|  |
| --- |
| **新修订的《保密法》新增和修改条款的解读**  **-----摘自百度文库** |
|  |
|  |
|  |
| **一、总则**  1、明确规定了国家秘密受法律保护的原则。  **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。  解读：  本条是关于国家秘密法律保护原则和本法适用范围的规定。  第一款确立国家秘密受法律保护原则。国家秘密直接关系国家安全和利益，必须受到法律保护。总则部分明确宣示国家秘密受法律保护，有利于明确保守国家秘密的国家责任，有利于强化机关、单位及相关人员特别是涉密人员的保密职责，有利于增强机关、单位和公民的保密意识。  第二款明确保密法律关系的义务主体。保密法律义务是宪法义务的具体化。义务主体包括一切国家机关、武装力量、政党、社会团体、企业事业单位和公民。“国家机关”，是指中央和地方各级国家权力机关、行政机关、审判机关、检察机关；“武装力量”，是指中国人民解放军现役部队和预备役部队、中国人民武装警察部队和民兵；“政党”，是指中国共产党及参政的各民主党派；“社会团体”，是指各级工会组织、共青团组织、妇女联合会组织等人民团体，也包括各种学会、协会、研究会等组织；“公民”，是指具有中华人民共和国国籍的人。  以上义务主体可以分为两大类，一类是国家秘密知悉范围内的主体，一类是国家秘密知悉范围外的主体。这两类主体承担的保密义务有所不同。如国家秘密知悉范围内的人员，应当依法保守、保护所知悉、管理的国家秘密；国家秘密知悉范围外的人员，不得非法获取国家秘密，不得非法持有国家秘密载体，在国家秘密安全受到威胁时应采取保护措施并及时报告。  第三款明确危害国家秘密安全的行为必须受到法律追究。“危害国家秘密安全的行为”，主要包括严重违反保密规定的行为，泄露国家秘密的行为，境内外一切组织、机构和人员非法获取国家秘密的行为等。对危害国家秘密安全的行为，按照情节轻重，依法追究法律责任。严重违反保密规定，应当追究行政责任的，依照《中华人民共和国公务员法》（以下简称《公务员法》）、《行政机关公务员处分条例》等法律法规处理；情节严重，构成犯罪的，依照《中华人民共和国刑法》（以下简称《刑法》）追究刑事责任。  **2、修改完善了保密工作方针**  **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。  解读：  本条是关于保密工作方针的规定。  “积极防范、突出重点”，是1983年中央提出的保密工作方针，体现了保密工作的基本特点和规律。保密工作的本质特征决定了保密工作必须以防范为主，把工作重点放在预防上，做到防患于未然，最大限度地减少窃密泄密事件的发生。“积极防范”，强调的是主动、事先的防范，以防止窃密泄密为出发点，构筑人防、物防、技防相结合的坚固的综合防范体系。“突出重点”，就是要确保核心秘密的绝对安全。国家秘密信息涉及领域广、数量大，应当根据保密管理对象涉密程度不同，采取相应的保护措施，合理分配保密资源，把核心秘密作为重点加以保护。如对绝密级国家秘密、保密要害部门部位、核心涉密人员、绝密级信息系统，必须采取更严格的保密管理措施。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。国家秘密在任何一个地区、部门或环节被泄露，都会损害国家安全和利益，影响保密工作的整体效能。在加强重点保密管理的同时，必须坚持全面管理，实施综合防范。  “依法管理”，就是要依照国家法律法规管理国家秘密。将“依法管理”确定为保密工作方针的内容，是依法治国、建设社会主义法治国家的必然要求，是推进保密依法行政、不断提高保密工作制度化、规范化、程序化水平的迫切需要。依法管理，一是有法可依，要求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，要求机关、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，要求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，要求对违反保密法律法规的行为依法查处，严肃追究法律责任。  “既确保国家秘密安全，又便利信息资源合理利用”，是对1988年保密法中“既确保国家秘密又便利各项工作”这一表述的修改。“便利各项工作”的表述，是针对当时存在保密范围过宽、保密过度等给相关工作开展带来不便的问题提出来的，在当时特定条件下具有一定的积极意义。考虑到在实施过程中，“便利各项工作”有时容易被曲解，成为一些机关、单位和人员规避保密规定、不履行保密义务的借口，这次修订将其修改为“便利信息资源合理利用”。这一修改要求，在确保国家秘密安全的同时，充分遵循信息化条件下信息资源利用和管理的客观规律，建立科学有效的保密管理制度，促进信息资源的合理利用。  规定法律、行政法规规定公开的事项，应当依法公开，是为了正确处理公开与保密的关系，既确保国家秘密安全，又充分保障公民的知情权、参与权和监督权。信息保密和信息公开是辩证统一的，都是为了维护国家和人民的利益。该公开的不公开，不该公开的公开了，都会损害国家和人民的利益。“依法公开”，一是指法律法规要求公开的必须公开，不得以保密为由不予公开或者拒绝公开；二是指公开前必须依法进行保密审查，公开事项不得涉及国家秘密；三是指公开的程序和方式必须符合法律规定。  **3、规定了机关单位实行保密工作责任制**  **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。  解读：  本条是关于机关、单位保密工作的基本要求。  规定机关、单位实行保密工作责任制，体现了《中华人民共和国宪法》第二十七条关于一切国家机关“实行工作责任制”的要求。保密工作责任制主要包括领导干部保密工作责任制、定密责任制、保密要害部门部位负责人及工作人员责任制、涉密信息系统管理和维护人员责任制等。实行保密工作责任制，有利于加强保密工作组织领导，明确相关人员保密工作职责，确保保密工作落到实处。  在保密工作责任制中，保密工作领导责任制尤为重要。党中央对领导干部落实保密工作责任制历来高度重视，相继下发了一系列文件规定。《中共中央关于加强新形势下保密工作的决定》指出，各地区各部门要“落实保密工作领导责任制”。领导干部应当在职权范围内对保密工作担负起领导和管理的责任。党政主要负责同志要担负起全面领导的责任，重视、关心和支持保密工作；分管保密工作的负责同志要担负起具体组织领导的责任；分管有关方面工作的负责同志要管好分管工作范围内的保密工作。保密工作领导责任制的执行情况，由组织人事和纪检监察部门纳入领导干部民主生活会和政绩考核内容。《中国共产党纪律处分条例》、《中共中央保密委员会关于党政领导干部保密工作责任制的规定》明确规定，对不认真履行保密工作领导责任制，疏于保密管理或在保密工作方面失职的领导干部实行责任追究。一是在保密工作方面不负责任，致使发生重大失泄密事故，造成或者可能造成较大损失的，对负有主要领导责任者，给予警告或者严重警告处分；造成或者可能造成重大损失的，对负有主要领导责任者，给予撤销党内职务处分。二是对单位存在重大泄密隐患或者发生失泄密事件负有主要领导责任的党政领导干部，视情节轻重，按照干部的管理权限给予警告、严重警告、撤销党内职务、留党察看或者开除党籍处分。三是对玩忽职守、拒不履行保密工作领导职责，造成严重失泄密后果的党政领导干部，要依法追究其法律责任。  “健全保密管理制度”，是指机关、单位依据有关保密法律、法规、规章的规定，结合本机关、本单位涉及国家秘密的具体情况，制定本机关、本单位的保密制度。主要包括：国家秘密确定、变更和解除制度，涉密信息及涉密载体保密管理制度，信息系统和信息设备保密管理制度，信息公开保密审查制度，保密要害部门部位保密管理制度，领导干部保密管理制度，涉密人员保密教育和管理制度，保密工作责任制考核制度等。  “完善保密防护措施”，是指机关、单位为确保国家秘密安全所采取的管理措施和技术措施，包括人防、物防、技防等。如对涉密信息系统实行分级保护，采取技术防护措施等。  “开展保密宣传教育”，是指机关、单位应当定期对工作人员特别是领导干部和涉密人员进行保密形势、保密法律法规、保密技术防范知识等方面的教育培训，以增强保密意识和保密技能。  “加强保密检查”，是指机关、单位应当切实加强对本机关、本单位遵守保密法律法规、落实保密责任、采取保密防护措施及其效果等进行检查，以查促管，以查促防，以查促改，以查促教。  **二、国家秘密的范围和密级**  **1、建立定密责任人制度。**  **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。  解读：  本条是关于定密责任人制度的规定。  定密是一项十分重要的专门工作，政策性、行业性、专业性都很强。针对当前定密主体宽泛、责任不明确、程序不规范等问题，这次修订专门设立了定密责任人制度。  第一款规定定密责任主体。明确定密责任人为机关、单位负责人及其指定的人员。机关、单位负责人是法定的定密责任人。定密工作量较大、业务工作具有特殊保密要求的机关、单位，可以由机关、单位负责人指定人员，履行定密责任人的职责。定密责任人职责既包括按照保密事项范围确定国家秘密，也包括根据情况变化变更和解除国家秘密。  第二款规定定密工作程序。明确先由承办人对照保密事项范围提出国家秘密确定、变更和解除的具体意见，再由定密责任人审核批准并承担法律责任。  授权专门人员行使定密权，是许多国家的通行做法。如美国《国家安全信息保密》规定，原始定密权只能由下列人员行使：总统、副总统，总统任命并在《联邦日志》上公布的有关机构负责人和官员，以及上述具有原始定密权人以书面形式授权的其他官员。俄罗斯《联邦国家秘密法》规定，有权确定国家秘密的官员要经过俄罗斯联邦总统批准，他们大多是国家权力机关的负责人，对决定将某一具体信息定为国家秘密承担个人责任。法国《部际保密条例》规定，有权定密的官员由各部部长在其职权范围内根据规定的条件进行确定。近年来，国家保密行政管理部门先后在部分省、自治区、直辖市、中央国家机关组织开展了定密责任人制度试点工作。下一步，将制定具体办法，进一步明确定密责任人的职责权限、资格条件、指定程序及管理培训制度等。  **2、上收定密权限。**  **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。  解读：  本条是关于定密权限的规定。  第一款确立定密应当遵守权限的原则。国家秘密属于国家所有，定密属于国家事权，定密权限应当由法律限定。机关、单位是否具有定密权和具有何种层级的定密权，必须依照法律规定。  第二款对定密权作出限定。这次修订改变了以往任何机关、单位都可以确定任何密级的做法，上收了定密权限，不再授予县级机关定密权，取消了设区的市、自治州一级机关绝密级定密权。本款还规定，具有定密权的中央国家机关、省级机关和设区的市、自治州一级的机关，可以授予下级机关、单位相应密级的定密权。为了进一步明确定密权限，确保定密授权慎重节制，国家保密行政管理部门将另行制定具体办法予以规范。  第三款规定无权定密的处理办法。主要有两种情形，一种是上级机关、单位对某一事项已经定密的，机关、单位在执行时应按该事项已定密级确定。如中央下发的国家秘密文件，各地区各部门在贯彻过程中，就该事项再产生的涉密文件资料，应当按中央文件的密级确定同等密级，不得擅自改变密级。另一种是机关、单位（包括无定密权的县级机关）产生保密事项范围有明确规定而无权确定相应密级的国家秘密事项时，应当先行采取保密措施，同时立即报请具有相应定密权的上级机关、单位确定，没有上级机关、单位的，则根据该事项所涉及的业务范围，报请具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。接到定密报告的机关、单位或者保密行政管理部门，应当及时作出批复。  第四款规定公安、国家安全机关的定密权限。强调公安、国家安全机关必须在其工作范围内，按照规定的定密权限定密。  **3、明确保密期限。**  **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。  解读：  本条是关于国家秘密保密期限的规定。  第一款规定确定保密期限，应当根据国家秘密事项的类型性质、重要程度、时效需要及其他制约因素，按照维护国家安全和利益的需要，将保密期限规定在明确的时间内。在确定保密期限时，能够确定具体期限的应当予以明确，保密的具体期限，可以是应当保密的时间段，也可以是明确的解密时间；不能明确具体期限的，应当将能够明确判断的某种情形的出现或者事件的发生设置为解密条件，一旦设定的条件成立，该国家秘密事项的保密期限即告终止。  第二款对不同密级国家秘密事项的保密期限分别限定了最长时限，即绝密级不超过30年，机密级不超过20年，秘密级不超过10年。机关、单位在确定保密期限时，应当在上述时限内确定一个合理的保密期限。本款“另有规定”，主要是指在保密事项范围中明确规定某类国家秘密事项保密期限为“长期”的情况。这些国家秘密事项具有较强的稳定性，长期关系国家安全和利益，即使确定为本款限定的最长保密期限，也难以满足保密需求。  第三款明确保密期限的3种具体表现方式，分别是保密期限、解密时间、解密条件。保密期限为具体的时限，如规定具体保密期限为5年，则从制发之日起满5年的，该秘密事项即自行解密；解密时间为具体日期或时刻，如规定某一秘密事项的解密时间为2020年5月1日，则到2020年5月1日该秘密事项保密期限到期，自行解密；解密条件为具体明确便于判断的事件或情形，如规定某一秘密事项以执行完毕作为解密条件的，则该事项实施完成后，自行解密。机关、单位在确定具体事项的保密期限时，如果所依据的保密事项范围已经对该类事项的保密期限作了明确规定，应当按照规定确定保密期限。  第四款规定特殊解密条件，即国家秘密事项经正式公布即视为解密。一般情况下，国家秘密需经法定程序，解密后才能确定是否公开。本款把正式公布视同解密，兼顾了程序与效率。“正式公布”，是指履行批准手续后通过媒体、政府门户网站、告示等正规途径对外公开发布。机关、单位通过正式公布这一特殊方式解密时，应当履行法定的信息发布审批程序，并作出记载。未经批准擅自公布涉密信息的，不能视为正式公布，应当作为泄密事件处理。  **4、完善解密制度。**  **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。  解读：  本条是关于解密制度的规定。  解密制度是定密制度的重要组成部分。解密意味着解除有关保密措施，知悉范围内的机关、单位和人员不再需要履行相关保密义务。  本条主要规定两种解密方式。一是**自行解密**，即保密期限已满的国家秘密事项，自行解密。机关、单位对于保管、使用的国家秘密保密期限已满而未收到原定密机关、单位延长保密期限通知的，可以认定该项国家秘密已经自行解密，不需要继续履行相应的保密义务。二是**审查解密**。机关、单位应当定期审核所确定的国家秘密事项，特别是保密期限即将届满的国家秘密事项。经审核，仍在保密期限内但不需要继续保密的，应当及时履行程序予以解密；认为仍应继续保密，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。本条规定了两种“不需要继续保密”的法定条件。一种是**定密时依据的保密事项范围已作调整，该事项已不再属于国家秘密的**。另一种是**公开不会损害国家安全和利益的**。有权决定提前解密或者延长保密期限的机关、单位，包括原定密机关、单位及其上级机关，作出决定后，应当通知原知悉范围的机关、单位和人员。  适用本条规定应当注意，保密事项范围中明确规定某类事项的保密期限为“长期”的，原定密机关、单位认为需要解密的，应当提请规定保密事项范围的机关批准，不得擅自决定解密。对于非由本机关、本单位确定的国家秘密事项，认为符合解密条件或者需要延长保密期限的，可以向原定密机关、单位或者其上级机关提出建议，不得自行决定。延长保密期限的决定应当在保密期限届满之前作出，并提前发出通知，避免知悉范围内的机关、单位和人员在保密期限届满时未接到通知而自行解密。  解密制度是许多国家保密制度的重要内容。如美国《国家安全信息保密》规定了系统审查解密、强制审查解密、自动解密等3种解密方式。为解决解密工作不适当、不统一、不及时问题，美国还专门建立了国家解密中心，负责指导、协调、监督各部门解密工作。俄罗斯《联邦国家秘密法》对解密也有专门规定：一是规定了保密期限。国家秘密信息的保密期不得超过30年。如有特殊需要，可由部门间保密工作委员会作出延长保密期的决定。二是规定了解密的条件。根据国际条约应当公开的信息或者客观情况发生改变，没有必要继续保护的信息应当解密。三是规定了解密审查。有权将信息定为国家秘密的国家机关负责人必须定期（至少每5年一次）重新审核各机关、企业、机构、组织现行保密信息清单的内容，特别是有关信息定密的必要性及密级的合理性。四是规定了解密监督制度。有权将信息定为国家秘密的国家机关负责人可根据其任命的专家委员会的意见，作出原信息载体定密期延长的决定。国家机关、企业、机构、组织负责人有权将由下属人员不当定密的信息解密。  **三、保密制度**  **1、**涉密信息系统保密管理制度。  **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  解读：  本条是关于涉密信息系统保密管理的规定。  第一款确立涉密信息系统分级保护原则。  “涉密信息系统”，是指由计算机及其相关和配套设施、设备构成的，按照一定应用目标和规则存储、处理、传输国家秘密信息的系统或网络。涉密信息系统与公共信息系统的区别，主要体现在4个方面：一是信息内容不同。涉密信息系统存储、处理和传输的信息涉及国家秘密和其他敏感信息，应严格控制知悉范围；公共信息系统存储、处理和传输的信息不能涉及国家秘密。二是设施、设备标准不同。涉密信息系统的安全保密设施、设备，必须符合国家保密标准；公共信息系统的安全保密设施、设备也应符合一定技术标准要求，但并不要求执行国家保密标准。三是检测审批要求不同。涉密信息系统必须满足安全保密需求，符合国家保密标准要求，投入使用前必须经安全保密检测评估和审查批准；公共信息系统投入使用前也需要进行相关检测，但检测的目的和要求不同。四是使用权限不同。涉密信息系统要严格控制使用权限；公共信息系统则是开放性的，只要具备一定访问条件就可以使用。  “涉密程度”，是指涉密信息系统存储、处理和传输的国家秘密信息的密级，是确定系统安全保密防护级别的依据。涉密信息系统应当按照系统规划设计处理信息的最高密级，划分为绝密、机密和秘密三个级别，并按照不同强度的防护要求进行保护。集中处理工作秘密的信息系统，应当参照秘密级信息系统进行保护。  “分级保护”，是指涉密信息系统的建设使用单位依据分级保护管理办法和国家保密标准，对不同级别的涉密信息系统采取相应的安全保密防护措施，确保既不“过防护”，也不“欠防护”。各级保密行政管理部门根据涉密信息系统的不同级别实施相应的监督管理，确保涉密信息系统及其存储、处理、传输的国家秘密信息的安全。  第二款规定涉密信息系统保密设施、设备规划建设和配备要求。一是涉密信息系统必须配备符合国家保密标准的设施、设备。国家保密局制定的《涉及国家秘密的信息系统分级保护技术要求》、《涉及国家秘密的信息系统分级保护方案设计指南》、《涉及国家秘密的信息系统分级保护管理规范》等国家保密标准对此有明确规定。二是涉密信息系统保密设施、设备建设必须与整个系统同步规划，同步建设，同步运行，在方案设计、工程实施、投入使用和系统运行等阶段，保证保密设施、设备建设与系统建设过程同步，以实现安全保密防护措施与系统应用的有机结合，避免“带病运行”。  第三款规定涉密信息系统投入使用必须经检查合格。根据《涉及国家秘密的信息系统审批管理规定》，涉密信息系统投入**使用前**必须经过系统测评和系统审批两个环节。系统**建设完成后**，应通过国家保密行政管理部门授权的测评机构的安全保密测评，经具有审批权限的保密行政管理部门审查批准，符合涉密信息系统分级保护要求后，方可投入使用。  根据涉密信息系统分级保护管理规定和标准要求，除上述系统测评和系统审批两个环节外，涉密信息系统的全过程保密管理还包括系统定级、方案设计论证、工程实施、日常保密管理、保密监督检查和系统废止等环节，各个环节均应满足相应的保密管理要求。**系统定级**，是指涉密信息系统建设使用单位依据系统规划设计处理信息的最高密级，确定系统的保护等级。**方案设计论证**，是指涉密信息系统建设使用单位组织涉密信息系统集成资质单位等，依据分级保护技术要求、管理规范和方案设计指南，进行系统方案设计，并组织开展方案评审。**工程实施**，是指涉密信息系统集成资质单位依据分级保护建设方案，组织实施工程建设，监理资质单位负责工程监理。在涉密信息系统投入运行后，建设使用单位应当加强**日常保密管理**，明确安全保密管理策略，组建安全保密管理机构，设置安全保密管理人员，落实保密管理制度，并组织实施系统运行过程中的安全保密管理。涉密信息系统建设使用单位要定期**对系统安全保密状况、安全保密制度落实情况进行自查，并接受保密行政管理部门的检查**。**系统废止，**是指涉密信息系统不再使用时，系统建设使用单位应当向保密行政管理部门备案，并按照保密要求对涉密信息设备、产品、国家秘密载体等进行处理。  **2、增加不得将涉密计算机、涉密存储设备接入互联网及其他公共信息网络等禁止性规定。**  **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。  解读：  本条是关于信息系统和信息设备保密管理的禁止性规定。  针对信息系统和信息设备使用过程中存在的安全保密问题，本条明令禁止5种违反信息系统和信息设备使用保密管理规定的行为。这一规定对有效防范和遏制信息化条件下的窃密泄密事件发生具有重要作用。  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，将导致涉密信息处于不可控状态，直接危害国家秘密安全。  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，容易被植入“木马”等窃密程序，使涉密信息系统受远程控制，导致国家秘密被窃取。  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，将使国家秘密失去有效控制和保护，极易造成泄密。  擅自卸载、修改涉密信息系统的安全技术程序、管理程序，将造成涉密信息系统技术防护措施部分或全部失效，导致技术防护和管控能力下降或丧失，大大增加泄密风险。  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，其中存储的国家秘密信息即使删除仍可通过技术手段恢复，存在严重泄密隐患。  理解本条规定，需要把握以下概念：  “涉密存储设备”，是指用于存储涉密信息的各类介质和设备的总称，主要包括计算机硬盘、移动硬盘、光盘、优盘、存储卡、记忆棒、录音带、录像带等存储介质，以及具有信息存储功能的打印机、传真机、复印机、扫描仪、照相机、摄像机等设备。  “安全技术程序、管理程序”，是指为确保涉密信息系统的运行安全、信息安全而安装在涉密信息系统中，对系统进行安全保密防护的应用程序。**安全技术程序**主要包括身份鉴别程序、访问控制程序、主机监控程序、防病毒程序等。**安全管理程序**主要包括权限管理程序、审计管理程序、安全策略管理程序等。  “安全技术处理”，是指为保证涉密信息安全，对退出使用的涉密信息设备所采取的符合国家保密标准要求的技术处理措施，包括对涉密存储设备进行销毁或者信息消除，以确保涉密信息无法被恢复。  **3、**强化**网络运营商、服务商的责任。**  **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。  解读：  本条是关于公共信息网络运营商、服务商保密义务的规定。  在现行公共信息网络监督管理规定的基础上，本条明确了互联网及其他公共信息网络运营商、服务商的配合调查、情况报告和信息删除义务。  “运营商”，是指提供固定电话、移动电话和互联网、广播电视网络运营服务的企业。“服务商”，是指提供网络接入服务、信息浏览、文件下载、电子邮件及其他服务的企业。  配合调查义务，是指应当按照公安机关、国家安全机关、检察机关的要求，提供泄密案件调查所需要的信息等。情况报告义务，是指发现利用公共信息网络发布信息涉及国家秘密的，应当立即停止传输，保存有关记录，并报告公安机关、国家安全机关或者保密行政管理部门。信息删除义务，是指根据公安机关、国家安全机关或者保密行政管理部门的要求，删除在公共信息网络上运行的国家秘密信息。  **4、涉外保密审批管理制度。**  **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。  解读：  本条是关于对外提供国家秘密和境外人员因工作需要知悉国家秘密保密管理的规定。  针对对外交往与合作中涉密事项增多、境外人员在国有企业担任高管等情况，本条建立了对外提供国家秘密事项、境外人员知悉国家秘密的审批制度和保密协议制度。  “对外交往与合作中需要提供国家秘密事项”，是指在对外交往与合作中，从国家整体利益和对外交往合作的实际出发，权衡利弊，遵循合理、合法、适度、对等的原则，经有关机关审查批准后，向境外合作方提供国家秘密。机关、单位对外提供国家秘密时，应确定范围，进行保密审查并作必要的技术处理，报有审批权限的部门批准，执行政府间保密协定或与对方签订保密协议，任何组织和个人不得擅自对外提供国家秘密。目前，涉及这方面的具体规定主要包括《对外经济合作提供资料保密暂行规定》和《国家秘密技术出口审查规定》等。根据现有规定，机关、单位经批准后，可以根据工作需要对外提供机密级以下国家秘密，绝密级国家秘密不得对外提供。  “任用、聘用的境外人员”，是指机关、单位根据工作需要，任用、聘用的具有外国国籍的人员及港、澳、台地区的人员。随着我国对外交流与合作的不断深入，许多领域引进境外人才，任用、聘用境外管理人员、科研人员的情况日益增多。这些人员在工作中确需接触、知悉我国家秘密的，应按照“谁主管，谁负责”和“一事一批”原则，报有关机关批准。  机关、单位对外交往合作中提供国家秘密事项的，应根据有关保密法律法规，与接受方签订保密协议，要求其承担保密义务。协议的基本内容包括：对外提供的国家秘密事项及理由、承担的保密义务、违约责任等。机关、单位任用、聘用境外人员的，应根据有关保密法律法规与接触、知悉国家秘密的境外人员签订保密协议，要求其承担保密义务。协议的基本内容包括：需要知悉的国家秘密事项及理由、承担的保密义务、违约责任、协议的法律效力等。机关、单位应指定专门机构和人员对保密协议执行情况进行经常性的监督检查。一旦发现违反协议的情形或存在威胁国家秘密安全的行为，应立即采取有效措施，消除泄密隐患，并依法严肃追究有关责任人员的责任。  **5、企业事业单位从事涉密业务保密审查制度。**  **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。  解读：  本条是关于从事涉及国家秘密业务的企业事业单位保密管理的规定。  “保密审查”，是指保密行政管理部门单独或者会同有关部门依据相关规定和程序，对企业事业单位是否具备从事涉及国家秘密业务的条件、资格进行审核、检查和确认。保密审查的内容主要包括：企业事业单位性质、保密组织机构建设、保密制度与管理措施、保密条件保障、资本构成、人员情况等。保密审查一般采取书面审查和现场审查的方式进行。书面审查主要通过审阅申请单位提交的书面材料，对申请单位是否符合申请条件，是否同意受理并进行现场审查作出决定；现场审查主要针对书面审查中的有关问题，按照有关审查程序进行现场验证和核实，作出是否符合标准的判断。  近年来，根据国务院有关行政审批授权，保密行政管理部门对国家秘密载体制作复制单位、涉及国家秘密的信息系统集成单位、武器装备科研生产单位，实行保密资质管理。国家保密局相继制定了《印刷、复印等行业复制国家秘密载体暂行管理办法》、《涉及国家秘密的计算机信息系统集成资质管理办法》、《武器装备科研生产单位保密资格审查认证管理办法》等一系列管理规定，对保密资质单位实行分级分类管理。根据本法规定，国务院将制定具体办法，对从事涉及国家秘密业务的种类和申请条件、受理审查程序、监督管理、法律责任等进行规范。  “签订保密协议”，是指机关、单位根据有关保密法律法规的规定，与受委托从事涉及国家秘密业务的企业事业单位签订要求其保守国家秘密的书面协议。机关、单位应针对所委托的涉密业务，提出具体保密要求，采取保密措施，严格限定国家秘密知悉范围，并采取必要的保密技术防护措施，加强涉密信息系统和信息设备、涉密载体的管理。  **6、涉密人员保密管理制度。**  **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。  解读：  本条是关于涉密人员管理和权益保护的基本规定。  第一款规定涉密人员分类管理制度。“涉密岗位”，是指在日常工作中产生、经管或者经常接触、知悉国家秘密事项的岗位。日常工作中产生、经管或者经常接触、知悉绝密级国家秘密事项的岗位为核心涉密岗位；日常工作中产生、经管或者经常接触、知悉机密级国家秘密事项的岗位为重要涉密岗位；日常工作中产生、经管或者经常接触、知悉秘密级国家秘密事项的岗位为一般涉密岗位。在上述岗位工作的人员分别为核心涉密人员、重要涉密人员和一般涉密人员。机关、单位应当按照所在岗位涉密程度的不同，确定涉密人员类别。“分类管理”，是指对不同涉密岗位上工作的涉密人员，采取不同的管理措施。机关、单位应根据有关规定和工作实际，制定具体划分标准和管理办法。  第二款规定涉密人员上岗审查制度。任用、聘用涉密人员，应由用人单位组织人事部门会同保密工作机构，依据涉密人员任职条件，进行严格任前审查。审查内容一般包括个人和家庭基本情况、现实表现、主要社会关系以及与国（境）外机构、组织、人员交往等情况。  第三款规定涉密人员的基本条件。政治素质方面，应当政治立场坚定，坚决执行党的路线、方针、政策，认真落实各项保密规章制度；品行方面，应当品行端正，忠诚可靠，作风正派，责任心强；工作能力方面，应当掌握保密业务知识、技能和基本的法律知识。  第四款规定涉密人员权益保障制度。涉密人员由于工作岗位的特殊性，在就业、出境、学术成果发表等方面会受到一定限制，按照权利与义务相对等原则，在限制涉密人员合法权益时，应当依法保护涉密人员合法权益，给予相应补偿，这体现了党和国家对涉密人员的关心和爱护。  **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。  解读：  本条是关于涉密人员上岗保密要求的规定。  在涉密岗位工作，不仅需要具备很强的政治素质、业务素质，还要具备很强的保密意识和相应的保密专业知识技能。任用涉密人员，必须坚持先培训、后上岗。机关、单位对涉密人员上岗前的保密教育培训应包括以下主要内容：保密形势和敌情教育，保密工作方针、政策和法律法规教育，保密知识技能教育，岗位职责教育等。  涉密人员上岗前签订保密承诺书，对于提高涉密人员保密意识，强化涉密人员保密责任具有重要意义。保密承诺书的主要内容包括了解并遵守各项保密制度、知悉并履行保密义务、自愿接受保密审查、承担法律责任等。2009年3月，中央组织部、国家保密局、人力资源和社会保障部、国家公务员局在全国党政机关和涉密单位组织开展保密承诺书签订工作，有效加强了涉密人员教育管理，促进了涉密人员管理的规范化，初步建立了保密承诺制度。机关、单位应当把保密承诺书的签订和管理作为一项经常性工作来抓，建立健全保密承诺长效管理机制。  **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。  解读：  本条是关于涉密人员出境审批的规定。  加强涉密人员出境管理，既是保护国家秘密安全的需要，也是保护涉密人员自身安全的需要。“有关部门”，是指按照干部人事管理权限，批准、任用涉密人员的主管部门。“有关机关”是指公安机关、国家安全机关。  有关部门审批涉密人员出境要严格掌握，必要时征求公安机关、国家安全机关的意见。公安机关、国家安全机关认为涉密人员出境可能对国家安全造成危害或者对国家利益造成重大损失的，有关部门不得批准。  限制涉密人员出境是一些国家通行的做法。如德国《安全审查法》规定，从事安全敏感性工作的人员，在前往适用特别规定的国家旅行之前，无论是公务旅行还是私人旅行，都应当事先向主管机关或组织报告。如果有充分的理由证明，由于请求旅行的人员或者特定的安全敏感性岗位所决定，请求旅行的人员有可能受到外国安全机构的关注并对其构成极大威胁时，主管机关有权限制其旅行。俄罗斯、美国等国家对涉密人员出境管理也有类似规定。  **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。  解读：  本条是关于涉密人员脱密期管理的规定。  “脱密期管理”，是指在一定期限内，从就业、出境等方面对离岗离职涉密人员采取限制措施。“离岗”，是指离开涉密工作岗位，仍在本机关、本单位工作的情形。“离职”，是指辞职、辞退、解聘、调离、退休等离开本机关、本单位的情形。脱密期管理要求主要包括：与原机关、单位签订保密承诺书，做出继续遵守保密义务、不泄露所知悉国家秘密的承诺；及时清退所持有和使用的国家秘密载体和涉密信息设备，并办理移交手续；未经审查批准，不得擅自出境；不得到境外驻华机构、组织或或者外资企业工作；不得为境外组织人员或者外资企业提供劳务、咨询或者服务。  涉密人员的脱密期应根据其接触、知悉国家秘密的密级、数量、时间等情况确定。一般情况下，核心涉密人员为3年至5年，重要涉密人员为2年至3年，一般涉密人员为1年至2年。脱密期自机关、单位批准涉密人员离开涉密岗位之日起计算。对特殊的高知密度人员，可以依法设定超过上述期限的脱密期，甚至在就业、出境等方面予以终身限制。  涉密人员离岗的，脱密期管理由本机关、本单位负责。涉密人员离开原涉密单位，调入国家机关和涉密单位的，脱密期管理由调入单位负责；属于其他情况的，由原涉密单位、保密行政管理部门或者公安机关负责。  **四**、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。  解读：  本条是关于制定保密规章和国家保密标准的规定。  《中华人民共和国立法法》（以下简称《立法法》）第七十一条规定：“国务院各部、委员会、中国人民银行、审计署和具有行政管理职能的直属机构，可以根据法律和国务院的行政法规、决定、命令，在本部门的权限范围内，制定规章。”国家保密行政管理部门主管全国保密工作，具有与国务院直属机构同样的行政管理职能。这次修订，明确赋予国家保密行政管理部门保密规章制定权，对加强保密法规制度建设，提高国家秘密依法管理水平具有重要作用。  保密规章是我国保密法律体系的重要组成部分，由国家保密行政管理部门根据法律、行政法规的规定，在本部门的权限范围内制定。“依照法律、行政法规”，是指要依据保密法、保密法实施条例和国务院有关保密工作的决定、命令，以及其他涉及保密工作的法律法规，同时严格遵循《立法法》、《规章制定程序条例》的有关规定制定保密规章。保密法实施以来，国家保密局依照有关法律法规，单独或者会同有关部门制定了一系列规章和规范性文件。修订后的保密法确立了一些新的重要制度，国家保密局将及时制定配套规章制度，同时对现有的规章和规范性文件进行清理，尽快建立健全与新的形势和任务相适应的保密规章制度体系。  国家保密标准由国家保密行政管理部门制定和发布（代号为“BMB”），主要分为管理标准和技术标准两大类。这次修订，明确了国家保密标准的法律地位。1992年以来，国家保密局制定了一系列国家保密标准，内容涉及电磁泄漏发射防护类、安全保密产品与设施类、涉及国家秘密的信息系统分级保护类等，是指导和规范保密技术防护与检查监管、安全保密产品管理等工作的重要依据。目前已发布的国家保密标准均为强制性标准。  **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。  解读：  本条是关于保密监督管理主要职责的规定。  “依法组织开展”，是指保密行政管理部门依照保密法律法规，提出有关工作规划，部署安排工作任务，督促落实工作措施，并协调解决有关问题。  保密宣传教育是党和国家宣传教育工作的重要组成部分，是保密工作的重要基础。保密宣传教育工作的主要内容包括，宣传党和国家的保密工作方针政策、保密法律法规，开展保密形势教育、保密知识技能培训、保密学科建设和学历教育等。保密宣传教育的重点对象是各级领导干部、涉密人员。要通过保密教育培训，切实提高各级领导干部和涉密人员的保密意识，增强保密防范知识和技能。要把保密教育培训与落实保密工作责任制结合起来，切实提高各级领导干部履行保密工作领导和管理职责的能力和水平。同时，应当面向全社会，努力推动保密宣传教育进机关、进社区、进企业、进农村、进课堂、进家庭，增强广大公民维护国家安全和利益的意识。要充分利用传统和现代传媒手段，灵活运用讲座、报告、技术演示、窃密泄密案例展示等多种形式开展保密宣传教育，提高针对性和实效性。  保密检查是保密行政管理部门对贯彻执行党和国家保密工作方针政策、保密法律法规情况进行监督管理的主要手段。保密检查的对象主要是机关、单位，检查内容主要包括保密工作责任制落实、制度建设、宣传教育、定密工作、保密要害部门部位管理、国家秘密载体管理、涉密人员管理、重大活动和项目保密管理、保密技术防范、泄密案件查处等情况。在发现其他组织、个人有涉嫌违反保密法律法规的行为时，也应当进行保密检查。保密检查的形式主要有综合检查与专项检查，定期检查与不定期检查等。为应对高技术窃密的威胁，必须加大技术检查力度，提高保密检查的科技含量，加强对涉密载体、涉密信息设备、涉密信息系统和涉密场所等的检查，切实增强泄密隐患和漏洞的发现能力。  保密技术防护是为防范涉密信息泄露或被窃取，应用保密科技装备和手段，对涉密载体、涉密信息设备、涉密信息系统和涉密场所等进行的安全技术保护，主要包括物理安全防护、运行安全防护和信息安全保密防护等。保密技术防护能力是国家整体保密能力的重要体现。当前，我国保密技术防护整体水平较低，一些机关、单位保密技术防护基础薄弱，保密行政管理部门必须加大保密技术防护工作力度，大力推进技术自主创新，加快保密技术装备强制配备，切实提高保密技术防护能力和水平。  泄密案件查处是依法对涉嫌泄露国家秘密的违法、违纪行为进行调查核实，组织进行密级鉴定和危害评估，对涉及的责任人员进行处理，对发现的泄密隐患和漏洞采取有针对性整改补救措施的执法活动。查处工作的主要环节包括立案、调查、处理和结案。在立案环节，应对领导批办、检查发现和机关、单位报告、群众举报、有关部门移送的涉嫌泄露国家秘密的线索和案件进行审核，作出是否进行调查和处理的决定。在调查环节，应查明泄密原因、确定泄密责任人、进行技术核查取证、进行密级鉴定和危害评估，及时采取补救措施，同时，对泄密机关、单位提出整改要求。在处理环节，应在查清泄密案件事实的基础上，根据违法违纪行为的性质和情节，督促有关机关、单位对泄密责任人作出处理，涉嫌构成犯罪的，依法移送检察机关、公安机关或者国家安全机关追究刑事责任。结案是泄密案件查处工作的最后一个环节，保密行政管理部门对已经落实整改措施、有关责任人员受到处理的，或者涉嫌构成犯罪移送检察机关、公安机关或者国家安全机关的，应依法结束案件调查，按照有关规定建立案件档案。保密行政管理部门可以根据需要，在一定范围内对泄密案件情况进行通报，充分发挥泄密案件的警示教育作用。  保密行政管理部门的指导、监督，目的是督促机关、单位按照“谁主管，谁负责”的原则，贯彻执行党和国家保密工作方针政策，落实保密法律法规规定，履行保密工作各项职责，抓好保密工作落实，而不是替代机关、单位开展具体工作。“指导”，主要包括制发文件、召开会议、教育培训、提供咨询、提出工作意见和建议等方式。“监督”，主要包括督促、检查、调查、考核或者评估等方式。针对当前保密工作的新情况新问题，特别是机关、单位保密工作力量普遍比较薄弱的现状，保密行政管理部门应当不断加大工作力度，进一步加强对机关、单位保密工作的指导和监督，切实提高机关、单位保密工作水平。  **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。  解读：  本条是关于定密监督职责的规定。  为提高机关、单位定密的准确性、规范性，这次修订明确了保密行政管理部门的定密监督职责。  “国家秘密确定、变更或者解除不当”主要有5种情形：一是权限不当，即没有定密权的机关、单位定密，或者有定密权的机关、单位超出权限范围定密；二是依据不当，即未按照有关保密事项范围定密，如保密事项范围明确规定应当定密而没有定密，或者与保密事项范围规定的密级、保密期限明显不符；三是程序不当，即未按照保密法律法规规定的定密程序定密，如定密未经定密责任人审核批准，密级、保密期限、知悉范围变更后未及时书面通知；四是内容不当，即在确定密级时未同时确定保密期限和知悉范围；五是标志不当，即国家秘密标志不完整、不规范。保密行政管理部门对查实的定密不当问题，要及时发出纠正建议书，限期纠正。有关机关、单位接到纠正通知后，应当及时改正。  保密行政管理部门应当加强对机关、单位定密工作的监督。一是加强检查，将定密工作情况纳入保密检查范围，通过组织定密工作专项检查或抽查，及时发现和纠正机关、单位定密工作中存在的问题。二是对案件查处、密级鉴定工作中发现的机关、单位存在的定密问题，及时予以纠正。三是对机关、单位和个人反映的定密不当问题，及时进行核查处理。四是开展定密统计工作，掌握机关、单位定密工作情况。  **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。  解读：  本条是关于保密检查及发现问题处理的规定。  组织开展保密检查是保密行政管理部门的职责，配合保密行政管理部门的检查是机关、单位的义务。“配合”，是指机关、单位应如实提供遵守保密制度的情况，为保密行政管理部门开展保密检查提供人员协助、设备支持和工作场所等必要的工作条件，接受保密行政管理部门提出的工作意见和建议，认真落实整改措施等。  保密行政管理部门对检查中发现的违规、泄密问题，应当根据不同情况，采取以下处理方式：  一是限期整改。发现机关、单位制度建设不完善，涉密人员、涉密载体和涉密信息系统保密管理不严格，人防、物防、技防措施不到位，可能使国家秘密接触、知悉范围扩大或者失去控制的，保密行政管理部门应当要求其采取纠正、补救措施，提出整改意见，明确整改要求和整改期限，并根据整改情况决定是否进行复查。  二是责令停止使用。发现机关、单位处理涉密信息的设施、设备、场所不符合国家保密标准，技术防护没有达到保密要求，存在明显的泄密隐患和漏洞，继续使用将导致国家秘密失控或者泄露的，保密行政管理部门应当立即责令停止使用，予以封存，需要技术核查取证的，可以暂予扣留。  三是建议处分并调离。发现机关、单位有关涉密人员有本法第四十八条所列情形之一的，保密行政管理部门应当及时提出处分建议；对情节严重不适合在涉密岗位工作的，还应当建议机关、单位将其调离涉密岗位。  四是督促、指导查处工作。发现涉嫌泄露国家秘密的，保密行政管理部门应当要求有关机关、单位开展调查处理工作，及时听取案件查处情况汇报，组织进行密级鉴定和危害评估，督促对责任人员作出处理，并指导制定和监督落实整改方案。对重大泄密案件，或者跨地区、跨部门、跨领域的泄密案件，保密行政管理部门应当组织有关机关、单位共同调查处理。  五是涉嫌犯罪的，移送司法机关。保密行政管理部门经调查认为涉嫌犯罪的，应当依法移送有关机关。涉嫌构成《刑法》第一百一十一条为境外窃取、刺探、收买、非法提供国家秘密、情报罪的，移送国家安全机关；涉嫌构成《刑法》第二百八十二条非法获取国家秘密罪，非法持有国家绝密、机密文件、资料、物品罪的，移送公安机关；涉嫌构成《刑法》第三百九十八条故意泄露国家秘密罪、过失泄露国家秘密罪的，移送检察机关。  **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。  解读：  本条是关于收缴非法获取、持有的国家秘密载体的规定。  非法获取、持有国家秘密载体是直接侵害国家秘密安全的行为。保密行政管理部门对非法获取、持有的国家秘密载体予以收缴，是防止国家秘密载体进一步失控而采取的强制性保护措施。“非法获取、持有”参见本法第二十五条有关释义。“收缴”，是指保密行政管理部门将行为人非法获取、持有的国家秘密载体依法收回并作出处理。实施收缴要严格履行程序。对收缴的国家秘密载体应进行核查，查清密级、数量、来源渠道、流失范围等，并区别不同情况，采取相应处理措施。采取收缴措施，要注意把握以下几点：收缴应当在保密检查中进行，实施收缴的主体是保密行政管理部门，收缴的对象是非法获取、持有的国家秘密载体，相对人有配合的法律义务。  **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。  解读：  本条是关于密级鉴定的规定。  密级鉴定，是指对有关事项是否属于国家秘密以及属于何种密级进行鉴别和认定。密级鉴定的内容包括涉及国家秘密事项的真伪、密级、保密期限、是否解密等。密级鉴定结论是保密行政管理部门以及检察机关、公安机关、国家安全机关、监察机关等查办案件和法院审理案件的重要依据。  近年来，保密行政管理部门与有关办案机关加强协调配合，不断规范密级鉴定工作，形成了一套比较完备的制度办法。密级鉴定制度包括以下内容：  一是提起密级鉴定的机关主要是检察机关、公安机关、国家安全机关、监察机关等。  二是密级鉴定的主体只能是国家保密行政管理部门和省、自治区、直辖市保密行政管理部门，地市级以下保密行政管理部门不具有密级鉴定权。  三是密级鉴定的基本程序主要是：审查提起鉴定材料的完整性及有无进行密级鉴定的必要；审查材料内容的真伪和出处；向有关部门或办案机关了解与鉴定工作有关的案情；向材料产生机关、单位或其业务主管部门了解有关情况，征求有关专家的意见；由材料产生单位或其业务主管部门对材料泄露时的密级、保密期限和危害情况提出鉴定参考意见；依据有关保密法律法规和保密事项范围，参考材料产生单位或其业务主管部门提出的密级鉴定参考意见，对鉴定材料作出鉴别和认定；向提请密级鉴定的机关出具密级鉴定书。  **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。  解读：  本条是关于处分监督的规定。  为强化对严重违规和泄露国家秘密责任人员的责任追究，本条明确了保密行政管理部门处分监督的职责。“不依法给予处分”，主要包括应当给予处分而不处分，应当追究领导责任而不追究，对责任人员的处理明显偏轻或者偏重，没有按规定时限予以处理等情形。“拒不纠正”，主要是指机关、单位对保密行政管理部门提出的纠正建议，无正当理由拒绝执行，或者推诿、拖延，在规定时限内不作处理等情形。  保密行政管理部门提出纠正建议，主要采用书面建议方式，也可根据工作需要，采取约谈有关机关、单位负责人或者现场督查等方式。对于机关、单位拒不执行纠正建议的，保密行政管理部门可以根据具体情况，按照干部管理权限提请该机关、单位的上一级业务主管部门或者监察机关，依法追究负有责任的领导人员和直接责任人员的责任。  **五、法律责任**  **1、明确了严重违反保密规定行为的法律责任。**  **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。  解读：  本条是关于严重违规行为法律责任的规定。  第一款明确本法第二十四条、第二十五条、第二十六条列举的禁止行为的法律责任。这些违规行为是导致保密措施失效，国家秘密失控，保密技术防护体系受到破坏，国家秘密安全遭受严重威胁的最常见、最典型的行为，应当依法追究有关责任人员的法律责任。这一规定表明，不论是否产生泄密实际后果，只要发生所列举的严重违规行为之一的，都应依法追究责任。  本款主要规定两种法律责任形式：  一是行政责任。对国家工作人员，应按照《公务员法》、《行政监察法》、《行政机关公务员处分条例》的有关规定，依法给予处分。  二是刑事责任。对于情节严重、符合刑事立案标准的，应当依法移送检察机关、公安机关或者国家安全机关，追究刑事责任。根据《最高人民检察院关于渎职侵权犯罪案件立案标准的规定》，故意泄露国家秘密的立案标准是：泄露绝密级国家秘密1项（件）以上的；泄露机密级国家秘密2项（件）以上的；泄露秘密级国家秘密3项（件）以上的；向非境外机构、组织、人员泄露国家秘密，造成或者可能造成危害社会稳定、经济发展、国防安全或者其他严重危害后果的；通过口头、书面或者网络等方式向公众散布、传播国家秘密的；利用职权指使或者强迫他人违反国家保守秘密法的规定泄露国家秘密的；以牟取私利为目的泄露国家秘密的；其他情节严重的情形。过失泄露国家秘密的立案标准是：泄露绝密级国家秘密1项（件）以上的；泄露机密级国家秘密3项（件）以上的；泄露秘密级国家秘密4项（件）以上的；违反保密规定，将涉及国家秘密的计算机或者计算机信息系统与互联网相连接，泄露国家秘密的；泄露国家秘密或者遗失国家秘密载体，隐瞒不报、不如实提供有关情况或者不采取补救措施的；其他情节严重的情形。  第二款规定对尚不构成犯罪，且不适用处分人员的处理。“不适用处分的人员”，主要是指不属于组织人事和监察机关规定的可以给予处分范围的人员。不适用处分的人员有所列举的严重违规行为之一的，由保密行政管理部门督促其所在机关、单位根据内部管理规定，或者合同约定的条款，给予教育、训诫、经济处罚和解聘等不同形式的处理。  **2、明确了机关、单位发生重大泄密案件或者定密不当的法律责任。**  **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。  解读：  本条是关于机关、单位发生重大泄密案件和定密不当法律责任的规定。  “重大泄密案件”，是指符合《人民检察院直接受理立案侦查的渎职侵权重特大案件标准》规定标准的案件。根据该规定，在故意泄露国家秘密案中，重大案件是：故意泄露绝密级国家秘密1项以上，或者泄露机密级国家秘密3项以上，或者泄露秘密级国家秘密5项以上的；故意泄露国家秘密造成直接经济损失50万元以上的；故意泄露国家秘密对国家安全构成严重危害的；故意泄露国家秘密对社会秩序造成严重危害的。特大案件是：故意泄露绝密级国家秘密2项以上，或者泄露机密级国家秘密5项以上，或者泄露秘密级国家秘密7项以上的；故意泄露国家秘密造成直接经济损失100万元以上的；故意泄露国家秘密对国家安全构成特别严重危害的；故意泄露国家秘密对社会秩序造成特别严重危害的。在过失泄露国家秘密案中，重大案件是：过失泄露绝密级国家秘密1项以上，或者泄露机密级国家秘密5项以上，或者泄露秘密级国家秘密7项以上并造成严重危害后果的；过失泄露国家秘密造成直接经济损失100万元以上的；过失泄露国家秘密对国家安全构成严重危害的；过失泄露国家秘密对社会秩序造成严重危害的。特大案件是：过失泄露绝密级国家秘密2项以上，或者泄露机密级国家秘密7项以上，或者泄露秘密级国家秘密10项以上的；过失泄露国家秘密造成直接经济损失200万元以上的；过失泄露国家秘密对国家安全构成特别严重危害的；过失泄露国家秘密对社会秩序造成特别严重危害的。  “造成严重后果的”，是指应当定密的事项不定密，致使国家秘密失去保护，造成泄密的；不应当定密的事项定密，严重影响信息资源合理利用，造成较大负面影响的。  “直接责任人员”，是指直接实施违规、泄密行为的人员。“直接负责的主管人员”，是指负有直接领导责任的机关、单位负责人或者直接责任人所在部门的负责人。  **3、明确了互联网及其他公共信息网络运营商、服务商的法律责任。**  **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。  解读：  本条是关于互联网及其他公共信息网络运营商、服务商法律责任的规定。  依照有关法律法规和职责分工，公安机关、国家安全机关和信息产业主管部门对互联网及其他公共信息网络运营商、服务商分别负有相关监督管理职责。对违反本法第二十八条规定的，应当依照《中华人民共和国治安管理处罚法》、《中华人民共和国电信条例》、《计算机信息网络国际联网安全保护管理办法》、《互联网信息服务管理办法》等法律法规予以处罚。  “违反本法第二十八条规定的”，主要包括：互联网及其他公共信息网络运营商、服务商没有履行配合公安机关、国家安全机关、检察机关对泄密案件进行调查的义务；发现发布的信息涉及泄露国家秘密，没有立即停止传输和保存客户发布信息的内容及有关情况记录，并及时向公安机关、国家安全机关、保密行政管理部门报告；没有按照公安机关、国家安全机关、保密行政管理部门要求，及时对互联网或公共信息网上发布的涉密信息予以删除，致使涉密信息继续扩散。  **4、明确了保密行政管理部门工作人员的法律责任。**  **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。  解读：  本条是关于保密行政管理部门工作人员法律责任的规定。  《公务员法》第五十三条及第一百零四条明确规定，公务员必须遵守纪律，不得滥用职权、玩忽职守、徇私舞弊，违者应当依法给予处分；情节严重的，应当按照《刑法》第三百九十七条、第四百零二条有关规定，追究刑事责任。这次修订，明确保密行政管理部门工作人员不依法履行保密管理职责的法律责任，体现了权责统一的原则，有利于加强对保密行政管理部门工作人员的监督和管理，有利于强化责任意识，加强自我约束，正确履行职责。  “滥用职权”，是指保密行政管理部门工作人员超越职权范围或者违背法律授权的宗旨、违反法律程序行使职权的行为。“玩忽职守”，是指保密行政管理部门工作人员严重不负责任，不履行或不正确履行职责的行为。“徇私舞弊”，是指保密行政管理部门工作人员在履行职责过程中，利用职务之便，弄虚作假、徇私谋利的行为。应当注意的是，本条适用主体必须是各级保密行政管理部门中负有保密管理职责的人员，不包括各级机关、单位的专兼职保密干部，同时，违法行为必须是在履行保密管理职责过程中发生的。 |