protiviti®
Global Business Consulting
甫瀚

《网络安全事件报告管理办法（征求意见稿）》— 运营者应对建议

敏于知

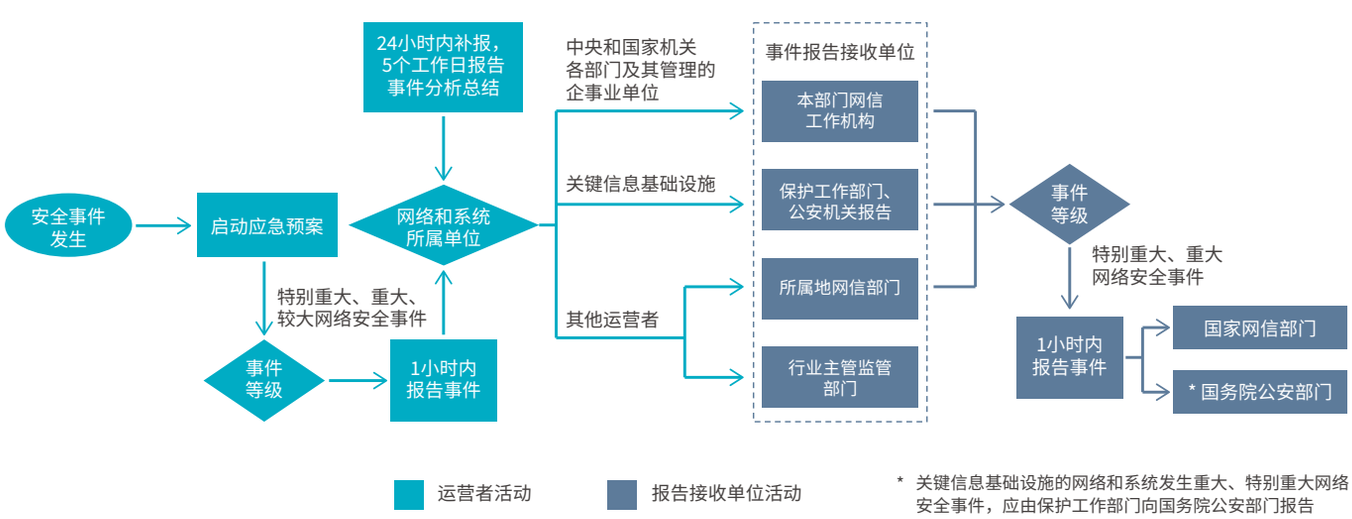
国家互联网信息办公室，在 2023 年 12 月 8 日发布了关于《网络安全事件报告管理办法（征求意见稿）[1]》（以下简称“《办法》”）公开征求意见的通知，向社会征集关于该草案的意见。

《办法》概要

《办法》旨在规范网络安全事件的报告，减少网络安全事件造成的损失，维护国家网络安全。依据上位法《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《关键信息基础设施安全保护条例》等法律法规，《办法》明确了网络安全事件报告的主体、监管统筹部门、事件报告内容和要求，以及相应的法律责任。《办法》中提到主要的定义和相关方如下：

- 适用范围：境内建设运营的网络、或通过网络提供服务的网络运营者；
- 监管统筹部门：网信工作机构、国家网信部门；
- 网络安全事件：由于人为原因、软硬件缺陷或故障、自然灾害等，对网络和信息系统或其中的数据造成危害，对社会造成负面影响的事件；
- 事件报告主体：网络或网络服务运营者。

网络安全事件报告流程



* 关键信息基础设施的网络和系统发生重大、特别重大网络安全事件，应由保护工作部门向国务院公安部门报告

[1] 国家互联网信息办公室关于《网络安全事件报告管理办法（征求意见稿）》公开征求意见的通知，发布于中央网络安全和信息化委员会办公室网站：www.cac.gov.cn/2023-12/08/c_1703609634347501.htm

《办法》要点

对于《办法》中要求的事件报告、事件跟进和事后处置的流程，甫瀚咨询总结其要点如下：

1 小时内报告

当监测到网络安全事件发生之后，运营者应启动应急预案对网络安全事件进行处置，并根据《网络安全事件分级指南》对于**特别重大、重大、较大网络安全事件在 1 小时内进行报告**。甫瀚咨询认为，网络安全事件的影响可能根据时间的推移而变化，在事件发生的初始，网络安全事件依据其影响，可能不会被定为较大或以上等级的网络安全事件。因此《办法》中提到的 1 小时，建议解释为在**事件等级初步确认的 1 小时内**进行报告。

对于 1 小时内报告网络安全事件的要求，需要运营者通过网络安全事件监测和管理工具，及时、准确地发现网络安全事件；依据网络安全事件应急预案，由网络安全事件响应小组协调处置、报告事件。

事件报告内容

《办法》提出，如运营者无法在 1 小时内判定原因，可先报告网络安全事件发生的**设施的基本情况、事件的基本情况**和其**已造成的影响**；并在 24 小时内补报**事件的影响、原因、攻击路径、漏洞、应对措施**等信息。另外，《办法》要求运营者在事件发生 5 工作日内**报告事件分析总结，即事后分析报告**。

甫瀚咨询认为，为符合《办法》的要求，运营者的网络安全事件响应人员需要有网络安全事件的分析能力，分析攻击事件的线索，并在可能的情况下采取必要的取证工作。相关人员也应有能力给出应对事件的处置建议，并可以组织事后的总结分析和整改跟进。

网络安全事件等级

《办法》的附件—《网络安全事件分级指南》可以指导运营者对网络安全事件等级进行判断。相较 2017 年中央网信办印发的《国家网络安全事件应急预案》，《指南》提出了**可量化的度量标准**，以指导运营者更直观的判定网络安全事件的等级。运营者可以根据网络安全事件等级，做出事件报告决定。甫瀚咨询通过下表予以一定的归纳总结。

我们可以看出部分的影响或危害的等级判定依然比较模糊，运营者在必要的情况下，需根据行业的最佳实践或根据事件报告接收单位的指导，进而对网络安全事件的等级进行准确的判断。

网络安全事件的影响或危害	网络安全事件等级		
	特别重大网络安全事件	重大网络安全事件	较大网络安全事件
党政机关门户网站、重点新闻网站	**省级**以上网站，**24 小时**以上不能访问	**地市级**以上网站，导致 **6 小时**以上不能访问	**地市级**以上网站，**2 小时**以上不能访问
关键信息基础设施	**整体**中断运行 **6 小时**以上；或**主要功能**中断运行 **24 小时**以上	**整体**中断运行 **2 小时**以上；或**主要功能**中断运行 **6 小时**以上	**整体**中断运行 **30 分钟**以上；或**主要功能**中断运行 **2 小时**以上。
工作、生活	单个**省级**行政区 30% 以上人口	单个**地市级**行政区 **30%** 以上人口	单个**地市级**行政区 **10%** 以上人口
居民用水、用电、用气、用油、取暖或交通出行	影响 **1000 万人**以上	影响 **100 万人**以上	影响 **10 万人**以上
重要数据泄露	对国家安全和社会稳定构成**特别严重**威胁	对国家安全和社会稳定构成**严重**威胁	对国家安全和社会稳定构成**较严重**威胁
个人信息泄露	**1 亿人**以上个人信息	**1000 万人**以上个人信息	**100 万人**以上个人信息

违法有害信息传播	① 在**主页**上出现并持续 **6 小时**以上，或在**其他页面**出现并持续 **24 小时**以上； ② 通过社交平台**转发 10 万次**以上； ③ 浏览或点击次数 **100 万次**以上； ④ 省级以上网信部门、公安部门认定为是“**特大范围传播**”的	① 在**主页**上出现并持续 **2 小时**以上，或在**其他页面**出现并持续 **12 小时**以上； ② 通过社交平台**转发 1 万次**以上； ③ 浏览或点击次数 **10 万次**以上； ④ 省级以上网信部门、公安部门认定为是“**大范围传播**”的	① 在**主页**上出现并持续 **30 分钟**以上，或在**其他页面**出现并持续 **2 小时**以上； ② 通过社交平台**转发 1000 次**以上； ③ 浏览或点击次数 **1 万次**以上； ④ 省级以上网信部门、公安部门认定为是“**较大范围传播**”的
经济损失	**1 亿元**以上	**2000 万元**以上	**500 万元**以上
其他对国家安全、社会秩序、经济建设和公众利益造成影响	**特别严重**影响	**严重**影响	**较严重**影响

事件报告接收单位

依据受影响的系统和网络的归属，《办法》为运营者指定了网络安全事件报告接收单位。他们包括中央和国家机关及其企事业单位的**网信工作机构、关基保护工作部门、地方网信办、行业主管单位**。指定的事件报告接收单位根据事件等级，将重大、特别重大的网络安全事件在 1 小时内向**国家网信部门**报告。另外，如果关键信息基础设施遭到重大、特别重大网络安全事件，将由相关单位报告**国务院公安部**。涉及犯罪的网络安全事件，运营者也应向**公安机关**报告。

对于《办法》中的报告要求，运营者应及时判断网络安全事件的范围和影响，明确事件中网络和系统的归属，按照《办法》提到的事件报告接收单位。运营者也应依据《办法》及时更新网络安全事件报告流程。

法律责任

《办法》要求运营者按规定主动报告网络安全事件。且第八条提到：为运营者提供服务的组织和个人，应提醒运营者对安全事件进行报告,可向所属地网信部门或国家网信部门报告隐瞒或拒不上报的事件和相关运营者。对于未按照该《办法》规定报告网络安全事件的运营者，网信部门将依法按照法律、法规进行处罚，并追究责任。

《网络安全事件报告管理办法（征求意见稿）》虽仍处于征求意见稿的阶段，但它的公示为保障国家安全、社会秩序和公民利益起到了作用。对网络安全事件进行报告和监管，可以保障运营者实施网络安全保护义务和责任，减少网络安全事件对国家安全、社会秩序、公民利益造成的损失，完善网络安全法律建设。

运营者将面临的挑战

《办法》规范了安全事件报告的流程，确认了网络安全事件接收单位，但同时也要求运营者提升自身的网络安全事件响应和报告的能力。运营者需要及时响应网络安全事件，在有限时间内判断网络安全事件的影响，确定事件等级，分析事件的线索、原因，采取相应处置措施。

依据《办法》提出的要求，甫瀚咨询认为运营者可能面临着以下合规挑战：

- 网络安全事件响应流程、报告流程和预案不够完善；
- 缺少有效的网络安全防护、监测和取证工具；
- 网络安全事件响应、分析、处置团队缺乏专业知识和专业能力；
- 网络安全事件响应团队配合和经验不足。

运营者应如何应对

甫瀚咨询建议运营者依据《办法》要求，结合最佳实践，进行差距分析和评估；制定包括工具、人员和流程在内的改进规划；依据运营者的风险偏好，进行改进和建设。

网络安全事件响应和报告差距分析

- **明确合规需求：**运营者根据《办法》要求进行适用性评估，分析识别可能发生的网络安全事件，评估网络安全事件发生后可能造成的影响和危害。从而，依据《网络安全事件分级指南》判断可能发生的事件的等级，并根据《办法》识别相应等级事件报告的要求。
- **进行差距分析：**运营者根据网络安全风险评估结果识别出可能发生的网络安全事件，分析自身对于网络安全事件的处置能力，识别差距。运营者可以从网络安全事件的防护、监测、响应及处置的角度，对工具、人员、和流程进行分析。

工具、人员和流程规划、建设

运营者从工具、人员能力和流程角度规划建设其网络安全响应、处置、报告能力，以减小和《办法》中提到的网络安全事件报告要求的差距，提升其网络安全事件处置的能力。

- **安全工具：**运营者可以通过部署网络安全防护工具，来抵御网络安全攻击事件，减小发生网络安全事件的可能性和影响。同时，运营者可以完善其网络安全监测工具，及时发现网络安全威胁，以减少系统和网络安全事件的影响范围和影响时间。另外，运营者应准备必要的安全取证工具，保证其准确分析安全事件的根因。
- **团队能力：**运营者内部参与安全事件响应的团队，需要具有业务知识和专业能力，协助判断网络安全事件对业务的影响，决定事件处置方案。利用工具，对事件进行识别、分析和评估，并制定安全事件的处置方案和建议。在事件后期，提出整改意见。
- **流程管理：**运营者需要建立网络安全事件响应的流程，以协调各个相关方规范、快速地响应网络安全事件。根据不同的网络安全事件类型和等级，制定安全事件检测、响应、恢复等指标，减少事件的处置时间，达到《办法》提出的及时报告的要求。

持续改进

- **评估发现：**运营者在运营和变更过程中，对网络和系统的网络安全风险进行评估，以确认网络或系统是否会遭受不同的网络安全事件，并重新对网络安全事件发生的影响和处置能力进行评估。
- **审计及技术测试：**运营者也可以通过审计、预案演练和第三方渗透测试等方式，来识别网络安全事件响应和报告过程中工具、人员和流程环节存在的缺失，并进行改进。

达于行

甫瀚咨询可提供的服务

甫瀚咨询可以为运营者的网络安全事件响应和报告提供专业的安全运营人员，协助运营者规划、设计、建设、提升网络安全事件响应和报告的能力；参与运营者的网络安全事件响应过程，以协助运营者准确及时地处置、报告网络安全事件；帮助运营者评估、检测其网络安全事件响应和报告的能力。

我们可提供的网络安全事件响应和运营服务包括：

网络安全运营能力的评估和优化

根据行业最佳实践和标准，或通过展开渗透测试、红紫队演练，来评估运营者的网络安全事件处置和响应能力。分析运营者在网络安全事件处置上的差距，给出专业建议，协助优化解决方案和流程，通过演练等方式提升运营者网络安全事件响应能力。

网络安全事件响应的规划和设计

通过评估运营者面临的安全威胁和风险，依据运营者的风险偏好、安全治理战略、组织架构和人员能力等情况，帮助运营者规划网络安全事件响应和报告的建设，设计网络安全事件防护、监测和响应方案，并为运营者网络安全建设提供咨询服务。

网络安全运营托管服务

为运营者提供专业的安全人员，负责运营者的网络安全事件监测、响应和分析工作，包括安全技术解决方案和流程的实施、维护和更新，帮助运营者处置网络安全运营范围内的安全事件。

关于甫瀚咨询

甫瀚咨询是一家全球性的咨询机构，为企业带来领先的专业知识、客观的见解、量身定制的方案和卓越的合作体验，协助企业领导者们充满信心地面对未来。透过甫瀚咨询网络和遍布全球超过25个国家的逾85家分支机构和成员公司，我们为客户提供财务、信息技术、运营、数据、数字化、环境、社会及管治、治理、风险管理以及内部审计领域的咨询解决方案。

甫瀚咨询荣膺2023年《财富》杂志年度最佳雇主百强，我们为超过80%的财富100强及近80%的财富500强企业提供咨询服务，亦与政府机构和成长型中小企业开展合作，其中包括计划上市的企业。甫瀚咨询是Robert Half（纽约证券交易所代码：RHI）的全资子公司。Robert Half（于1948年成立，为标准普尔500指数的成员公司。

联系我们

彭銘楷
董事总经理
Michael.Pang@protiviti.com

赵欣
高级经理
Xin.Zhao@protiviti.com

曹学峰
经理
Xuefeng.Cao@protiviti.com

金岳阳
高级咨询顾问
Yueyang.Jin@protiviti.com

公司地址

北京
朝阳区建国门外大街 1 号
国贸写字楼 1 座 718 室
电话：(86.10) 8515 1233

上海
徐汇区陕西南路 288 号
环贸广场二期 1915-16 室
电话：(86.21) 5153 6900

深圳
福田区中心四路 1 号
嘉里建设广场 1 座 1404 室
电话：(86.755) 2598 2086

香港
中环 干诺道中 41 号
盈置大厦 9 楼
电话：(852) 2238 0499

protiviti 甫瀚

让每位员工享有平等的发展机会
甫瀚咨询并非一间注册会计师事务所，故并不就财务报表发表意见或提供鉴证服务。

关注甫瀚咨询
获取更多资讯