ICS 35.040
L80

中华人民共和国国家标准

GB/T XXXXX—XXXX

信息安全技术 关键信息基础设施网络安全保护基本要求

Information security technology -Basic requirements for cybersecurity protection of critical information infrastructure

（报批稿）

（本稿完成日期：2019-11-05）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照GB/T 1.1-2009《标准化工作导则 第1部分：标准的结构和编写》给出的规则起草。

本标准由全国信息安全标准化技术委员会（SAC/TC260）提出并归口。

本标准起草单位：北京赛西科技发展有限责任公司、中国电子技术标准化研究院、中国信息安全测评中心、国家信息技术安全研究中心、国家互联网应急中心、公安部信息安全等级保护评估中心、公安部第一研究所、国家工业信息安全发展研究中心、中国信息安全认证中心、中国互联网域名中心等。

本标准主要起草人：杨建军、姚相振、王惠莅、陈亮、宋璟、孙晓丽、周亚超、任卫红、孙军、袁静、张新跃、任泽君等。

引 言

为落实《中华人民共和国网络安全法》关于保护关键信息基础设施运行安全的要求，在国家网络安全等级保护制度基础上，充分借鉴我国相关部门在重要领域开展网络安全审查、网络安全检查等重点工作的成熟经验，充分吸纳国外在关键基础设施安全保护方面的成功举措，结合我国现有信息安全保障体系等成果，从识别认定、安全防护、检测评估、监测预警、事件处置等环节，提出关键信息基础设施网络安全保护基本要求，采取一切必要措施保护关键信息基础设施业务连续运行，及其重要数据不受破坏，切实加强关键信息基础设施安全保护。

信息安全技术 关键信息基础设施网络安全保护基本要求

1 范围

本标准规定了关键信息基础设施识别认定、安全防护、检测评估、监测预警、事件处置等环节的基本要求。

本标准用于关键信息基础设施的规划设计、开发建设、运行维护、退役废弃等阶段的安全保护工作，主要适用于关键信息基础设施运营者，也可供关键信息基础设施安全保护工作部门和关键信息基础设施安全保护的其他参与者参考。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 20984 信息安全技术 信息安全风险评估规范

GB/T 22239-2019 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

GB/T AAAA-AAAAA 信息安全技术 关键信息基础设施安全控制措施

3 术语和定义

GB/T 25069、GB/T 20984 中界定的以及下列术语和定义适用于本文件。

3.1

关键信息基础设施 critical information infrastructure

公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的信息设施。

4 安全保护基本原则

关键信息基础设施的安全保护应遵循重点保护、整体防护、动态风控、协同参与的基本原则，建立网络安全综合防御体系。

重点保护是指关键信息基础设施网络安全保护应首先符合网络安全等级保护政策及GB/T 22239-2019等标准相关要求，在此基础上加强关键信息基础设施关键业务的安全保护。

整体防护是指基于关键信息基础设施承载的业务，对业务所涉及的多个网络和信息系统（含工业控制系统）等进行全面防护。

动态风控是指以风险管理为指导思想，根据关键信息基础设施所面临的安全风险对其安全控制措施进行调整，以及时有效的防范应对安全风险。

协同参与是指关键信息基础设施安全保护所涉及的利益相关方，共同参与关键信息基础设施的安全保护工作。

5 主要环节及活动

本标准所指的关键信息基础设施运营者（以下简称运营者）负责关键信息基础设施的运行、管理，对本组织关键信息基础设施安全负主体责任，履行网络安全保护义务，接受政府和社会监督，承担社会责任。

关键信息基础设施网络安全保护包括识别认定、安全防护、检测评估、监测预警、事件处置五个环节。图1所示为一般情况下的环节之间的关系图，当关键信息基础设施运行时，根据实际情况环节之间的关系有所变动。

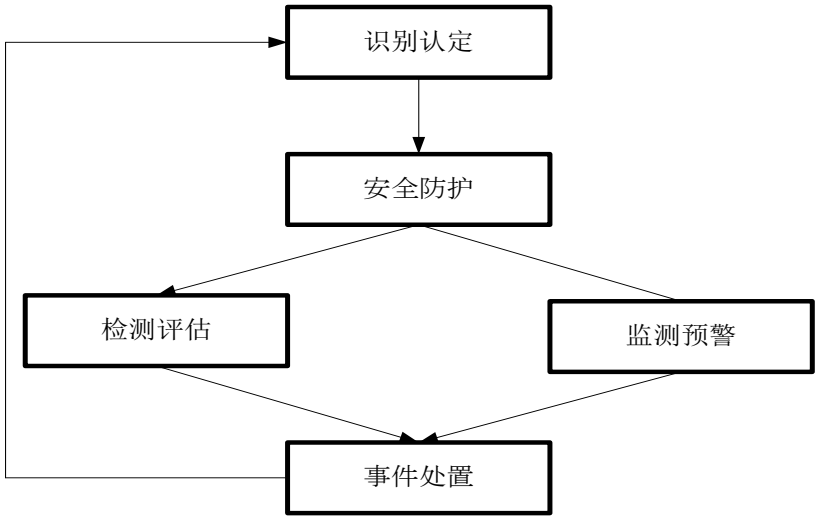

图 1 关键信息基础设施网络安全保护各环节关系图

a）识别认定：运营者配合保护工作部门，按照相关规定开展关键信息基础设施识别和认定活动，围绕关键信息基础设施承载的关键业务，开展业务依赖性识别、风险识别等活动。本环节是开展安全防护、检测评估、监测预警、事件处置等环节工作的基础。

b）安全防护：运营者根据已识别的安全风险，实施安全管理制度、安全管理机构、安全管理人员、安全通信网络、安全计算环境、安全建设管理、安全运维管理等方面的安全控制措施，确保关键信息基础设施的运行安全。本环节在识别关键信息基础设施安全风险的基础上制定安全防护措施。

c）检测评估：为检验安全防护措施的有效性，发现网络安全风险隐患，运营者制定相应的检测评估制度，确定检测评估的流程及内容等要素，并分析潜在安全风险可能引起的安全事件。

d）监测预警：运营者制定并实施网络安全监测预警和信息通报制度，针对即将发生或正在发生的网络安全事件或威胁，提前或及时发出安全警示。

e）事件处置：对网络安全事件进行处置，并根据检测评估、监测预警环节发现的问题，运营者制定并实施适当的应对措施，恢复由于网络安全事件而受损的功能或服务。

本标准对关键信息基础设施运营者提出关键信息基础设施安全保护基本要求。为满足这些要求，运营者需要采用相应安全控制措施，安全控制措施的选择可参考GB/T AAAAA-AAAA。

6 识别认定

6.1 业务识别

运营者应：

a）识别本组织的关键业务和关键业务所依赖的外部业务，识别外部业务对本组织关键业务的重要性。

b）当关键业务为外部业务提供服务时，识别本组织关键业务对外部业务的重要性。

c）梳理关键业务链，明确支撑本组织关键业务的关键信息基础设施分布和运营情况。

6.2 资产识别

运营者应：

a）识别关键业务链所依赖的资产，建立关键业务链相关的网络、系统、服务和其他资产清单。

b）基于资产类别、资产重要性和支撑业务的重要性，对资产进行优先排序，确定资产防护的优先级。

c）实现对关键信息基础设施相关资产的自动化管理，根据关键业务链所依赖资产的实际情况实时动态更新。

6.3 风险识别

运营者应根据关键业务链开展安全风险及其影响分析，识别关键业务链各环节的威胁、脆弱性、已有安全控制措施及主要安全风险点，确定风险处置的优先级，形成安全风险报告。

注：风险分析的方法可参照 GB/T 20984。

6.4 重大变更

运营者应在关键信息基础设施发生改建、扩建、所有人变更等重大变化有可能影响认定结果时，例如网络拓扑改变、业务链改变等，重新开展识别工作，并更新资产清单，及时将相关情况报告保护工作部门，按规定进行重新认定。

7 安全防护

7.1 网络安全等级保护制度

运营者应符合国家网络安全等级保护制度相关要求，对相关信息系统开展定级备案、相应等级的测评、安全建设、整改及自查工作。

7.2 安全管理制度

运营者应：

a）建立适合本组织的网络安全保护计划，结合关键业务流的安全风险报告，明确关键信息基础设施网络安全保护工作的目标、安全策略、组织架构、管理制度、技术措施、实施细则及资源保障等，形成文档并经审批后发布至相关人员。网络安全保护计划应至少每年修订一次，或发生重大变化时进行修订。

注 1：安全策略包括但不限于：安全互联策略、安全审计策略、身份管理策略、入侵防范策略、数据安全防护策略、自动化机制策略（配置、漏洞、补丁、病毒库）、供应链安全管理策略、安全运维策略等。

注 2：管理制度包括但不限于：风险管理制度、网络安全考核及监督问责制度、网络安全教育培训制度、人员管理制度、业务连续性管理及容灾备份制度、三同步制度、供应链安全管理制度等。

b）基于关键业务链、供应链等安全需求建立或完善安全策略和制度，并根据关键信息基础设施面

临的安全风险和威胁的变化相应调整。

7.3 安全管理机构

运营者应：

a）成立指导和管理网络安全工作的委员会或领导小组，由组织主要负责人担任其领导职务，设置专门的网络安全管理机构，建立首席网络安全官制度，建立并实施网络安全考核及监督问责机制。

b）安全管理机构主要人员应参与本组织信息化决策。

c）安全管理机构相关人员应参加国家、行业或业界网络安全相关活动，及时获取网络安全动态，并传达到本组织。

7.4 安全管理人员

运营者应：

a）对安全管理机构的负责人和关键岗位的人员进行安全背景和安全技能审查，符合要求的人员方能上岗，关键岗位包括与关键业务系统直接相关的系统管理、网络管理、安全管理等岗位。关键岗位应专人负责，并配备 2 人以上共同管理。

b）运营者应建立网络安全教育培训制度，定期开展基于岗位的网络安全教育培训和技能考核，应规定适当的关键信息基础设施从业人员和网络安全关键岗位从业人员的年度培训时长，教育培训内容应包括网络安全相关制度和规定、网络安全保护技术、网络安全风险意识等。

c）在上岗前对人员进行安全背景审查，当必要时或人员的身份、安全背景等发生变化时（例如取得非中国国籍）应根据情况重新进行安全背景审查。应在人员发生内部岗位调动时，重新评估调动人员对关键信息基础设施的逻辑和物理访问权限，修改访问权限并通知相关人员或角色。应在人员离岗时，及时终止离岗人员的所有访问权限，收回与身份认证相关的软硬件设备，进行离职面谈并通知相关人员或角色。

d）与从业人员签订安全保密协议，在安全保密协议中，应约定安全职责、奖惩机制，以及当离岗后的脱密期限。

7.5 安全通信网络

7.5.1 互联安全

运营者应：

a） 建立或完善不同等级系统、不同业务系统、不同区域之间的安全互联策略。

b） 保持相同的用户其用户身份、安全标记、访问控制策略等在不同等级系统、不同业务系统、不同区域中的一致性。例如，可以使用统一身份与授权管理系统/平台。

c） 对不同局域网之间远程通信时采取安全防护措施，例如在通信前基于密码技术对通信的双方进行验证或认证。

7.5.2 边界防护

运营者应：

a） 对不同网络安全等级系统、不同业务系统、不同区域之间的互操作、数据交换和信息流向进行严格控制。例如：采取措施限制数据从高网络安全等级系统流向低网络安全等级系统。

b） 应对未授权设备进行动态检测及管控，只允许通过运营者自身授权和安全评估的软硬件运行。

7.5.3 安全审计

运营者应加强网络审计措施，监测、记录系统运行状态、日常操作、故障维护、远程运维等，留存相关日志数据不少于12个月。

7.6 安全计算环境

7.6.1 鉴别与授权

运营者应：

a） 运营者应明确重要业务操作或异常用户操作行为，并形成清单。

b） 对设备、用户、服务或应用、数据进行安全管控，对于重要业务操作或异常用户操作行为，建立动态的身份鉴别方式，或者采用多因子身份鉴别方式等。

c） 针对重要业务数据资源的操作，基于安全标记等技术实现访问控制。

7.6.2 入侵防范

运营者应：

a） 实现对新型网络攻击行为（如 APT 攻击）的入侵防范。

b） 具备系统主动防护能力，及时识别并阻断入侵和病毒行为。

7.6.3 数据安全防护

运营者应：

a） 建立数据安全管理责任和评价考核制度，制定数据安全计划，实施数据安全技术防护，开展数据安全风险评估，制定网络安全事件应急预案，及时处置安全事件，组织数据安全教育、培训。

b） 制定数据安全管理策略，明确数据和个人信息保护的相应措施。

c） 将在我国境内运营中收集和产生的个人信息和重要数据存储在境内，因业务需要，确需向境外提供数据的，应当按照国家相关规定和标准进行安全评估，法律、行政法规另有规定的，依照其规定。对数据的全生命周期进行安全管理，基于数据分类分级实现相应的数据安全保护。

d） 严格控制重要数据的公开、分析、交换、共享和导出等关键环节，并采取加密、脱敏、去标识化等技术手段保护敏感数据安全。

e） 建立业务连续性管理及容灾备份机制，重要系统和数据库实现异地备份。

f） 业务数据安全性要求高的实现数据的异地实时备份。

g） 业务连续性要求高的实现业务的异地实时切换，确保关键信息基础设施一旦被破坏，可及时进行恢复和补救。

7.6.4 自动化工具

运营者应使用自动化工具来支持系统账户、配置、漏洞、补丁、病毒库等的管理。对于漏洞、补丁，应在经过验证后及时修补。

7.7 安全建设管理

7.7.1 网络安全与信息化同步要求

运营者应：

a）在新建或改建、扩建关键信息基础实施设施时，充分考虑网络安全因素，在规划、建设和投入使用阶段保证安全措施的有效性，并采取测试、评审、攻防演练等多种形式验证。必要时，可建设关键业务的仿真验证环境。

b）当关键信息基础设施退役废弃时，按照数据安全管理策略对存储的数据进行处理。

7.7.2 供应链安全保护

运营者应：

a）制定供应链安全管理策略，包括：风险管理策略、供应商选择和管理策略、产品开发采购策略、安全维护策略等。

b）建立供应链安全管理制度，设置相应的供应链安全管理部门，提供用于供应链安全管理的资金、人员和权限等可用资源。

c）保证产品的设计、研发、交付、使用、废弃等各阶段，以及制造设备、工艺等的供应链安全风险基本可控。

d）选择有保障的供应商，防范出现因政治、外交、贸易等非技术因素导致产品和服务供应中断的风险。

e）在能提供相同产品的多个不同供应商中做选择，以防范供应商锁定风险。

f）要求供应商承诺不非法获取用户数据、控制和操纵用户系统和设备，或利用用户对产品的依赖性谋取不正当利益或者迫使用户更新换代。

g）采购、使用的网络关键设备和网络安全专用产品，应通过国家规定的检测认证。

h）采购、使用的网络产品和服务，应符合法律、行政法规的规定和相关国家标准的要求，可能影响国家安全的，应当通过国家安全审查。

i）发现使用的网络产品、服务存在安全缺陷、漏洞等风险时，及时采取措施消除风险隐患，涉及重大风险的应当按规定向保护工作部门报告。

j）采购网络产品和服务时，明确提供者的安全责任和义务，要求提供者做出必要安全承诺，并签订安全保密协议，协议内容应包括安全职责、保密内容、奖惩机制、有效期等。

7.8 安全运维管理

运营者应：

a）保证关键信息基础设施的运维地点位于中国境内，如确需境外运维，应当符合我国相关规定。

b）应要求维护人员签订安全保密协议。

c）确保优先使用已登记备案的运维工具，如确需使用由维护人员带入关键信息基础设施内部的维护工具，应在使用前通过恶意代码检测等测试。

8 检测评估

8.1 检测评估制度

运营者应建立健全关键信息基础设施安全检测评估制度，应包括但不限于检测评估流程、方式方法、周期、人员组织、资金保障等。

8.2 检测评估方式和内容

运营者应：

a）自行或者委托网络安全服务机构对关键信息基础设施安全性和可能存在的风险每年至少进行一次检测评估，并及时整改发现的问题。

b）检测评估内容包括但不限于网络安全制度（国家和行业相关法律法规政策文件及运营者制定的制度）落实情况、组织机构建设情况、人员和经费投入情况、教育培训情况、网络安全等级保护工作落实情况、密码应用安全性评估情况、技术防护情况、云服务安全评估情况、风险评估情况、应急演练情

况、攻防演练情况等，尤其关注关键信息基础设施跨系统、跨区域间的信息流动，及其关键业务流动过程中所经资产的安全防护情况。

c）新建关键信息基础设施，或关键信息基础设施在改建、扩建中发生重大变化时，应自行或者委托网络安全服务机构进行检测评估，评估变更部分所引起的业务信息流的变更，评估是否引入新的风险，并对发现的安全问题进行有效整改后方可上线。

e）在安全风险抽查检测工作，提供网络安全管理制度、网络拓扑图、重要资产清单、关键业务介绍、网络日志等必要的资料和技术支持，针对抽查检测工作中发现的安全问题和风险进行及时整改。

9 监测预警

9.1 监测预警制度

运营者应：

a）制定自身的监测预警和信息通报制度，确定网络安全预警分级标准，明确监测策略、监测内容和预警流程，对关键信息基础设施的网络安全风险进行监测预警。

b）关注国内外及行业关键信息基础设施安全事件、安全漏洞、解决方法和发展趋势，并对涉及到的关键信息基础设施安全性进行研判分析，必要时发出预警。

c）建立关键信息基础设施的预警信息响应处置程序，明确不同级别预警的报告、响应和处置流程。

d）建立通报预警及协作处置机制，建立和维护外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。

e）建立组织机构内部管理人员、内部网络安全管理机构与内部其他部门之间的沟通与合作机制，定期召开协调会议，共同研判、处置网络安全问题。

f）建立网络安全信息共享渠道，例如建立与保护工作部门、研究机构、网络安全服务机构、业界专家之间的沟通与合作机制，共享的信息可以是漏洞信息、威胁信息、最佳实践、前沿技术等。

9.2 监测

运营者应：

a）对关键业务所涉及的信息系统进行监测（例如：对加密通信进行监测，对应用层进行监测，对不同等级系统、不同业务系统、不同区域之间的信息流动进行监测等），对监测获得的信息采取保护措施，防止其受到未授权的访问、修改和删除。

b）分析信息系统通信流量或事态的模式，建立常见系统通信流量或事态的模型，并使用这些模型调整监测设备，以减少误报和漏报。

c）采用自动化机制对关键业务所涉及的信息系统的所有监测信息进行整合分析，以便及时关联、分析关键信息基础设施的网络安全态势。

d）能对将关键业务运行所涉及的各类信息进行关联，并分析整体安全态势。包括：分析不同存储库的审计日志并使之关联；系统内多个组件的审计记录进行关联；将取自审计记录的信息与得自物理访问监控的信息关联；将来自非技术源的信息（例如供应链活动信息、关键岗位人员信息等）与审计信息关联；网络安全信息共享信息关联等。

e）通过安全态势分析结果来确定安全策略和安全控制措施是否合理有效，必要时进行更新。

9.3 预警

运营者应：

a）在发现可能危害关键业务的迹象时，监测机制应能采用自动化的方式及时报警，并自动化地采取对关键业务破坏性最小的行动。例如：恶意代码防御机制、入侵检测设备或者防火墙等弹出对话框、发出声音或者向相关人员发出电子邮件等方式进行报警。

b）对网络安全共享信息和报警信息等进行综合分析、研判，必要时生成内部预警信息。对于可能造成较大影响的，应按照相关部门要求进行通报。内部预警信息的内容应包括：基本情况描述、可能产生的危害及程度、可能影响的用户及范围、建议采取的应对措施等。

c）当内部预警信息发出之后，情况出现新的变化，运营者应向有关人员和组织及时补发最新内部预警信息。

d）能持续获取预警发布机构的安全预警信息，分析、研判相关事件或威胁对自身网络安全保护对象可能造成损害的程度，必要时启动应急预案。获取的安全预警信息应按照规定通报给相关人员和相关部门。

f）采取相关措施对预警进行响应，当安全隐患得以控制或消除时，应执行预警解除流程。

10 事件处置

10.1 事件管理制度

运营者应：

a）具备网络安全事件的处理能力，建立网络安全事件管理制度，明确不同网络安全事件的分类分级、不同类别和级别事件处置的流程等，制定应急预案等网络安全事件管理文档。

b）为网络安全事件处置提供相应资源，指定专门网络安全应急支撑队伍、专家队伍，保障安全事件得到及时有效处置。

c）按规定参与和配合相关部门开展的网络安全应急演练、应急处置等工作。

10.2 应急预案

运营者应：

a) 在国家网络安全事件应急预案的框架下，根据行业和地方的特殊要求，制定本组织的网络安全事件应急预案。应急预案中应明确，一旦信息系统中断、受到损害或者发生故障时，需要维护的关键业务功能，并明确遭受破坏时恢复关键业务和恢复全部业务的时间。应急预案不仅应包括本组织应急事件的处理，也应包括多个组织间的应急事件的处理（适用时）。

b) 在制定应急预案时，同所涉及到的运营者内部相关计划（例如业务持续性计划、灾难备份计划等）以及外部服务提供者的应急计划进行协调，以确保连续性要求得以满足。

c) 在应急预案中包括非常规时期、遭受大规模攻击时等处置流程。

d) 对网络安全应急预案定期进行评估修订，并持续改进。

e) 每年至少组织 1 次跨组织、跨地域的应急演练（适用时）。

10.3 响应和处置

10.3.1 事件报告

运营者应：

a）当发生有可能危害关键业务的安全事件时，应及时向安全管理机构报告，并组织研判，形成事件报告单。

b）及时将可能危害关键业务的安全事件通报到可能受影响的内部部门和人员，并按照规定向关键业务供应链涉及的、与事件相关的其他组织通报安全事件。

10.3.2 事件处理和恢复

运营者应：

a）按照事件处置流程、应急预案进行事件处置，恢复关键业务和信息系统到已知的状态。

b）在事件发生后尽快收集证据，按要求进行信息安全取证分析，并确保所有涉及的响应活动被适当记录，便于日后分析。在进行取证分析时，应与业务连续性计划相协调。

c）在事件处理完成后，应采用手工或者自动化机制形成完整的事件处理报告。事件处理报告包括：不同部门对事件的处理记录、事件的状态和取证相关的其他必要信息、评估事件细节、趋势和处理。

d）在恢复关键业务和信息系统后，应对关键业务和信息系统恢复情况进行评估，查找事件原因，并采取措施防止关键业务和信息系统遭受再次破坏、危害或故障。

e）在进行事件处理活动时，协调组织内部多个部门和外部相关组织，以更好的对事件进行处理，并将事件处理活动的经验教训纳入事件响应规程、培训以及测试，并进行相应变更。

10.3.3 事件通报

运营者应及时将安全事件及其处置情况通报到可能受影响的部门和相关人员，向关键业务供应链涉及的、与事件相关的其他组织提供安全事件信息，并按照规定通报相关部门。

10.4 重新评估

运营者应根据检测评估、监测预警中发现的安全隐患和发生的安全事件，以及处置结果，并结合安全威胁和风险变化情况开展评估，必要时重新开展风险评估，并更新安全策略。

参考文献

[1] 《中华人民共和国网络安全法》 ，2016
[2] 《关键信息基础设施安全保护条例（征求意见稿）》，2017
[3] 《个人信息和重要数据出境安全评估办法（征求意见稿）》，2017
[4] GB/Z 20986-2007 信息安全技术 信息安全事件分类分级指南
[5] GB/T 20988-2007 信息安全技术 信息系统灾难恢复规范
[6] GB/T 22081-2016 信息技术 安全技术 信息安全控制实践指南
[7] GB/T 32921-2016 信息安全技术 信息技术产品供应方行为安全准则
[8] GB/T 32924-2016 信息安全技术 网络安全预警指南
[9] Framework for Improving Critical Infrastructure Cybersecurity
[10] NIST Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations