保密标准，分别对不同资质种类，按照甲乙不同等级对这些基本条件和保密标准进行了具体化，不但有利于申请单位有针对性地准备，也有利于行政许可的公开、公正、透明。

责任编辑／孙战国

网络空间安全保密困境与移动目标防御

□刘小虎　张玉臣

如今，网络将“人、机、物”深度关联融合，传统防御手段的短板愈加明显——封堵不尽的漏洞，修补不完的补丁，守擂方始终处于被动局面。针对网络空间“矛强盾弱”“易攻难守”的困境，亟须突破现有防御技术，把握新时代安全保密的主动权。

网络空间不安全的本源

一是软硬件设计生产中无法避免的漏洞。漏洞是发起网络攻击的前提。软件由数百万行代码组成，硬件由数以万计的门电路构成。受软硬件设计人员认知局限、行为习惯及技术水平的影响，设计生产无法规避漏洞，甚至防护软件、防御设备等也存在安全保密缺陷。

二是网络产品或多或少存在后门。网络产品提供商为了后期管理、维护、升级等原因，可能会开放某些特殊的软件权限、硬件端口等，有意设计或无意间形成了一些具有“暗功能”的后门。在网络产品全球化供应的今天，漏洞或后门日益成为一种战略资源，不排除某些国外公司出于经济利益或政治目的，发起攻击。

三是用户使用时无法确保依规操作。安全保密链条中最薄弱的环节是使用者本身。尤其是简单配置网络、弱化口令密码等不合规的行为，更会加剧风险。同时，网络空间中的各类信息系统相互联通，加上规模化生产等原因，网络信息产品“同源、同构、同质”特性突出，为攻击方掌握漏洞、实施渗透、发起攻击、持续潜伏等提供了极大便利。

传统网络防御的游戏规则

网络安全保密经历了通信保密、信息安全和信息保障3个发展阶段，形成了以防护、检测、响应、恢复为代表的纵深防御体系。

为抵御网络攻击，现有的防御措施主要有3种：一是源代码审查，旨在设计和生产软硬件时，通过层层审查和标准化操作尽量减少漏洞；二是事后打补丁，但有些网络攻击可能已造成不可挽回的损失；三是主动检测并识别攻击，也是最重要的网络防御措施，其中又可分为3类。

一是基于规则的防御，典型代表是防火墙，其功能类似于“城墙”——用户为防御设备设置黑名单或白名单后，由系统进行筛选过滤。二是基于特征的防御，典型代表是入侵检测，其功能类似于“门卫”——防御设备需存储并维护一个特征库，通过特征匹配来检测和发现网络攻击。三是基于行为的防御，典型代表是入侵防御，其功能类似于“看守”——防御设备对主体行为进行验证，发现可疑行为时，分析判断是否为网络攻击。

可以看出，传统网络防御是通过附加或外在的防御措施达到目的。但通过这些静态、孤立、被动式的防御手段“查漏堵门”“杀毒灭马”越来越难以有效应对更高级的网络攻击。特别是APT攻击，它往往带有国家或某种组织背景，攻击方长期探测扫描某一目标，制定专门的攻击策略，编写特定代码，给网络安全保密造成重大威胁。

攻击与防御的不对称性

网络攻击与防御是一场动

态博弈，但双方并不对等，攻击方可自由选择对象、时机和方法。具体表现为：

一是攻防信息不对称。现有防御手段需要以攻击来源、特征、途径和行为等先验知识作为基础，但信息收集难度较大。而防御方采取的防御设备、策略等大多是同构、同质的，可轻易被攻击方掌握。

二是攻防时间不对称。攻击方可长期对目标网络的组成要素、承载协议及网络应用的固有漏洞反复探测、分析和渗透，直至达到攻击目的。但现有防御手段通常以发布补丁、修补漏洞、添加或修改防火墙规则等方式进行，其中的时间差为实施网络攻击提供了时机。

三是攻防成本不对称。攻击方只需找出任意一个安全漏洞，即可长驱直入，而防御方即使发现再多的安全漏洞，也不能保证系统完美无缺，必须全时全方位部署，“小攻大防”的格局无形中提升了成本。

目前，网络攻击可分为3种：“已知的已知攻击”，即防御方能够准确检测和发现的网络攻击；“已知的未知攻击”，即防御方能够感知网络攻击，却不知道究竟遭受了什么；“未知的未知攻击”，即防御方即使遭到了网络攻击，也无法检测和发现。

传统的防御手段在防御“已知的已知攻击”方面很有成效，在防御“已知的未知攻击”方面也取得了一定的效果，但在防御“未知的未知攻击”时却显得束手无策，亟须创新突破。

移动目标防御的优势

2011年，美国科学技术委员会发布《可信网络空间：联邦网络空间安全研发战略规划》，移动目标防御作为网络安全保密的新型技术之一，或可为我们提供借鉴。

它提供了一种动态防御思想，其目的不是构建完美的防御系统，而是通过动态改变系统内部的一个或多个属性，增强自身的不确定性和随机性，从而增加攻击的复杂度，以此扭转攻防双方的不对称性。

移动目标防御自提出以来，立即成为国内外研究热点，并回答了3方面的问题。

一是“为什么移动”。移动目标防御通过改变系统配置，可有效降低系统的确定性、相似性和静态性，让攻击方难以发现漏洞，或即使发现了也不能持续利用。简而言之，系统的安全能力不是靠防火墙、入侵检测等设备构建的，而是通过动态变化内生的，以此形成一个攻击者无法掌握规律、无法破解结构的防御体系，进而有效避免恶意攻击。

二是“什么时间移动”。“移动”又称为自适应跳变，主要有基于时间间隔的、基于异常事件的和基于系统状态的3种形式。其中，基于时间间隔的又分为固定时间间隔和随机时间间隔。此外，也要考虑到系统安全性与可用性之间的平衡。系统跳变慢，就可能暴露漏洞，引发攻击，降低安全性；系统跳变快，也会耗费计算资源，增长服务时延，降低可用性。

三是“移动什么”。主要包括网络层、平台层、运行环境层、软件层、数据层5个层次。网络层包含随机地址、端口、网络拓扑结构和配置等；平台层包含操作系统、处理器构架、虚拟机和存储系统等；运行环境层包含地址空间及指令集随机化等；软件层包含程序的指令序列、指令格式、内部数据结构布局等；数据层包含数据的格式、语法、编码等。通过各层的主动跳变、快速迁移形成动态环境，为攻击者布下迷宫。

如果将安全防御比喻成打靶。在传统防御思想下，系统静态、同构，相当于攻击方打固定靶，经过长时间的瞄准，自由选择最佳击发时机，击中的概率自然也就较高。但在移动目标防御思想下，系统动态、多变，相当于打移动靶，击中的概率就会大幅降低。

当然，安全保密的核心是人。在突破相关技术的同时，也要对人性的弱点和管理的漏洞加以防范，才能不给攻击者留下可乘之机，为做好新时代网络安全保密工作奠定坚实基础。

（作者单位：信息工程大学）

保密小常识

保密工作的原则

保密工作的原则是对党和国家保密工作优良传统和丰富经验的继承发扬，紧紧抓住当前保密工作的根本问题和关键环节，深刻揭示了保密工作的客观规律，具有丰富的科学内涵和鲜明的时代特征，必须在工作中始终遵循。

最小化原则

最小化原则，是指严格按照有关保密规定和标准确定、管理国家秘密，确保国家秘密数量最少、知悉范围最小、涉密环节最简。在定密方面，严格按照保密事项范围规定确定国家秘密，确保定密精准、知悉范围最小、保密期限最短；在载体管理方面，按照工作需要，严格控制涉密载体数量，实行统一集中管控；在载体流转方面，尽量简化环节。

全程化原则

全程化原则，就是坚持国家秘密在哪里，保密工作就做到哪里，按照严格规范的标准和要求实施保密管理，实现全过程、全范畴、全方位、全天候覆盖。全过程，主要指国家秘密存在的整个生命周期；全范畴，主要指涉及国家秘密的地区部门、行业系统、领域区域等各个方面；全方位，主要指全部管理对象；全天候，主要指对国家秘密的保护不间断、不脱节。

精准化原则

精准化原则，就是根据不同行业、领域特点和涉密程度，采取相应保护措施，合理分配力量资源，精心设计方案，精细实施活动，精准制定标准，确保管理对象清晰、管理措施有效、管理流程闭环。“精准化”不是“精简化”，要避免减少必要的制度规定、人员安排和设施设备配备，削弱管理成效。

自主化原则

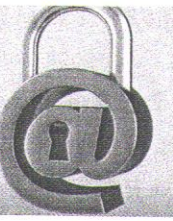
自主化原则，就是要积极应对信息化条件下技术窃密的严峻形势，大力加强保密科技工作，大幅提升自主创新能力，全面掌握核心关键技术，研制并推广应用具有自主知识产权、先进可靠实用、覆盖保密工作各领域各环节的保密技术产品，构建全方位、立体式、多层次的保密技术防护和检查监管体系，确保党和国家秘密安全。

法制化原则

法制化原则，是指进一步健全以保密法为主干的保密法规制度，形成上下衔接配套、行业领域全覆盖的保密法规体系，把保密工作的方方面面完全纳入法制轨道，形成依法办事、依法管理的工作模式。具体地说，就是把依法管理的各项要求落实到国家秘密从产生、使用、存储、流转到销毁的全过程，落实到从定密、降密到解密，从制定规范、监督管理到案件查处的各个环节，实现保密工作各环节、各领域的依法管理。

责任编辑/徐 琛

保密小测试



判断题

1 按照保密法第四十九条的规定：机关单位违反本法规定，对应当定密的事项不定密，或者对不应当定密的事项定密，造成严重后果的，由有关机关单位依法对直接负责的主管人员和其他直接责任人员给予处分。对定密而言，“直接负责的主管人员”是指定密责任人，“直接责任人员”是指承办人。（ ）

2 定密责任人和承办人出现应当确定国家秘密而未确定的、不应当确定国家秘密而确定的、超出定密权限定密的、未按照法定程序定密的、未按规定标注国家秘密标志等情况的，机关单位应当及时纠正并进行批评教育；造成严重后果的，依纪依法给予处分。（ ）

3 制定保密事项范围的中央有关机关，可以根据定密工作实际，直接对本行业、本领域保密事项范围直接进行调整、修订。（ ）

4 机关单位确定国家秘密应当依据保密事项范围进行。保密事项范围没有明确规定但属于保密法第九条、第十条规定情形的，应当确定为国家秘密。（ ）

单项选择题

5 传递秘密载体，应当密封包装，且传递秘密载体的信封或者袋牌上应当标明什么？（ ）
A.密级　　B.密级和编号　　C.密级、编号和收发件单位名称

6 对绝密级的国家秘密文件、资料和其他物品，非经以下哪个单位批准，不得复制和摘抄。（ ）
A.原确定密级的机关单位的上级机关或上级保密行政管理部门
B.原确定密级的机关单位或者其上级机关
C.原确定密级的机关单位。

7 集中存储、处理工作秘密的信息系统和信息设备，参照（　）级信息系统和信息设备管理。
A.秘密　　B.机密　　C.绝密

8 国家机关和涉密单位的涉密信息系统投入使用前应经过（ ）审查批准。
A.本单位保密委员会　　B.本单位主管领导　　C.保密行政管理部门

责任编辑/孙战国

密件经手责任重　切勿违规受惩处

□宋筱婷

涉密文件保密管理，可谓“老生常谈”，在不同场合、以不同视角被屡屡提及。但我们往往忽视的是，涉密文件保密管理，并非个体所能独立完成，在整个文件运转过程中，往往存在多名经手人，一人发生疏忽，则整个安全屏障即被打破。所以，以“人”为视角，深入研究从“入手”“倒手”再到“出手”的整个经手过程中如何做好保密管理，是确保涉密文件万无一失必须审慎思考的问题。

典型案例

一、密件“入手”环节

案例1：2018年4月，某市机要部门通知原市检验检疫局服务中心文件专管员周某紧急去取一套涉密文件，但周某忙于手头其他工作，难以走开。周某认为，取文件而已，反正谁去都一样，便未向分管领导报告，私自委托新入职尚未接受保密培训的驾驶员赵某帮其代领。赵某领取文件后，出于炫耀心理，在返回途中于车内私自用手机将其中3份机密级文件首页进行拍照，并实时在微信群“相亲相爱一家人”中发布，造成泄密。案件发生后，有关单位对赵某作出解除劳动合同，并移交司法机关的处理；取消周某文件专管员资格，责令作出书面检查，并处罚金1000元；对服务中心主任文某进行诫勉谈话；给予该局办公室主任刘某党内警告处分，对副局长任某、局长奉某进行约谈，并责令作出书面检查。

案例2：2014年1月下旬，临近春节放假，某单位机要员李某已收拾完桌面办公用品，准备放假。“李某，快来帮忙分年货啦！抓紧时间，别耽误大家过节。”李某一听，来了精神，火速支援，在单位办公楼前的小广场上和大家一起忙活起来。正忙得热火朝天，市委的机要车来送机要文件了，李某的心思一心记挂着年货，便在办公楼门口签收了装有9份秘密级文件的6个信封，随手放在大楼一楼就近的窗台上（未拆封、未登记）；分完年货后，也忘记将信封带回办公室。2月底清退文件时，李某才发现密件已丢失。后经该单位、市保密局及当地公安机关全力查找，仍未能找回。案件发生后，有关部门给予李某开除党籍、公职处分，给予该单位保密办主任潘某撤销党内职务、行政降级处分，给予党委书记姜某党内严重警告、行政记大过处分。

二、密件“倒手”环节

案例3：2019年1月，有关部门在工作中发现，某市政府部门办公室刘某使用QQ软件传输涉密文件扫描件。经查，刘某为收件方，发件方为同处室的同事霍某。原来，为尽快完成某项目申报任务，其他部门同事王某通过机密级涉密计算机将材料以压缩包形式发给霍某，督促其抓紧按要求开展工作。因时间紧、任务重，霍某仅粗粗查看了压缩包中的一级目录，未发现存在于二级目录中的1份机密级文件，便用光盘将该压缩包从涉密计算机中导出，复制到自己的连接互联网计算机上并通过QQ发给刘某。案发时，刘某也尚未及时查看压缩包中所有文件，未发现其

中包含密件。目前，此案正在进一步查处中。

案例4：2019年2月，夜已深，某市政府业务部门工作人员望某在办公室加班整理文件，发现一份传阅的机密级会议纪要对业务工作具有很强的指导和借鉴意义，便产生了全文留存以便学习参考的想法。望某知道，按规定若想留存密件需履行报批手续并使用涉密复印机进行复印，但涉密复印机由单位文印室统一管理，已经锁门。此时的望某已十分疲惫，实在不想第二天再“折腾”了，便关了办公室的门，偷偷用手机对该文件进行了拍照，并使用手机软件对拍摄的涉密文件进行文字识别后发送至自己的办公用互联网计算机上，转化为Word文档进行编辑。目前，此案正在进一步查处中。

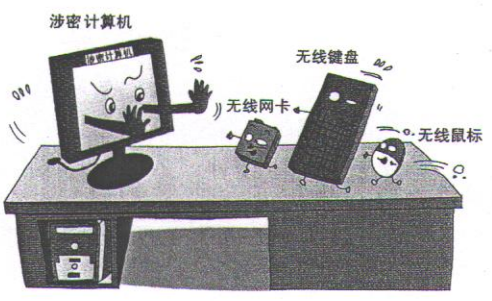
三、密件“出手”环节

案例5：2016年12月，有关部门在工作中发现，某参公事业单位研究室主任蒋某在连接互联网的计算机中违规存储、处理大量涉密材料，其中绝密级国家秘密1份、机密级国家秘密12份、秘密级国家秘密59份，涉及国家秘密数量多、时间跨度大。经查，蒋某为转业干部，曾辗转部队多个部门工作，业务经验丰富。该计算机中存储、处理的涉密文件为其2008年转业时私自留存。据蒋某称，其日常有收集资料的习惯，认为这种做法对新岗位熟悉工作帮助很大。事件发生后，有关部门给予直接责任人员严厉处分。

案例6：2015年5月，有关部门在工作中发现，某县县委宣传部一台连接互联网的计算机违规存储、处理国家秘密信息。经查，该计算机使用人为工作人员易某。同年3月，工作人员陈某因临盆在即，产假交接工作过程中，贪图省事，未按规定履行工作交接手续，在未告知相关领导及同事的情况下，私自将移动硬盘中的部分涉密文件与非涉密文件一并拷贝至易某使用的非涉密计算机上（内含3份秘密级文件）。易某接手工作后，工作量激增，未能及时对陈某交接的电子文件过目，导致对该情况未能及时发现并作出正确处理。事件发生后，有关单位给予陈某、易某行政警告处分，在全地区范围内进行通报批评；并对县委宣传部主要领导进行诫勉谈话。

案件分析

需要说明的是，本文未将故意卖密牟利、对外提供等极端恶劣情形包含在内，仅限于机关单位日常工作的范围内分析讨论。



一、从主观意识上看

1.故意，即主动追求或被动放任行为后果发生的情况。一是主动追求。案例1中赵某将涉密文件首页拍照后主动发布至微信群就属于典型的主动追求泄露后果发生。此类案件中，行为人往往通过泄露后果的实现来达到某种私人目的。该目的并不一定是经济利益，也可表现为图炫耀、还人情或讲义气等，甚至是为了作为自己处于某种状态、位置的证明。二是被动放任。案例4中望某违规传递、案例5中蒋某私自留存、案例6中陈某违规交接的行为，都属于将涉密文件置于危险境地，对后续可能产生的危害后果持放任态度，不予考虑。上述情况的根源都在于将个人的利益、便利凌驾于国家秘密安全之上。

2.过失，即行为存在瑕疵却对行为后果持否定态度的情况。一是疏忽大意。案例2中李某因忙于手头其他工作对密件随手放置，案例3中霍某、刘某及案例6中易某未能对文件及时查看均属于此类情况。在文件经手过程中，往往存在阻碍行为人审慎履职的特殊情况、特殊时间点等客观因素是案件发生的重要原因。特殊情况，如时间紧、任务重；特殊时间点，如节假日前夕、休假前夕、场所变动前夕等，此类案件多发易发。二是

过于自信。明知违规但自认为没有危害或危害不会发生。案例1中作为文件专管员的周某，自认为不会出问题，在明知文件“专管”要求的情况下，仍私自委托新人赵某代领文件，最终追悔莫及。

二、从行为方式上看

1.密件“入手”环节。可以表现为私自委托不属于涉密文件知悉范围人员去收取密件导致泄密；或收取密件时心存旁骛，忙于其他工作、私人事务，如放假、下班、就医等，对密件随手处置泄密；或“入手”时不按规定置于保密柜中，随意放于桌面、玻璃柜、抽屉等位置，导致文件丢失或被他人复印、窃取等。实践中，还曾发生取件返程途中违规乘坐公共交通工具将密件遗失的情况。

2.密件“倒手”环节。从对象上看，分为“倒”给别人和“倒”给自己。可以表现为对自己传阅的文件不认真审阅，未能及时发现文件密级、保密期限、发放范围等核心要素，导致通过互联网违规传递；或贪图便利，明知不符合保密规定，仍然违规复印、扫描、摘录、汇编；或为参考学习，私自拍照上传至互联网计算机中等。实践中，还曾发生为了将字体放大方便观看而将文件拍照后上传至互联网计算机的情况。

3.密件“出手”环节。可以表现为该移交不移交，将手中密件隐匿不交或私自留存备份，从阶段性经手变为长期持有，后续或自用、或贩卖，进而造成泄密或泄密隐患；也可以表现为“一揽子”移交，不按规定将密件、非密件分类移交，不详细告知接手人注意事项，甚至“单方”移交，不与接手人发生接触，自顾自办理完毕。这极易导致接手人对情况不了解，进而造成误操作，形成连锁反应。案例6就属于这种情况，实践中还曾发生不告知移交的计算机中存在涉密文件导致接手人误连互联网的情况。

应对措施

一、加强保密教育，树正思想“三观”。一是树正“利益观”。将国家利益时刻放在首位，严禁将密件作为实现个人目的的工具和手段，绝不能将个人利益凌驾于国家秘密安全之上。二是树正“业绩观”。完成工作不拖延固然重要，但保量更要保质，不能因时间紧、任务重就放松了工作标准和要求，坚决杜绝各种图便利、走捷径的行为。三是树正“大局观”。真正确立“文件保密一盘棋”的思想，从自身做起。在密件“出手”环节要坚决摒弃“文件出手脱干系”的错误思想，坚持“扶上马、送一程”，完整、准确交接，认真讲解，有效避免接手人遗漏。在密件“入手”环节要坚持认真、细致的工作作风，对入手文件不能简单放置，要逐一过目，做到心中有数，发现问题，及时处理，将失泄密隐患消于无形。

二、推进保密管理，强化制度落实。一是科学、合理配置资源。合理配置人力资源，在涉及核心、紧急、重大工作且文件经手数量巨大时，或抽调专人帮助工作，或灵活机动设置岗位替补，有效防范个人“多线作战”、工作过于繁重导致工作失误的情况。合理配置办公资源，尤其是经手密件数量多、密级高的岗位，及时配备涉密计算机、涉密扫描仪、涉密复印机，为便利工作创造条件，尽可能杜绝“因公”图便利受惩处的情况，保护好文件经手人工作的积极性和主动性。二是组织签订专项保密承诺书。立足密件经手流程，结合具体岗位职责，签订专项保密承诺书，详细列举具体岗位职责、密件经手风险点及相关法律责任，既明晰了工作标准和要求，又起到了保密教育的现实效果。三是组织定期检查，及时发现隐患。针对文件经手数量大、密级高的人员和部门，定期组织自查、互查和抽查，实行纸质、电子密件全覆盖，以有效防范丢件、漏件、私留、私泄、私拷、私传、误传等情况的发生。此外，对为追求个人利益主动泄密，且造成文件内容大范围泄露的，依法依规严肃处理，绝不姑息；构成犯罪的，移交司法机关，依法追究刑事责任。

责任编辑/孙战国