《网络安全事件报告管理办法（征求意见稿）》要点解读

魏德华、李航程

2023 年 12 月 8 日，国家互联网信息办公室发布了《网络安全事件报告管理办法（征求意见稿）》（下称《管理办法》），向社会公开征求意见。《管理办法》并附两个附件：附件一《网络安全事件分级指南》、附件二《网络安全事件信息报告表》。意见征集截止时间为 2024 年 1 月 7 日。

一、适用主体

《管理办法》的适用主体为：在中华人民共和国境内建设、运营网络或者通过网络提供服务的网络运营者。《管理办法》第八条进一步针对“为运营者提供服务的组织或个人”提出要求，当“发现运营者发生较大、重大或特别重大网络安全事件时”应当提醒运营者报告网络安全事件，运营者拒不报告的，可向网信部门报告；第九条亦“鼓励社会组织和个人向网信部门报告较大、重大或特别重大网络安全事件”。

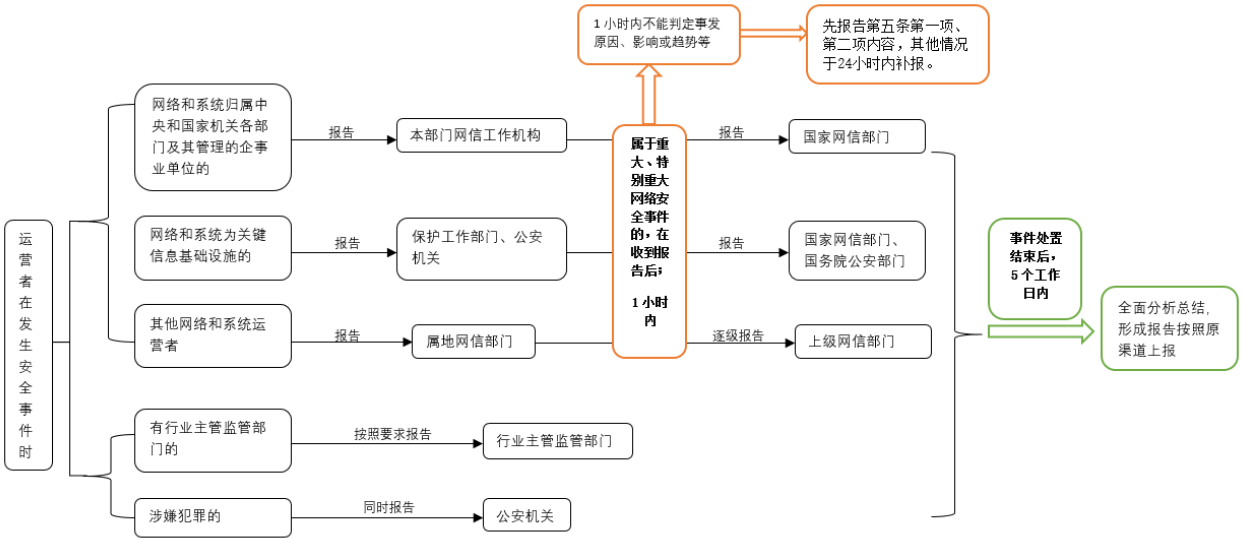
二、报告内容

根据《管理办法》第五条及附件二《网络安全事件信息报告表》，报告内容至少包括：

1. 事发单位基本信息；
2. 事发时间、地点、事件类型、事发网信系统功能描述、影响危害、已采取措施及效果；
3. 事态发展简要经过；
4. 初判原因；
5. 调查所需线索；
6. 进一步应对措施及工作建议；
7. 事件现场保护情况；
8. 其他应当报告的情况。

三、报告流程

运营者在发生较大、重大或特别重大网络安全事件时，应当于 1 小时内进行报告。具体报告流程请参见下图。



四、法律责任

《管理办法》明确规定了运营者未按照规定报告网络安全事件的，网信部门按照有关法律、行政法规的规定进行处罚。同时明确了对迟报、漏报、谎报或者瞒报的运营者及有关责任人从重处罚；以及，对已采取合理必要的防护措施努力降低事件影响的运营者及有关责任人免除及从轻处罚的情形。

五、结语

《管理办法》另附有两个附件。附件一《网络安全事件分级指南》为网络安全事件分级分类提供指引，明确了特别重大、重大、较大、一般网络安全事件的分级分类方法。附件二《网络安全事件信息报告表》为网络安全事件报告的具体内容提供了参考模板。

《管理办法》尚处于征求意见稿阶段，的近律师行将持续关注网络安全事件报告的相关立法状态，并对可能影响您业务的动态提供更新。如想了解网络安全事件报告的具体建议，请与我们联络。

欲了解更多资讯吗？

钟咏雪
合伙人
cynthia.chung@deacons.com
+852 2825 9297

朱敏慧
合伙人
machiuanna.chu@deacons.com
+852 2825 9630

陈艾姿
合伙人
elsie.chan@deacons.com
+852 2825 9604

廖海燕
合伙人
helen.liao@deacons.com
+852 2825 9779

麦思帆
合伙人
mark.stevens@deacons.com
+852 2825 5192

魏德华
资深顾问律师
edwarde.webre@deacons.com
+852 2825 9730