

春风拂面，阳光普照，一年中最宜人的时节悄然而至。春季正是结伴出游、踏青赏景的美好时光，然而出行期间，国家安全风险同样不容忽视。让我们通过一组小测验，看看你是否能成功规避这些风险，切实守护国家安全。



拍照打卡时的抉择

小张和三名“驴友”相约戈壁徒步旅行，翻过一座沙丘，看见荒凉的戈壁上奇迹般生长着几棵胡杨树，附近拉着铁丝网，立着“军事禁区”警示牌，“驴友”举起单反相机便要拍摄，这时小张应该？

A.拿出手机快速拍完发朋友圈+定位

B.请“驴友”为自己拍个九宫格，回去发微博

C.劝阻“驴友”拍摄，将美景收在心底

正确答案:C

小安提示：《中华人民共和国军事设施保护法》第十七条规定：禁止对军事禁区进行摄影、摄像、

录音、勘察、测量、定位、描绘和记述。出行拍摄留念，切勿对准军事禁区等涉密场所，如发现可疑人员在军事禁区附近拍摄请及时制止，并向国家安全机关反映。

春季聚会时的炫耀

小李的三叔在某科研单位工作，在一次春游家庭聚餐时，三叔喝醉了酒便开始吹嘘：“我们单位那个××工程可厉害了，××核心成果已达到世界领先水平，这些秘密你们想不想知道？”面对这一情况小李应该？

A.继续追问细节

B.打开手机录视频

C.立即阻止三叔的行为，避免造成泄密危害

畅游春风十里 国家安全有你

正确答案：C

小安提示：《中华人民共和国国家安全法》第七十七条规定：保守所知悉的国家秘密是公民和组织应当履行的维护国家安全的义务。与亲友聚会时，切勿因酒酣耳热而泄露国家秘密、工作秘密或内部敏感信息，以免酿成大错。

出游回国时的手信

小孙带父母去某国旅游，入住的民宿老板听闻小孙母亲喜欢养花，便送出几包当地特有的花卉种子当做伴手礼，小孙母亲收下后十分高兴，并计划在返程时带回国栽种，这时小孙

应该？

A.帮忙装进行李箱

B.提前向有关部门报备，确保种子安全后再带回国

C.与民宿老板保持联系，经常购买各类特色种子

正确答案：B

小安提示：《中华人民共和国生物安全法》第六十条规定：任何单位和个人未经批准，不得擅自引进、释放或者丢弃外来物种。春季出国旅游时，请勿随意携带当地动植物标本和种子回国，以免造成生物安全隐患。

踏青游玩时的偶遇

小吴外出踏青游玩期间，偶遇某外国“测绘团队”，该团队测绘行为十分可疑，不但经常更换观测位置，还使用精密仪器采集地理坐标信息，架设远距离高清摄像设备拍摄涉密场所，这时小吴应该？

A.过去看看热闹，并热心帮忙

B.继续自己的行程，不再关注

C.及时向国家安全机关反映

正确答案：C

小安提示：《中华人民共和国测绘法》第八条规定：外国的组织或者个人在中华人民共和国领域从事测绘活动，应当与中华人民共和国有关部门或者单位合作进行，并不得涉及国家秘密和危害国家安全。春季出行期间，如遇可疑人员开展测绘活动，请及时向国家安全机关反映，条件允许且能确保自身安全的情况下，可记录相关人员、车辆等特征，为后续工作留存证据。国家安全，人人有责。让我们在享受春光的同时，时刻绷紧安全之弦，共同筑牢维护国家安全的钢铁长城。如遇有可疑情况可通过12339国家安全机关举报受理电话、网络举报平台（www.12339.gov.cn）、国家全部微信公众号举报受理渠道或者直接向当地国家安全机关进行举报。

服务外包并非“一包了之”

随着经济社会的快速发展，服务外包成为众多单位优化资源配置、提升运营效率的重要手段。对于涉密机关、单位而言，服务外包在带来便利的同时，也暗藏着失泄密隐患。机关、单位务必保持高度警惕，采取有效措施加以防范。

疏于管理酿大案

部分服务外包人员因工作需要，可能长期在单位办公，或者协助开展专项工作，存在接触知悉国家秘密的机会，若不严格落实保密管理，可能引发失泄密案件。如某重要涉密单位长期将办公楼物业管理外包给某物业服务公司运营，并未对该公司开展必要的保密监管。该公司保洁人员段某为满足个人私欲主动联系境外间谍情报机关，后经指使借从事保洁服务之机，通过盗取、偷拍等方式为境外间谍情报机关提供1项机密级、2项秘密级国家秘密及其他6项情报，造成重大失泄密，危害我国家安全。

审查不严有隐患

个别机关、单位资质审查不严，将涉密工作外包给无保密资质公司，或者涉密人员由于轻信、疏忽，将涉密文件资料提供给服务人员，由此引发的失泄密案件时有发生。如有关部门在工作中发现，有网民在文库类网站出售5份涉密文件。经查，某公司不具备涉密档案数字化资质，骗取多个机关单位档案管理部门信任后，承包档案资料数字化业务。该公司员工蒋某利用工作便利，先后窃取、复制档案资料中几十份涉密文件并带回家中，为谋取私利，又将其中几份放在互联网上出售，致使国家秘密泄露。

合围拉拢遭攻陷

境外间谍情报机关高度关注重点安全领域企业，企图通过钓鱼邮件、网络探扫等方式，持续不断攻击相关企业，并把掌握系统管理权限的运维人员作为攻击窃密的首选目标，对我国家安全构成现实威胁。如小李是某邮件系统厂家运维

人员，具备远程管理账号和系统管理员账号权限，负责为客户的邮件系统提供技术支持。为图方便，小李经常个人电脑上记录甲方客户的账号密码和系统管理员账号密码。境外间谍情报机关利用开源情报信息锁定了小李运维人员身份，并对小李的电脑进行了网络攻击，窃取了其电脑中的客户账号密码信息，进而通过网络跳板，对上千家重点要害部门邮件系统实施窃密，获取了大量重点要害部门内部邮件数据，造成了严重的现实危害。

国家安全机关提示

服务外包中的失泄密隐患不容忽视，涉密机关、单位必须时刻保持警惕，加强管理和防范，确保国家秘密安全。

夯实责任防风险

涉密机关、单位应夯实保密管理主体责任，明确“发包”部门监管责任，签署协议时应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。应从严审查承包单位资质条件，特别是购买服务涉及国家秘密的，应把好资质关口、签订保密协议、提出保密要求。

强化监督堵漏洞

涉密机关、单位应会同承包方建立健全各项规章制度和安全操作规范，并采取切实有效的措施确保落实到位。应积极构建人防、物防、技防“三位一体”安全防护体系，多措并举，筑牢安全保密防线。应对承包单位提供服务的过程、保密制度的执行情况、服务人员的保密行为等进行监督审计，定期排查问题隐患，防范出现偏差和风险。

加强教育保安全

涉密机关、单位应落实上岗审查要求，加强对服务外包人员的背景审查，确保其具备相应的专业技能和从业资格。应关注外包服务公司对员工的管理情况，定期对外包服务人员开展保密教育培训，提出具体保密要求，切实提升服务人员保密意识和防泄密能力，共同织密织牢安全保密防护网。（均转自国家安全部微信公众号）