ICS 35.040
CCS L 80

LD

中华人民共和国劳动和劳动安全行业标准

LD/T 04—2022

人力资源社会保障
网络安全监测和应急处置规范

Specification for human resources and social security
network security monitoring and emergency disposal

2022-06-22 发布　　2022-07-01 实施

中华人民共和国人力资源和社会保障部　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件用于指导人力资源社会保障部门开展网络安全监测和应急处置工作。

本文件由中华人民共和国人力资源社会保障部信息中心提出并归口。

本文件起草单位：中华人民共和国人力资源和社会保障部信息中心、奇安信科技集团股份有限公司。

本文件主要起草人：高琦、马丹蕾、张嵩、王岩、耿建军、唐淑静、韩晓颖、成勇、张博、王祥宇、李笑男、陈明、沈士祥、马艳婷、谢博、王可煜。

引　言

为适应人力资源社会保障信息化发展要求，提高网络安全监测和应对突发网络安全事件能力，预防和减少网络安全事件造成的损失和危害，保障基础信息网络和重要信息系统安全稳定运行，快速响应及有效处置网络安全事件，满足人力资源社会保障网络安全体系建设和管理的需要，人力资源社会保障部组织并制定了人力资源社会保障网络安全监测和应急处置规范。

人力资源社会保障
网络安全监测和应急处置规范

1 范围

本文件给出了人力资源社会保障部门网络安全监测框架和分类，规定了网络安全监测基础要求、网络安全监测技术要求、网络安全事件分类方法、网络安全事件分级规则、应急处置机构与职责、应急处置机构与职责要求，并给出安全事件应急处置流程及具体操作方法。

本文件适用于各级人力资源社会保障部门开展网络安全监测和应急处置工作。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 18030 信息技术中文编码字符集

GB/T 20984 信息安全技术信息安全风险评估规范

GB/T 20985 信息技术安全技术信息安全事件管理指南

GB/Z 20986 信息安全技术信息安全事件分类分级指南

GB/T 22239 信息安全技术网络安全等级保护基本要求

GB/T 25069 信息安全技术术语

国家网络安全事件应急预案

人力资源社会保障行业网络安全事件应急预案

3 术语和定义

GB/T 18030、GB/T 20984、GB/T 20985、GB/Z 20986、GB/T 22239、GB/T 25069和GW0204-2014界定的以及下列术语和定义适用于本文件。

3.1

信息系统 information system

应用、服务、信息技术资产或其他信息处理组件。

3.2

网络安全 cybersecurity

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

3.3

数据　data

关于可感知或可想象到的任何事物的事实。

3.4

网络安全事件　network security incident

指由于自然或者人为以及软硬件本身缺陷或故障的原因，可能对信息系统造成损害，或对社会造成负面影响的事件。

3.5

信息　information

有意义的数据。

3.6

安全监测　security monitoring

以网络安全事件为核心，通过对网络和安全设备日志、系统运行数据等信息进行实时采集，以关联分析等方式对监测对象进行风险识别、威胁发现、安全事件实时告警及可视化展示。

3.7

应急处置　emergency response

有关人员实施网络安全事件监测、预警、分析、响应和恢复等服务。

4　网络安全监测技术框架

4.1　监测主要构成

监测对象的监测过程与活动是网络安全监测技术的主要构成。主要包括以下内容：

a)　监测对象：为网络安全监测活动的采集行为提供数据源，如日志数据、包数据；

b)　监测过程与活动：通过对公众服务网和业务专网中信息系统的物理环境、通信环境、区域边界、计算环境进行数据采集、存储、分析，发现安全事件并展示与告警。

网络安全监测技术框架如图1所示：

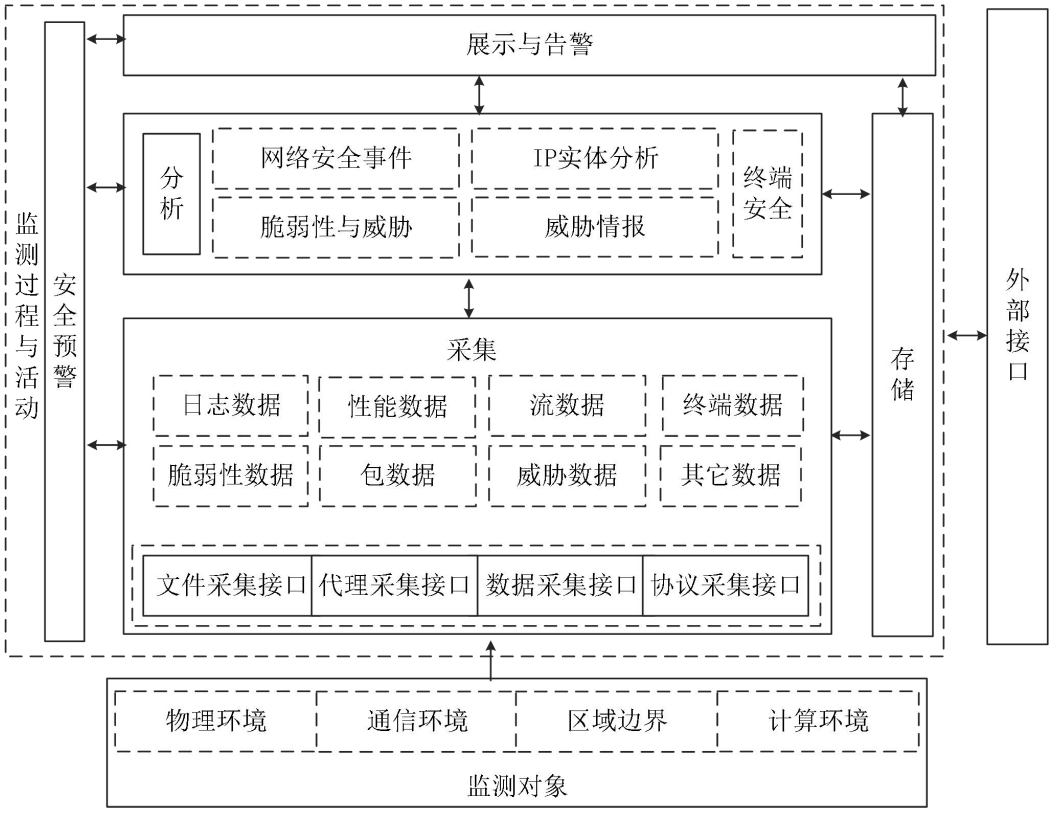

图 1　网络安全监测技术框架

4.2　监测分类

按照监测目标的不同，网络安全监测分为以下五类：

a) 网络安全事件监测：对具有损害人力资源社会保障系统业务运作和威胁网络安全的事件，按照网络安全事件不同分类、分级要求，分析识别并进行展示与告警；

b) 脆弱性与威胁监测：对监测对象的脆弱性、威胁进行评估分析，发现资产所面临的安全风险；

c) IP 实体监测：对内部实体 IP 进行分析，发现内部资产的脆弱性信息、被登录访问情况、主动外连行为等；对外部实体 IP 进行分析，发现外部 IP 的相关威胁信息；

d) 威胁情报监测：通过远控木马、APT 事件、勒索软件、黑色工具、流氓软件、其他恶意软件、窃密木马、网络蠕虫、僵尸网络等类型的威胁情报分析，发现网络安全事件；

e) 终端安全监测：纵观全网终端的安全态势，对全网终端风险做到量化观测、高效管理、全面监控。

5　网络安全监测技术要求

5.1　采集

数据采集应支持通过日志采集、协议采集、包采集等多种方式采集多种类型数据，并将采集到的数据转化为标准化数据格式：

a) 采集类型应具备从通信环境、区域边界、计算环境等采集日志数据、性能数据、流数据、威胁数据、脆弱性数据、包数据等多数据类型能力；

b) 应提供多种方式进行监测数据采集：

1) 基于文件采集、基于代理采集、基于数据采集、基于协议采集；

2) 主动采集、被动采集；

c) 采集协议支持 SNMP、Syslog、ODBC/JDBC、SFTP、NetBIOS、OPSEC 等；

d) 应提供日志分类和日志归一化手段，并转化为标准数据格式；

e) 流量采集需要完成协议解析和流量元数据收集；

f) 全网要求时钟统一，便于关联分析；

g) 采集过程不应影响采集对象正常运行。

5.2 存储

存储模块的主要功能是对监测数据进行存储和存储可靠性处理，应按照如下要求设计：

a) 应具备数据预处理功能，包括格式化处理、补充上下文信息（如用户、地理位置和区域）、数据发布等；

b) 应具备分布式存储功能，要能够将不同类型的异构数据进行分类存储，如归一化日志、流量元数据、PCAP 文件；

c) 应支持按需扩展存储节点；

d) 应满足可靠性、并发性的要求，并进行备份存储；

e) 监测数据中的重要信息应进行处理保证数据保密性；

f) 监测数据应采取校验机制保证数据完整性；

g) 重要监测数据应采取备份机制保证数据可用性；

h) 监测数据应设置访问权限，按权限限定监测数据使用；

i) 应根据具体情况对监测数据设定保存期限，并按照保存期限对数据进行存储；

j) 应对存储数据结构进行规划设计，对外部系统、上下级系统提供存储对接接口。

5.3 分析

采集到的数据应从安全事件、脆弱性与威胁、IP实体分析和威胁情报、终端安全方面进行分析，发现安全事件或威胁。具体应符合如下要求：

a) 安全事件分析应具备：

1) 采用多种关联分析技术综合分析，发现病毒感染、恶意代码、数据泄露、攻击入侵、人员违规行为与误操作等安全事件或风险；

2) 安全事件关联分析能力，通过关联分析比对识别异常行为；

3) Web 异常检测功能，通过 HTTP 协议流量分析、检测渗透行为；

4) 邮件异常检测能力，通过对 SMTP/POP3/IMAP 协议流量分析、检测基于电子邮件的外部渗透行为；

5) 按照组织内对事件分类分级的方法，对安全事件进行相应的分类分级，并按照流程进行处置分析；

b) 脆弱性与威胁分析应具备：

1) 脆弱性感知能力，对资产进行脆弱性检测和数据展示；根据不同维度进行展示，包括单个资产、安全域、信息系统等维度；

2) 威胁感知能力，对威胁进行展示和关联，包括已（未）遭受到的威胁；已遭受威胁需要对威胁进行分类，提取出关键威胁指标，提供组织的威胁态势；未遭受威胁需要对外部威胁情报进行分类展示、关联，提供与组织相关的位置威胁分析；

3) 威胁判定能力，将多个威胁进行关联分析和评估；

c) IP 实体分析应具备：

1) 通过内部 IP 的实体分析，快速获取该 IP 相关的资产信息、服务/端口暴露情况、威胁告警信息、漏洞/配置核查/弱口令等脆弱性信息、被登录访问情况、主动外连行为等，并从多维度进行可视化展示与分析；
2) 通过外部 IP 的实体分析，快速获取该 IP 相关的威胁信息、登录内网资产的情况、威胁情报鉴定信息和在网络中最早出现的时间等，并从多维度进行可视化展示与分析；

d) 威胁情报分析应具备：
1) 威胁情报库类型应包含：远控木马、APT 事件、勒索软件、黑色工具、流氓软件、其他恶意软件、窃密木马、网络蠕虫、僵尸网络等；
2) 通过域名、IP 地址、文件 MD5 值的本地威胁情报检索；威胁情报内容包含：IOC、攻击链阶段、置信度、类型描述、威胁家族、攻击事件/团伙、影响平台、情报状态、威胁描述等；
3) 自定义威胁情报，类型包含 IP、MD5、域名、URL、IP 地址:Port、IP 地址：URI、IP:Port/URI、域名:Port、域名:Port/UR；
4) 云端威胁情报查询，能够查询 IP、域名威胁类型分类，流行度评估，创建时间、更新时间、过期时间查看，能够实现开源情报判定对比、相关样本分析、情报拓线分析、历史 A 记录信息、注册信息（包含域名注册人、注册人所属组织、管理员邮箱、电话、传真、所属国家、服务运营商等），能够查看关联域名，域名数字证书等信息；

e) 终端安全分析应具备：
1) 通过集中管控能力，及时进行病毒库更新和补丁更新，解决潜在安全隐患；
2) 纵观全网终端的安全态势，对全网终端风险做到量化观测、全面监控。

5.4 展示

将采集到的安全数据和分析后的结果信息进行实时可视化展示。其展示内容和展示功能应具备如下要求：

a) 展示内容应包括：
1) 安全事件、脆弱性与威胁、IP 实体分析、威胁情报和终端安全的检测结果等实时信息；
2) 物理环境状态、拓扑关系、日志、事件和告警信息，以及事件间的关联关系；

b) 展示功能应具备：
1) 统计分析图形、报表方式展示；
2) 通过关键字快速检索获取相关日志和流量元数据及详细信息，查询追溯事件的相关原始信息；
3) 通过展示攻击过程和扩散路径，进行攻击链和攻击上下文信息的呈现，多维度展示安全威胁的影响和范围。

5.5 告警

使用告警模块对安全事件或危险进行安全监测提示，其分类、分级方式应满足下列要求：

a) 内容分类应包括：
1) 根据设备用途分为网络设备、安全设备、主机系统、数据库系统、应用程序、网管系统和日志服务器等；
2) 根据事件产生原因分为漏洞、病毒/木马、可疑活动、扫描探测、拒绝服务类、认证/授权/访问类等；

b) 根据原始事件的原始等级，重定义定级对应为“低危、中危、高危、危急”；

c) 告警方式应具备：
1) 保存告警信息直接进行展示、统计和分析；

2) 通过网络协议等多种方式发送告警相关的信息供第三方系统分析和处理；
3) 高级别告警应支持短信、即时通信等推送信息手段；
4) 告警响应动作应支持设备联动，包括对其它设备执行命令脚本、命令行等。

5.6 安全预警

使用预警模块对重大网络安全事件在内部进行安全影响评估，并持续跟进事态的发展，快速完成重大网络安全事件的预警及处置，应满足下列要求：

1) 通过导入预警包发起预警，对网络的安全影响面评估；
2) 能够呈现风险、受攻击和失陷资产的整体发展态势，以及响应处置趋势情况；
3) 能够呈现预警事件的事态发展图，以及资产被攻击或失陷时间顺序。

6 网络安全监测基础要求

6.1 性能要求

性能要求应明确的关键指标如下：

a) 原始数据并发采集能力、事件分析处理能力、事件告警延迟、1000 万条数据查询响应时间、1亿条数据查询响应时间、数据统计操作响应时间；
b) 稳定性指标要求应满足：
   1) 系统主要组件 7*24 小时运行；
   2) 系统年正常运行时间不低于 99.9%；
   3) 对被采集对象的内存资源占用率不超过 5%，对网络带宽占用率不超过 10%；
   4) 存储管理节点应保证至少一个节点正常运行且另外一个节点 30 分钟内恢复正常使用；
   5) 采集节点应保证至少一个正常工作；
   6) 集中管理节点和数据库节点应为双机或主备方式保证系统高可用性；
c) 存储能力指标要求应满足：
   1) 历史数据的保存期限不少于 6 个月；
   2) 系统日志的保存期限不少于 6 个月；
   3) 数据存储应具有备份和灾难恢复能力。

6.2 系统安全要求

支持通信加密、数据加密、状态监测、日志审计、数据备份与快速恢复、密码策略设置与核查、时间同步及超时登录设置。应具备如下要求：

a) 网络通信应采用加密协议；
b) 重要数据应加密存储；
c) 系统进行自身运行状态监测，并可产生告警；
d) 生成系统敏感操作日志，并执行定期的日志审计，查看权限仅授予审计员；
e) 系统配置信息和数据备份功能，系统崩溃时可通过备份快速恢复；
f) 与其他系统进行时间同步能力，至少每天同步一次；
g) 账号密码强度策略设置以及密码强度自动核查机制，并支持用户登录时的图形码验证功能；
h) 用户登录超时设置，按照。非法登录次数最多为 5 次登录失败后锁定时间不少于 10min，登录连接超时不得超过 10 min；

7 网络安全事件分类

7.1 分类原则

网络安全事件分为有害程序事件、网络攻击事件、数据攻击事件、设备设施故障事件、违规操作事件、不可抗力事件、其他事件等7个基本分类，每个基本分类分别包括若干个子类。

7.2 事件分类

7.2.1 概述

网络安全事件可能是由人为故意或意外行为引起的，也可能是由某些控制失效或不可抗力等原因引起的。本文件将威胁作为主要分类原则，同时适当考虑网络安全事件的产生原因、攻击方式、损害后果等，对网络安全事件进行分类。

7.2.2 有害程序事件（MI）

有害程序事件是指蓄意制造、传播或感染有害程序，从而造成系统损失或社会影响的事件。有害程序是指插入到信息系统中的一段程序，可危害系统中的数据、应用程序或操作系统的保密性、完整性或可用性，或影响信息系统的正常运行。

有害程序事件包括计算机病毒、网络蠕虫、特洛伊木马、僵尸网络、混合攻击程序、勒索软件、恶意代码内嵌网页、恶意代码宿主站点等事件，说明如下：

a) 计算机病毒（CV）：是指编制或者在计算机程序中插入的一段程序代码。它可以破坏计算机功能或者毁坏数据，并具有自我复制能力；
b) 网络蠕虫（NW）：是指与计算机病毒相对应，一种利用信息系统缺陷，通过网络自动传播并复制的恶意程序；
c) 特洛伊木马（TH）：是指伪装在信息系统中的非法远程控制程序，能够控制信息系统，包括从信息系统中窃取或截获数据；
d) 僵尸网络（BOT）：是指网络上受到黑客集中控制的一群计算机，它可以被用于伺机发起网络攻击，进行信息窃取或传播木马、蠕虫等其他有害程序；
e) 混合攻击程序（MA）：是指利用多种方法传播和感染其它系统的有害程序，可以兼有计算机病毒、网络蠕虫、特洛伊木马等多种组合特征。混合攻击程序也可以是一系列不同恶意程序组合运行的结果。例如，一个计算机病毒或网络蠕虫在侵入计算机系统后在系统中安装木马程序；
f) 勒索软件（RAN）：是一种恶意软件，通过感染用户的操作系统，采用加密用户的数据或拒绝用户访问设备等方式，使用户数据资产或计算资源无法正常使用，以此向用户勒索钱财换取解密密钥或恢复对设备的访问，赎金形式包括真实货币或虚拟货币；
g) 恶意代码内嵌网页（MCEWP）：是指因被嵌入恶意代码而受到污损的网页，该恶意代码在访问该网站的计算机系统中安装恶意软件；
h) 恶意代码宿主站点（MCHS）：是指诱使网站存储恶意代码，导致目标用户下载的站点；
i) 其它有害程序（OM）：是指不能包含在以上子类之中的有害程序。

7.2.3 网络攻击事件（NAI）

网络攻击事件是指通过网络或其他技术手段对信息系统攻击（或者利用信息系统配置、协议或程序中的脆弱性，或者强力攻击导致信息系统状态异常或对当前系统运行带来潜在危害）造成系统损失或社会影响的事件。

网络攻击事件包括拒绝服务、高级可持续性威胁、后门利用、漏洞利用、网络扫描窃听、干扰、登录尝试等事件，说明如下：

a) 拒绝服务（DoS）：是指因过度使用信息系统和网络资源（诸如 CPU、内存、磁盘空间或网络带宽）而引起，进而影响信息系统的正常运行，例如，PING 泛滥、电子邮件轰炸；
b) 高级可持续性威胁（APT）：是指某组织对特定对象展开的持续有效的攻击活动导致的网络安全事件，这种攻击活动具有极强的隐蔽性和针对性,通常会运用受感染的各种介质、供应链和社会工程学等多种手段实施先进的、持久的且有效的威胁和攻击；
c) 后门利用（EoB）：是指恶意利用软件和硬件系统设计过程中未经严格验证所留下的接口、功能模块、程序等，获取对程序或系统的访问权限；
d) 漏洞利用（EoV）：是指发掘并利用诸如配置、协议或程序的信息系统缺陷；
e) 网络扫描窃听（NSE）：是指利用网络扫描软件或窃听软件获取有关网络配置、端口、服务和现有脆弱性的信息；
f) 干扰（INF）：是指通过技术手段阻碍计算机网络、有线或无线广播电视传输网络或卫星广播电视信号；
g) 登录尝试（LA）：是指口令猜测、破解或账户信息收集等；
h) 其他网络攻击（ONA）：是指不能被包含在以上子类之中的网络攻击。

7.2.4 数据攻击事件（DAI）

数据攻击事件是指通过网络或其他技术手段，造成信息系统中的数据被篡改、假冒、泄漏、窃取等而造成系统损失或社会影响的事件。

数据攻击事件包括数据篡改、数据假冒、数据泄漏、数据窃取、数据拦截、数据丢失、数据错误、数据勒索等事件，说明如下：

a) 数据篡改（TWD）：是指未经授权接触或修改数据，例如服务请求数据篡改、服务响应数据篡改等；
b) 数据假冒（DC）：是指非法或未经许可使用、伪造系统数据，例如身份数据假冒、网页数据假冒等；
c) 数据泄漏（DLE）：是指通过技术手段或恶意操作使得信息系统中的数据对外透露，例如社会工程、网络钓鱼等；
d) 数据窃取（ToD）：是指未经授权利用技术手段恶意主动获取信息系统中的数据，例如窃听、间谍、位置检测等；
e) 数据拦截（DIN）：是指在数据到达目标接收者之前捕获数据；
f) 数据丢失（DLO）：是指因误操作、人为蓄意或软硬件缺陷等因素导致信息系统中的数据缺失；
g) 数据错误（DE）：是指输入或处理数据时发生错误；
h) 数据勒索（DB）：是指主动瞄准目标，通过劫持信息系统重要数据或个人敏感信息向目标勒索赎金，从而达到敲诈的目的；
i) 其它数据攻击（ODA）：是指不能被包含在以上子类之中的数据攻击。

7.2.5 设备设施故障事件（FFI）

设备设施故障事件是指由于信息系统自身故障或基础设施故障而导致的网络安全事件。

设备设施故障事件包括技术故障、基础设施故障、物理损害、辐射干扰等事件，说明如下：

a) 技术故障（TF）：是指信息系统或相关设备故障以及意外的人为因素导致信息系统故障或毁坏造成的系统损失，例如，硬件故障、软件故障、过载（信息系统容量饱和）、维护性破坏等；

b) 基础设施故障（IF）：是指支撑信息系统运行的基本系统和服务故障造成的系统损失，例如，电源故障、网络故障、空调故障、供水故障等；
c) 物理损害（PHD）：是指故意或意外的物理行动造成的系统损失，例如，火灾、水灾、静电、恶劣环境（诸如污染、灰尘、腐蚀、冻结），设备毁坏、介质毁坏、设备盗窃、介质盗窃、设备丢失、介质丢失、设备篡改、介质篡改等；
d) 辐射干扰（RI）：是指因辐射产生干扰造成的系统损失，例如，电磁辐射、电磁脉冲、电子干扰、电压波动、热辐射等；
e) 其它设备设施故障（OFF）：是指不能被包含在以上子类之中的设备设施故障。

7.2.6 违规操作事件（IOI）

违规操作事件是指人为故意或意外地损害信息系统功能造成系统损失的网络安全事件。

违规操作事件包括权限滥用、权限伪造、行为抵赖、恶意操作、误操作、人员可用性破坏、资源未授权使用、版权违反等事件，说明如下：

a) 权限滥用（AoA）：是指超出范围使用权限；
b) 权限伪造（FoR）：是指为了欺骗制造虚假权限；
c) 行为抵赖（DoA）：是指否认他/她所做的事情；
d) 恶意操作（MO）：是指故意执行非法操作；
e) 误操作（MISO）：是指不正确或无意地执行操作；
f) 人员可用性破坏（BoPA）：是指由人员缺失或缺席而造成；
g) 资源未授权使用（UUoR）：是指为未授权的目的访问资源，包括营利冒险，例如，使用电子邮件参加非法传销的连锁信；
h) 版权违反（BoC）：是指因贩卖或安装未经许可的商业软件或其他受版权保护的材料而引起，例如，盗版软件信息假冒是指通过假冒他人信息系统收发信息而导致的网络安全事件；
i) 其它违规操作（OIO）：是指不能被包含在以上子类之中的违规操作。

7.2.7 不可抗力事件（FMI）

用户访问网络通道安全性措施；网络安全监测系统自身的数据安全性保护措施、网络安全监测系统应用层安全检测措施等。不可抗力事件是指由于某些突发事件造成的网络安全事件。

不可抗力事件包括自然灾害、事故灾难、公共卫生事件、社会安全事件等事件，说明如下：

a) 自然灾害（ND）：例如，水旱灾害、气象灾害、地震灾害、地质灾害、海洋灾害等；
b) 事故灾难（AD）：例如，煤矿事故、火灾事故、特种设备事故、基础设施和公用设施事故、核与辐射事故、能源供应中断事故等；
c) 公共卫生事件（PHI）：例如，传染病、食品药品安全等；
d) 社会安全事件（SSI）：例如，群体性事件、恐怖袭击事件、涉外突发事件、金融安全事件等；
e) 其他不可抗力（OFM）：是指不能被包含在以上子类之中的不可抗力。

7.2.8 其他事件（OI）

其他事件类别是指未分类到上述类别中的网络安全事件。

8 网络安全事件分级

8.1 分级原则

8.1.1 概述

对网络安全事件的分级主要考虑三个要素：信息系统的重要程度、社会影响和系统损失。

8.1.2 信息系统的重要程度

信息系统的重要程度由信息系统所支撑运行的业务重要程度决定。这种重要程度以社会秩序、经济发展和公众利益以及业务对信息系统的依赖程度来表达，划分为特别重要信息系统、重要信息系统和一般信息系统。具体描述如下：

a) 特别重要信息系统，是指受到破坏后，会对社会秩序、经济发展和公共利益造成特别严重损害的信息系统；
b) 重要信息系统，是指受到破坏后，会对社会秩序、经济发展和公共利益造成严重损害，或对相关公民、法人和其他组织的合法权益造成严重或特别严重损害的信息系统；
c) 一般信息系统，是指受到破坏后，不危害社会秩序、经济发展和公共利益，但会对相关公民、法人和其他组织的合法权益造成一般损害的信息系统。

8.1.3 社会影响

社会影响是指网络安全事件对社会所造成影响的范围和程度，其大小主要考虑社会秩序、经济建设和公众利益等方面的影响，划分为特别重大的社会影响、重大的社会影响、较大的社会影响和一般的社会影响，说明如下：

a) 特别重大的社会影响：波及到一个或多个省市的大部分地区，对经济建设有极其恶劣的负面影响，或者严重损害公众利益；
b) 重大的社会影响：波及到一个或多个地市的大部分地区，对经济建设有重大的负面影响，或者损害到公众利益；
c) 较大的社会影响：波及到一个或多个地市的部分地区，可能扰乱社会秩序，对经济建设有一定的负面影响，或者影响到公众利益；
d) 一般的社会影响：波及到一个地市的部分地区，对社会秩序、经济建设和公众利益基本没有影响，但对个别公民、法人或其他组织的利益会造成损害。

8.1.4 系统损失

系统损失的大小主要考虑恢复系统正常运行和消除安全事件负面影响所需付出的代价，划分为特别严重的系统损失、严重的系统损失、较大的系统损失和较小的系统损失，说明如下：

a) 特别严重的系统损失：造成系统大面积瘫痪，使其丧失业务处理能力，或系统重要数据/个人敏感信息的保密性、完整性、可用性遭到严重破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价十分巨大，对于事发组织是不可承受的；
b) 严重的系统损失：造成系统长时间中断或局部瘫痪，使其业务处理能力受到极大影响，或系统重要数据/个人敏感信息的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价巨大，但对于事发组织是可承受的；
c) 较大的系统损失：造成系统中断，明显影响系统效率，使重要信息系统或一般信息系统业务处理能力受到影响，或系统重要数据/个人信息的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价较大；

d) 较小的系统损失：造成系统短暂中断，影响系统效率，使系统业务处理能力受到影响，或系统重要数据/个人信息的保密性、完整性、可用性遭到影响，恢复系统正常运行和消除安全事件负面影响所需付出的代价较小。

8.2 事件分级

见《人力资源社会保障行业网络安全事件应急预案》（人社厅发〔2017〕112号）中1.4。

9 应急处置机构与职责

9.1 应急处置机构

各省人力资源社会保障部门的网络安全和信息化工作领导小组承担本省网络安全事件领导小组的职责。如省级人力资源社会保障部门未设立网络安全和信息化工作领导小组，应成立本省人力资源社会保障部门的网络安全事件领导小组，负责网络安全事件处置组织、协调和领导工作。

网络安全事件领导小组下设网络安全事件工作小组，具体负责网络安全事件处置工作。具体处置机构和职责，参考《人力资源社会保障行业网络安全事件应急预案》。

9.2 职责

网络安全事件领导小组的主要职责包括：

a) 负责网络安全事件的应急指挥、组织协调和过程控制；
b) 负责研究、决定网络安全事件应急处置决策和应对措施；
c) 负责向监管部门和公安机关汇报应急处置进展情况和总结报告；
d) 负责统筹协调，确定相关职能部门应急处理工作职责及具体分工。

网络安全事件工作小组的主要职责包括：

a) 定期向网络安全事件领导小组汇报网络安全事件状况；
b) 在网络安全事件领导小组组织、协调、指导下，开展网络安全事件应急处置工作；
c) 负责对网络安全事件产生的影响和损失进行分析与评估，及时通报评估结果；
d) 组织、指导、监督各部门定期进行应急演练；
e) 网络安全事件领导小组交办的其他工作。

10 安全产品运营要求

对于安全产品要做到集中管理、集中运营，对病毒库、补丁库、规则库、威胁情报库等具备特征库的安全产品，要做到及时更新，更新频率不小于月/次。要做到系统能够对安全或系统日志进行统一的接纳管理，通过预警、监测、响应、阻断、恢复等5个方面对网络进行持续运营。

11 安全事件应急处置流程

安全事件应急处置流程为信息系统管理人员处置网络安全事件提供了一套行为的规范。当紧急事件发生时，信息系统管理员可以及时的确定如何采取措施应对紧急事件，提高对紧急事件的处理效率，从而保证整个系统的持续、正常的运行。涉及“安全事件监测”“启动预案”“应急处置”等内容，具体参考《人力资源社会保障行业网络安全事件应急预案》。

11.1 安全事件监测

11.1.1 监测范围

网络安全事件工作小组和信息系统管理人员对信息系统进行实时监测分析。具体监测范围参考“4.2 监测分类”。

11.1.2 监测方式

由网络安全事件工作小组负责，网络安全事件工作小组和信息系统管理人员对信息系统、网络安全系统、计算系统等进行实时监测分析。能够直观的查看内部资产的安全事件分布情况，将安全事件风险进行可视化展示。对网络日志，安全日志，流量日志进行检测关联分析，通过检测引擎、威胁情报、场景化检测规则、机器学习和关联规则等多维度进行威胁的研判，达到对产生的事件进行快速分析，快速判断正在发生或已经发生的网络入侵攻击行为。将发现的攻击事件进行报告，并及时采取有效阻断措施。同时判断系统及运行情况是否正常，分析应用产生的日志是否有恶意攻击行为。一旦发现异常日志事件，及时报告。

11.1.3 安全事件确认

网络安全事件工作小组和信息系统管理人员对信息系统进行实时监测分析，现满足“7.2事件分类”事件描述情况之一，可根据实际进行快速分析判断是否为网络安全事件，并向网络安全事件领导小组汇报。

11.1.4 确认安全事件等级

网络安全事件工作小组向网络安全事件领导小组进行安全事件上报，同时组织会议，根据“8.2 事件分级”进行定级，确定网络安全事件的等级，根据等级确定随后的处理步骤，并确定此事件的具体处理成员。

11.1.5 问题通报

网络安全事件，以及时上报，及时预警，及时处理为原则，对网络安全事件进行快速响应。网络安全事件领导负责制定问题通报机制，根据通报机制内容判断其事件影响范围，决定网络安全事件是否上报和预警。

11.2 启动预案

网络安全事件，以及时上报，及时预警，及时处理为原则，对网络安全事件进行快速响应。网络安全事件领导小组负责制定应急处置预案，根据应急处置预案内容，进行执行处置。根据网络安全事件的级别，启动相应级别的应急响应，具体内容可参考《人力资源社会保障行业网络安全事件应急预案》中的3.4预警响应和4.2应急响应。

11.3 应急处置

网络安全事件工作小组在应急处置工作中应通过口头、电话或书面方式定时向本单位网络安全事件领导小组汇报应急处置工作进展情况。依据《中华人民共和国网络安全法》规定，如遇安全事件中涉及犯罪情形的，除做好相应的应急处理外，还应保护好案发现场，同时向公安机关和网信部门报案。

a) 有害程序事件：对病毒及破坏性程序蔓延的，由应急响应组织进行处置，可以协调外部组织进行技术协助，分析有害程序，保护现场，必要时切断相关网络连接。应急响应组织先完成有害程序清除方案，并对方案进行验证，保证清除方案对业务无影响。再清除有害程序，恢复受影响网络和信息系统的正常运行；

b) 网络攻击事件：应急响应组织通过入侵检测和安全审计等方法确定攻击方法，采取措施保护现场，阻止攻击行为进一步造成危害。应急响应组织还需对现场进行全面勘查取证，查明网络攻击来源；

c) 数据攻击事件：应急响应组织对被泄露、窃取和丢失的秘密信息进行鉴定，确定信息的密级，确定泄密事件的性质。并对现场进行全面勘查取证，分析判断，查明泄密的渠道，确定窃密对象。应急响应组织需要采取有效措施，阻断泄密渠道；

d) 设备设施故障事件：应急响应组织及时修复设备故障，不能修复的设备，信息系统建设管理责任部门要立即进行更换，保障网络的畅通和重要信息系统的正常运行。应急响应组织及时查明设备设施故障的原因，完善设备部分方案；

e) 违规操作事件：应急响应组织及时违规操作事件造成影响进行判断，对网络和信息系统的受损情况进行调查取证，对违规操作人员进行处理，严重者移交公安机关进行处置；

f) 不可抗力事件：应急响应组织对事件进行内部和外部进行紧急通报，并协调外部组织协助应急响应组织对网络和信息系统的受损情况进行调查，并对灾害性事件进行评估，充分评估涉及部门、业务范围和社会影响。评估后，对发生事件的网络和信息系统应尽快恢复信息系统的正常运行；

g) 其它事件：应急响应组织对各种其它安全事件，特别是跟自身业务、自身系统、设备特殊性相关的安全事件的处理，需要有应急处置专门的措施，比如工业网络安全领域的安全事件，需要有专门的应急处置措施。

11.4 结束响应

网络安全事件经应急处置后，事件得以完全解决，系统完全恢复正常运行；或事态影响下降到可接受范围内，系统主要功能恢复正常运行，按“谁启动、谁结束”的原则，由网络安全事件领导小组组长下达应急结束指令。

11.5 事件调查和报告

网络安全事件工作小组应对事件进行研究分析和调查处理，查明安全事件的性质、原因、经过、危害和影响，提出调查处理建议和今后同类事件的安全防范措施，以防止同类事件再次发生。同时，网络安全事件领导小组提出对具体责任人的处罚决定，如涉及违法行为的，应依据法律、法规，应移交相关部门处理。事件调查完成后，应形成安全事件调查结果报告。事件的调查处理和总结评估工作原则上在应急响应结束后15天内完成。