4.15 全民国家安全教育日保密宣传周活动专题宣传

中华人民共和国保守国家秘密法

（1988 年 9 月 5 日第七届全国人民代表大会常务委员会第三次会议通过 2010 年 4 月 29 日第十一届全国人民代表大会常务委员会第十四次会议修订）

第一章总则

第一条 为了保守国家秘密，维护国家安全和利益，保障改革开放和社会主义建设事业的顺利进行，制定本法。

第二条 国家秘密是关系国家安全和利益，依照法定程序确定，在一定时间内只限一定范围的人员知悉的事项。

第三条 国家秘密受法律保护。

一切国家机关、武装力量、政党、社会团体、企业事业单位和公民都有保守国家秘密的义务。

任何危害国家秘密安全的行为，都必须受到法律追究。

第四条 保守国家秘密的工作（以下简称保密工作），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。

法律、行政法规规定公开的事项，应当依法公开。

第五条 国家保密行政管理部门主管全国的保密工作。县级以上地方各级保密行政管理部门主管本行政区域的保密工作。

第六条 国家机关和涉及国家秘密的单位（以下简称机关、单位）管理本机关和本单位的保密工作。

中央国家机关在其职权范围内，管理或者指导本系统的保密工作。

第七条 机关、单位应当实行保密工作责任制，健全保密管理制度，完善保密防护措施，开展保密宣传教育，加强保密检查。

第八条 国家对在保守、保护国家秘密以及改进保密技术、措施等方面成绩显著的单位或者个人给予奖励。

第二章国家秘密的范围和密级

第九条 下列涉及国家安全和利益的事项，泄露后可能损害国家在政治、经济、国防、外交等领域的安全和利益的，应当确定为国家秘密：

（一）国家事务重大决策中的秘密事项；

（二）国防建设和武装力量活动中的秘密事项；

（三）外交和外事活动中的秘密事项以及对外承担保密义务的秘密事项；

（四）国民经济和社会发展中的秘密事项；

（五）科学技术中的秘密事项；

（六）维护国家安全活动和追查刑事犯罪中的秘密事项；

（七）经国家保密行政管理部门确定的其他秘密事项。

政党的秘密事项中符合前款规定的，属于国家秘密。

第十条 国家秘密的密级分为绝密、机密、秘密三级。

绝密级国家秘密是最重要的国家秘密，泄露会使国家安全和利益遭受特别严重的损害；机密级国家秘密是重要的国家秘密，泄露会使国家安全和利益遭受严重的损害；秘密级国家秘密是一般的国家秘密，泄露会使国家安全和利益遭受损害。

第十一条 国家秘密及其密级的具体范围，由国家保密行政管理部门分别会同外交、公安、国家安全和其他中央有关机关规定。

军事方面的国家秘密及其密级的具体范围，由中央军事委员会规定。

国家秘密及其密级的具体范围的规定，应当在有关范围内公布，并根据情况变化及时调整。

第十二条 机关、单位负责人及其指定的人员为定密责任人，负责本机关、本单位的国家秘密确定、变更和解除工作。

机关、单位确定、变更和解除本机关、本单位的国家秘密，应当由承办人提出具体意见，经定密责任人审核批准。

第十三条 确定国家秘密的密级，应当遵守定密权限。

中央国家机关、省级机关及其授权的机关、单位可以确定绝密级、机密级和秘密级国家秘密；设区的市、自治州一级的机关及其授权的机关、单位可以确定机密级和秘密级国家秘密。具体的定密权限、授权范围由国家保密行政管理部门规定。

机关、单位执行上级确定的国家秘密事项，需要定密的，根据所执行的国家秘密事项的密级确定。下级机关、单位认为本机关、本单位产生的有关定密事项属于上级机关、单位的定密权限，应当先行采取保密措施，并立即报请上级机关、单位确定；没有上级机关、单位的，应当立即提请有相应定密权限的业务主管部门或者保密行政管理部门确定。

公安、国家安全机关在其工作范围内按照规定的权限确定国家秘密的密级。

第十四条 机关、单位对所产生的国家秘密事项，应当按照国家秘密及其密级的具体范围的规定确定密级，同时确定保密期限和知悉范围。

第十五条 国家秘密的保密期限，应当根据事项的性质和特点，按照维护国家安全和利益的需要，限定在必要的期限内；不能确定期限的，应当确定解密的条件。

国家秘密的保密期限，除另有规定外，绝密级不超过三十年，机密级不超过二十年，秘密级不超过十年。

机关、单位应当根据工作需要，确定具体的保密期限、解密时间或者解密条件。

机关、单位对在决定和处理有关事项工作过程中确定需要保密的事项，根据工作需要决定公开的，正式公布时即视为解密。

第十六条 国家秘密的知悉范围，应当根据工作需要限定在最小范围。

国家秘密的知悉范围能够限定到具体人员的，限定到具体人员；不能限定到具体人员的，限定到机关、单位，由机关、单位限定到具体人员。

国家秘密的知悉范围以外的人员，因工作需要知悉国家秘密的，应当经过机关、单位负责人批准。

第十七条 机关、单位对承载国家秘密的纸介质、光介质、电磁介质等载体（以下简称国家秘密载体）以及属于国家秘密的设备、产品，应当做出国家秘密标志。

不属于国家秘密的，不应当做出国家秘密标志。

第十八条 国家秘密的密级、保密期限和知悉范围，应当根据情况变化及时变更。国家秘密的密级、保密期限和知悉范围的变更，由原定密机关、单位决定，也可以由其上级机关决定。

国家秘密的密级、保密期限和知悉范围变更的，应当及时书面通知知悉范围内的机关、单位或者人员。

第十九条 国家秘密的保密期限已满的，自行解密。

机关、单位应当定期审核所确定的国家秘密。对在保密期限内因保密事项范围调整不再作为国家秘密事项，或者公开后不会损害国家安全和利益，不需要继续保密的，应当及时解密；对需要延长保密期限的，应当在原保密期限届满前重新确定保密期限。提前解密或者延长保密期限的，由原定密机关、单位决定，也可以由其上级机关决定。

第二十条 机关、单位对是否属于国家秘密或者属于何种密级不明确或者有争议的，由国家保密行政管理部门或者省、自治区、直辖市保密行政管理部门确定。

第三章保密制度

第二十一条 国家秘密载体的制作、收发、传递、使用、复制、保存、维修和销毁，应当符合国家保密规定。

绝密级国家秘密载体应当在符合国家保密标准的设施、设备中保存，并指定专人管理；未经原定密机关、单位或者其上级机关批准，不得复制和摘抄；收发、传递和外出携带，应当指定人员负责，并采取必要的安全措施。

第二十二条 属于国家秘密的设备、产品的研制、生产、运输、使用、保存、维修和销毁，应当符合国家保密规定。

第二十三条 存储、处理国家秘密的计算机信息系统（以下简称涉密信息系统）按照涉密程度实行分级保护。

涉密信息系统应当按照国家保密标准配备保密设施、设备。保密设施、设备应当与涉密信息系统同步规划，同步建设，同步运行。

涉密信息系统应当按照规定，经检查合格后，方可投入使用。

第二十四条 机关、单位应当加强对涉密信息系统的管理，任何组织和个人不得有下列行为：

（一）将涉密计算机、涉密存储设备接入互联网及其他公共信息网络；

（二）在未采取防护措施的情况下，在涉密信息系统与互联网及其他公共信息网络之间进行信息交换；

（三）使用非涉密计算机、非涉密存储设备存储、处理国家秘密信息；

（四）擅自卸载、修改涉密信息系统的安全技术程序、管理程序；

（五）将未经安全技术处理的退出使用的涉密计算机、涉密存储设备赠送、出售、丢弃或者改作其他用途。

第二十五条 机关、单位应当加强对国家秘密载体的管理，任何组织和个人不得有下列行为：

（一）非法获取、持有国家秘密载体；

（二）买卖、转送或者私自销毁国家秘密载体；

（三）通过普通邮政、快递等无保密措施的渠道传递国家秘密载体；

（四）邮寄、托运国家秘密载体出境；

（五）未经有关主管部门批准，携带、传递国家秘密载体出境。

第二十六条 禁止非法复制、记录、存储国家秘密。

禁止在互联网及其他公共信息网络或者未采取保密措施的有线和无线通信中传递国家秘密。

禁止在私人交往和通信中涉及国家秘密。

第二十七条 报刊、图书、音像制品、电子出版物的编辑、出版、印制、发行，广播节目、电视节目、电影的制作和播放，互联网、移动通信网等公共信息网络及其他传媒的信息编辑、发布，应当遵守有关保密规定。

第二十八条 互联网及其他公共信息网络运营商、服务商应当配合公安机关、国家安全机关、检察机关对泄密案件进行调查；发现利用互联网及其他公共信息网络发布的信息涉及泄露国家秘密的，应当立即停止传输，保存有关记录，向公安机关、国家安全机关或者保密行政管理部门报告；应当根据公安机关、国家安全机关或者保密行政管理部门的要求，删除涉及泄露国家秘密的信息。

第二十九条 机关、单位公开发布信息以及对涉及国家秘密的工程、货物、服务进行采购时，应当遵守保密规定。

第三十条 机关、单位对外交往与合作中需要提供国家秘密事项，或者任用、聘用的境外人员因工作需要知悉国家秘密的，应当报国务院有关主管部门或者省、自治区、直辖市人民政府有关主管部门批准，并与对方签订保密协议。

第三十一条 举办会议或者其他活动涉及国家秘密的，主办单位应当采取保密措施，并对参加人员进行保密教育，提出具体保密要求。

第三十二条 机关、单位应当将涉及绝密级或者较多机密级、秘密级国家秘密的机构确定为保密要害部门，将集中制作、存放、保管国家秘密载体的专门场所确定为保密要害部位，按照国家保密规定和标准配备、使用必要的技术防护设施、设备。

第三十三条 军事禁区和属于国家秘密不对外开放的其他场所、部位，应当采取保密措施，未经有关部门批准，不得擅自决定对外开放或者扩大开放范围。

第三十四条 从事国家秘密载体制作、复制、维修、销毁，涉密信息系统集成，或者武器装备科研生产等涉及国家秘密业务的企业事业单位，应当经过保密审查，具体办法由国务院规定。

机关、单位委托企业事业单位从事前款规定的业务，应当与其签订保密协议，提出保密要求，采取保密措施。

第三十五条 在涉密岗位工作的人员（以下简称涉密人员），按照涉密程度分为核心涉密人员、重要涉密人员和一般涉密人员，实行分类管理。

任用、聘用涉密人员应当按照有关规定进行审查。

涉密人员应当具有良好的政治素质和品行，具有胜任涉密岗位所要求的工作能力。

涉密人员的合法权益受法律保护。

第三十六条 涉密人员上岗应当经过保密教育培训，掌握保密知识技能，签订保密承诺书，严格遵守保密规章制度，不得以任何方式泄露国家秘密。

第三十七条 涉密人员出境应当经有关部门批准，有关机关认为涉密人员出境将对国家安全造成危害或者对国家利益造成重大损失的，不得批准出境。

第三十八条 涉密人员离岗离职实行脱密期管理。涉密人员在脱密期内，应当按照规定履行保密义务，不得违反规定就业，不得以任何方式泄露国家秘密。

第三十九条 机关、单位应当建立健全涉密人员管理制度，明确涉密人员的权利、岗位责任和要求，对涉密人员履行职责情况开展经常性的监督检查。

第四十条 国家工作人员或者其他公民发现国家秘密已经泄露或者可能泄露时，应当立即采取补救措施并及时报告有关机关、单位。机关、单位接到报告后，应当立即作出处理，并及时向保密行政管理部门报告。

第四章监督管理

第四十一条 国家保密行政管理部门依照法律、行政法规的规定，制定保密规章和国家保密标准。

第四十二条 保密行政管理部门依法组织开展保密宣传教育、保密检查、保密技术防护和泄密案件查处工作，对机关、单位的保密工作进行指导和监督。

第四十三条 保密行政管理部门发现国家秘密确定、变更或者解除不当的，应当及时通知有关机关、单位予以纠正。

第四十四条 保密行政管理部门对机关、单位遵守保密制度的情况进行检查，有关机关、单位应当配合。保密行政管理部门发现机关、单位存在泄密隐患的，应当要求其采取措施，限期整改；对存在泄密隐患的设施、设备、场所，应当责令停止使用；对严重违反保密规定的涉密人员，应当建议有关机关、单位给予处分并调离涉密岗位；发现涉嫌泄露国家秘密的，应当督促、指导有关机关、单位进行调查处理。涉嫌犯罪的，移送司法机关处理。

第四十五条 保密行政管理部门对保密检查中发现的非法获取、持有的国家秘密载体，应当予以收缴。

第四十六条 办理涉嫌泄露国家秘密案件的机关，需要对有关事项是否属于国家秘密以及属于何种密级进行鉴定的，由国家保密行政管理部门或者省、自治区、直辖市保密行政管理部门鉴定。

第四十七条 机关、单位对违反保密规定的人员不依法给予处分的，保密行政管理部门应当建议纠正，对拒不纠正的，提请其上一级机关或者监察机关对该机关、单位负有责任的领导人员和直接责任人员依法予以处理。

第五章法律责任

第四十八条 违反本法规定，有下列行为之一的，依法给予处分；构成犯罪的，依法追究刑事责任：

（一）非法获取、持有国家秘密载体的；

（二）买卖、转送或者私自销毁国家秘密载体的；

（三）通过普通邮政、快递等无保密措施的渠道传递国家秘密载体的；

（四）邮寄、托运国家秘密载体出境，或者未经有关主管部门批准，携带、传递国家秘密载体出境的；

（五）非法复制、记录、存储国家秘密的；

（六）在私人交往和通信中涉及国家秘密的；

（七）在互联网及其他公共信息网络或者未采取保密措施的有线和无线通信中传递国家秘密的；

（八）将涉密计算机、涉密存储设备接入互联网及其他公共信息网络的；

（九）在未采取防护措施的情况下，在涉密信息系统与互联网及其他公共信息网络之间进行信息交换的；

（十）使用非涉密计算机、非涉密存储设备存储、处理国家秘密信息的；

（十一）擅自卸载、修改涉密信息系统的安全技术程序、管理程序的；

（十二）将未经安全技术处理的退出使用的涉密计算机、涉密存储设备赠送、出售、丢弃或者改作其他用途的。

有前款行为尚不构成犯罪，且不适用处分的人员，由保密行政管理部门督促其所在机关、单位予以处理。

第四十九条 机关、单位违反本法规定，发生重大泄密案件的，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；不适用处分的人员，由保密行政管理部门督促其主管部门予以处理。

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。

第五十条 互联网及其他公共信息网络运营商、服务商违反本法第二十八条规定的，由公安机关或者国家安全机关、信息产业主管部门按照各自职责分工依法予以处罚。

第五十一条 保密行政管理部门的工作人员在履行保密管理职责中滥用职权、玩忽职守、徇私舞弊的，依法给予处分；构成犯罪的，依法追究刑事责任。

第六章附则

第五十二条 中央军事委员会根据本法制定中国人民解放军保密条例。

第五十三条 本法自 2010 年 10 月 1 日起施行。

沁县国家保密局宣

从泄密事件看保密防范

——对近年来窃密、泄密案例的分析

保密与泄密相伴而生，此长彼消。分析泄密事件，研究泄密发生规律，有助于提高保密防范水平，有针对性地做好保密工作。笔者通过对近年来发生的泄密案件进行框架性分析，试图总结出一些具有规律性的东西。

一、近年来泄密规律分析

（一）*泄密事件的发生与国际斗争、敌我斗争形势密切相关*。保密与泄密的较量，说到底，是国际政治斗争、敌我斗争的反映。中外关系变故、台海局势紧张时期，往往是泄密事件多发期。冷战结束以后，国际形势仍处在一个错综复杂的时期，世界各国尤其是大国对情报信息的战略需求大幅上升。情报信息的搜集、分析、处理和利用，已成为国家战略能力的重要组成部分。特别是，某些敌对势力把中国作为最大的异己力量和主要对手，全方位加强对华情报窃密活动。当前，境外敌对势力对我国的窃密活动增多，情报活动频繁，已经发生的窃密案件也都反映了泄密事件发生的这种趋势。

（二）*军事、外交领域是窃密的恒常重点*。西方国家和敌对势力从未放弃对我外交、军事秘密的觊觎。我国外交战略、国防建设和“杀手锏”武器装备的发展情况，早已成为境外情报部门的重点目标。如，某间谍采取承揽工程等手段窃取我军事秘密案、某机关干部向某国间谍组织长期提供我重大决策秘密和重要情报案等。近年来，敌特机关在这一领域花费的“本钱”更大、筹码更高。如，为得到我中央文件、领导人事变动情况，某外国公司长期不惜花费大量报酬和“顾问”费用，通过我国的公司人员非法获取我大量国家秘密。

（三）*窃密手段多样，在愈发重视高科技窃密的同时，并未放弃传统、人工的窃密方式*。一方面，境外情报机关广泛运用各种现代技术手段，进行情报窃密活动。间谍卫星、微型窃听窃照器材、加密遥控技术等广泛应用于情报搜集活动。一些发达国家利用在信息技术领域中的垄断地位，在外销设备中做手脚、安后门，制造安全隐患。窃密与反窃密斗争越来越具有高科技抗衡的特点。另一方面，境外情报机构从未放弃传统、人工的窃密手段。境外情报机关深知，无论技术多么先进，也了解不到对方脑子里所想的，间谍卫星拍不到办公室里的研究过程，这些都要靠人力的情报活动搜集。

（四）*“官方”窃密的同时，积极发展“民间”窃密组织*。某外国情报组织制定的对华情报方针指出，凡是能够运用公开、合法手段搞到的情报，就不用秘密的手段去搜集，以便腾出力量进行更深、更隐蔽的情报活动。境外组织的情报人员有的以经贸、投资办厂、旅游等公开合法手段为掩护，进行窃密活动。他们积极推行“雇员当地化”，用高薪聘请我政府官员为“顾问”，雇用我离退休干部为“联络员”。某西方国家已形成了民间化的情报组织体系，该国的许多商社都进行情报活动。有的国家还利用在我国设立的各种“中心”、“基金会”，实施国际学者交流计划等，开展渗透和情报活动。

二、保密防范的问题与不足

（一）*思想麻痹，保密意识差*。通过对泄密事件的分析，可以看出，不少人包括一些领导干部，缺乏基本的敌情观念和保密常识。有的领导干部在家人面前和公共场所随意谈及国家秘密；有的涉密单位保密审查形同虚设，参观、交流来者不拒；有的内外不分，认敌为友。2001 年 10 月，某单位在打扫地下室库房卫生时，由于缺乏基本的保密意识，将存于库房的大量涉密文件、资料卖给废品回收人员，造成严重泄密。某研究所一位外籍人士，经常以借阅图书名义从内部资料室借阅内部资料和秘密文件，甚至把资料、文件带到宾馆，有的资料还复印。这些都没有引起任何人的怀疑。正是这种麻痹和松懈，给窃密者留下了可乘之机。

（二）*管理不到位，保密制度不落实*。有些机关单位保密管理不到位，规章制度不落实。近年来，反映在这方面的问题十分突出。2004 年 8 月，在对某涉密公司进行保密检查时，发现大量涉密计算机与国际互联网连接，严重违反了涉密计算机保密管理的有关规定。某部门将有关绝密文件用特快专递进行传送，严重违反保密规定。某省委一干部擅自将涉密计算机与互联网相联，造成泄密。

（三）*保密应急响应迟钝*。主要表现在：不少窃密持续时间长、隐藏深、危害大；泄密发现、报告、查处不及时。有的间谍隐藏达 15 年之久。有个单位在绝密级文件丢失后，直至次年 9 月才向有关部门报告，至找到该文件，失控达 1 年零 2 个月。

（四）*泄密惩处不力，标准不统一*。个别地方和部门，出于本地、本部门利益，对泄密事件敷衍推诿，大事化小，小事化了；对责任人处理，避重就轻，得过且过。

三、有针对性地做好保密防范工作

（一）*重点是做好人的工作*。重视人的工作，是国际上保密工作的“通则”要求。美国联邦调查局有一个掌握核心机密的 200 多人的名单，为了防止他们泄密，有专门的保护措施，不准他们与外国人接触。近年来，境外情报组织日益向我党政军机关渗透，采取“打进来、拉出去”的办法，对我内部人员拉拢、腐蚀。对此，应当给予高度重视和警惕。当前，尤其要制定和加强涉密人员管理的规定，尽快研究解决涉密人员无序流动和“脱密期”流于形式的问题。

（二）*关键是完善、落实保密制度*。靠制度管人、管事。泄密事件的发生与违反保密制度须臾不离，这是所有泄密事件的共性。同样，减少泄密事件的发生，也要在完善制度、落实制度上下功夫。从对历年的泄密事件分析可以清晰地看出，在国家加大对军工企业和国家统一考试管理力度、各项相关制度得到有效落实后，这两个领域的泄密事件明显呈下降趋势。要通过制度建设，切实解决保密制度“说在嘴上，写在纸上，挂在墙上”的老问题，提高制度的执行力。

（三）*重视高技术的发展，依靠高技术手段抗衡窃密*。高技术抗衡窃密，表现在两个方面：一是防范；二是检查。当前，我国信息科学技术整体落后，保密技术发展与保密工作面临与形势不相适应的问题仍然十分突出。一方面，保密技术检查手段相对落后，对已经存在的泄密隐患不能及时发现；另一方面，保密技术防范能力较弱，管理措施主要靠“禁止”和“封堵”。发展保密技术，当务之急，是发展具有自主知识产权的保密技术产品和检查工具，尽快改变高技术产品和核心技术受制于人的被动局面。

（四）*构建泄密预警、应急机制，加大泄密督查、惩处力度*。要建立保密工作预警、应急响应机制，研究境外情报机关的窃密动向，及时、果断、高效处置泄密事件；要建立泄密事件危害评估机制，对重大泄密事件进行危害评估；要统一标准，规范执法行为，统一执法程序，提高执法水平，严肃查处泄密事件。

◎蒋 文