关键基础设施员工个人安全考虑与行动指南

介绍

在当今的威胁环境中，所有关键基础设施员工都应该保持警惕并承担起个人安全责任，不仅在日常工作中应当如此，生活中也不能懈怠。关键基础设施员工从事大量的服务工作，负责操作、运行和维护现代美国生活所必需的关键系统和资产。注意与您工作相关的任何风险或威胁，并遵守所有安全程序将有助于保护您、您身边的人以及您所服务的基础设施。个人安全可分为三个主要部分：人身安全、态势感知和网络安全。本行动指南并非详尽无遗，但可帮助您评估自己的安全状况，并提供缓解威胁的备选方案。[1]

评估对关键基础设施员工的适当保护水平

本指南概括介绍了如何在家中、工作场所、公共场所和网上保持安全。您可以根据自己的生活方式、安全漏洞和可能遇到的情况来决定哪些措施最适合您，例如，某些因素可能会增加工作场所暴力出现的可能：

- **独自工作**或在偏僻地区工作。
- **提供面对面的服务**或护理。
- **处理危险材料**或涉及国家安全的敏感信息。
- **负责保护**当地或国家关键基础设施。

在评估您的安全需求时，请考虑以下几点：

- **您的职业和专业角色。**您的工作或职业是否会让您成为具有吸引力的目标？
- **具体威胁。**是否有可靠证据表明您面临风险？
- **您的个人经历。**您过去是否遭受过攻击或威胁？
- **您个人具有的视觉标识符。**您是否表现出某种群体身份，该身份会让您成为具有吸引力的目标？

如今，关键基础设施员工可能面临各种威胁，如普通犯罪活动和暴力极端分子阴谋。如果您对上述任何问题或所有问题回答了“是”，这可能表明您以及与您共事的其他关键基础设施员工面临风险，并且您应该评估自己的安全需求。在评估您的个人安全时，关键在于采取一种平衡的方法，并记得把您的家庭和工作生活考虑在内—**在您采取个人安全实践和培养此类习惯时保持警惕，并不断评估您周围的环境。**您应根据感知到的威胁采取适当的措施。安全措施过多可能会给您带来不必要的压力和不便；然而，安全措施不充分可能会将您置于危险之中。

能够识别在哪些情况下容易受到攻击可有效避免此类情况发生或在面临威胁时做好准备。脆弱性是一种物理特征或操作属性，使得实体、资产、系统、网络或地理区域容易被利用或受到特定危害的影响。[2]攻击者将个人作为目标时可谓花样百出。攻击者发起攻击可能是为了制造尴尬、造成不便、干扰他人，也可能是想要对他人造成人身伤害、损害其健康或威胁其生命。

1 ProtectUK. 2022. 公共场所 (PAL) 指南：个人安全.8 月 8 日，2023 年访问. protectuk.police.uk/personal-security.

2 美国国土安全部. 风险指导委员会.2010.DHS 风险词典（2010 年版）.8 月 8 日，2023 年访问.cisa.gov/resources-tools/resources/dhs- risk-lexicon.

人身安全

保护您的家

您可以考虑采取许多简单的措施，以保护您和您的家。首先，您需要在住宅或房产周围安装安全系统或对其加以改进。您可用锁、钥匙、警报器和灯来保护门窗，并评估是否需要安装闭路电视 (CCTV) 系统。您可考虑在入口处和窗户上采用先进的门锁系统，并安装监控（多视角）视频监视系统。

您需要维护房产外的墙壁和栅栏等结构，确保任何可用于进入您家的工具或梯子存放在安全位置。您可考虑移除任何可造成破坏的东西，如松动的砖块、大石头和花园装饰品。您需要修剪和维护灌木和杂草等植物，以确保树叶：

- **不被**入侵者**用来**藏身或进入您家中。
- **不会阻挡**家中人员向外看的视线。

您可使用适当的锁具（包括电子锁和密码锁）保护外部 门窗。
最好多准备一套钥匙或入室密码，以便能在紧急情况下使用。如果密码泄露或钥匙丢失，您应考虑更换整个门锁系统。

您可出资在外部安装照明并加以维护，以照亮外门、停车场和房屋周围的人行道。考虑安装可以看到门窗的摄像头。您应将这些照明灯和摄像头布置在合适的位置，以消除个人可能躲避侦查的盲点。

如果您有车辆，但无法将其停放在车库或上锁的区域，可以尝试将其停放在公共视线可见的范围内。请将车停在光线充足的地方、CCTV 摄像头能看到的地方或有人看管的停车场。即使仅离开几分钟，也一定要关闭车窗，拿走贵重物品并锁好车。了解如何使用车内的防盗报警系统。除了车辆定位服务，还可启用包含声音和视觉通知的系统，以协助警方加快应对的脚步。

提前规划

请考虑制定家庭紧急行动计划，并练习在紧急情况下如何采取行动。如需了解如何制定计划，请访问：

fema.gov/blog/have-emergency-plan-your-family。

枪械袭击

现场行凶枪手是指一个或多个在人口密集区域主动杀人或企图杀人的个人。[3]现场行凶枪手事件往往无法预见，且演变迅速。混乱发生时，任何人都能发挥不可或缺的作用，以减轻现场行凶枪手事件的影响。

由于现场行凶枪手事件通常在 10 到 15 分钟内结束，执法人员来不及赶到现场，因此个人必须做好应对现场行凶枪手事件的身心准备。

发生现场行凶枪手事件时，请考虑根据贵组织的安全政策实施经过实践的应对策略，如“逃跑、躲藏、搏斗”这一应对模式。如需了解更多信息和资源，请访问 CISA 的现场行凶枪手应急准备主页。

利用火发起攻击

纵火是指任何蓄意或恶意焚烧或企图焚烧（无论是否有诈骗意图）住宅、公共建筑、机动车辆、飞机或其他个人财产的行为。[4] 纵火者可能出于报复、破坏、欺诈或掩盖罪行等动机放火。其可能会使用助燃剂和火焰或一种简易燃烧装置 (IID) 来点火。

在发动攻击之前，可能很难察觉到有人试图利用火造成威胁。您需要了解闻到烟味或目睹着火时应采取的措施。

3 联邦调查局，发布时间不详.现场行凶枪手安全资源.12 月 1 日，2023 年访问，fbi.gov/how-we-can-help-you/active-shooter-safety-resources.
4 网络安全和基础设施安全局.2021.行动指南：应对利用火发起的攻击.8 月 8 日，2023 年访问. cisa.gov/resources-tools/resources/fire-weapon-action-guide.

发生火灾时，请拨打 9-1-1，并听从紧急救援人员的指示。立即离开火灾现场，并尽可能提醒其他人。避开能闻到烟味或看到火光的区域。从室内场所撤离；关闭身后的所有房门以控制火势。如果您无法离开火灾现场，应尽量远离危险区域，并根据需要使用灭火器。保持态势感知，留意可疑活动或其他威胁。

请查看 CISA 发布的《行动指南：应对利用火发起的攻击》，学习更多技巧，以便在有人利用火发起攻击时缓解局面。

简易爆炸装置 (IED)

IED 是一种以简易方式放置或制造的装置，内含破坏性、致命、有毒、烟火或燃烧化学物质，旨在造成破坏、使人丧失能力、骚扰或分散他人的注意力。[5] 根据炸弹制造者的目标和可获得的材料，IED 可分为小型、简陋的装置（如通常装有炸药粉的超压装置或管状炸弹）和装有大量爆炸物的大型车载装置。

威胁的形式多种多样。如果您对某种情况或某一可疑物品感到担忧，请立即致电当地执法部门。表明有炸弹存在的示例包括无法解释的电线或电子设备、其他肉眼可见的类似炸弹的部件，以及不寻常的声音、蒸汽、烟雾或气味。涉及可疑装置的简易爆炸装置事件需要防爆小组对其做出响应，并能够判断装置是否存在风险并进行“安全处置”。

如需了解识别可疑物品的详细信息，请参阅《无人看管与可疑物品明信片和海报》并观看视频“怎么处理：可疑或无人看管物品“。

抗议和示威

如果公众抗议或示威活动发生在您家或您的营业场所附近，或甚至就发生在您的房产中，无论其任务和意图如何，请保持冷静。抗议活动看似令人生畏，但造成人身威胁的可能性不大。即使局势变得不稳定，您也要保持冷静。请待在室内，关好并锁好门窗，拉上窗帘/百叶窗。如果您感觉不安全或局势加剧，请致电当地执法部门。

如有必要，请记下对在场人员和车辆的描述。向警方提供任何监控录像、手机视频或照片，因为这可能有助于调查。

CISA 发布的《公众示威期间保护基础设施情况说明书》为可能在公众示威期间成为非法行为目标的企业提供了安全建议。

态势感知

态势感知是指了解周围发生的一切，考虑到所有情况并调整自己的行为，以降低自己、家人或同事受伤的风险。

访客

在让访客进入您家之前，请务必确认其身份。考虑安装猫眼或门上摄像头，以帮助您识别门外人的身份。在开门之前，请不明来历的访客表明身份。访客进入住宅后，始终与其维持近距离，最好让他们待在您面前或其他您能监测的位置。考虑随时携带手机。

敏感材料

始终妥善处理或销毁可能含有敏感或个人身份信息 (PII) 的机密材料。PII 包括可用于识别您身份的任何个人信息。

行人安全

在公共场所活动、行走或慢跑时，请时刻关注个人安全。采取适当的预防措施可以帮助您降低受伤和遭受暴力或侵犯的风险。您可考虑采取一些简单的措施，如提前规划好安全路线，去固定地点时变更路线，避开潜在的危险场所，如安静或光线不足的小巷、荒凉的停车场和偏僻的停车场。

5 美国国土安全部.联邦调查局，发布时间不详. *CISA* 安全和防范指南：反简易爆炸装置 *(C-IED)* 概念、共同目标及可用援助。8 月 8 日，2023 年访问.第 4 页. cisa.gov/resources-tools/resources/security-and-resiliency-guide-srg-and-annexes.

无论您何时身处公共场合，都要谨慎行事，并采取预防措施隐藏任何工作凭证或个人信息。在公共场所佩戴工牌或输入密码时要小心谨慎。如需了解更多信息和技巧，请访问美国国家公路交通安全管理局的行人安全网站。

保持态势感知

如果您在公共场所/环境中感到担忧或感觉不安全，请靠近人群。如果无法完成这一点，请调整您的动作，最大限度地提高您的态势感知，**并采取以下预防措施：**

请将手机放置在可拨打紧急电话的位置。

保持警惕，随时了解自己的确切位置和周围环境。

避免展示任何珠宝或贵重物品。

考虑该区域的照明、位置以及与当地其他企业的**距离**。

行走时应面对来往车辆，以避开从后方驶来的车辆。

保持双手空闲，时刻注意周围环境。

避免打电话、戴耳机或发送长短信。

行走时保持警惕，请勿逗留。

使用银行 ATM 机时，请避免在公众视线范围内展示货币。

拼车服务

使用拼车应用程序时，请考虑向朋友或同事发送您的位置和目的地等详细信息。
在接受拼车和进入车辆之前，请检查司机和车辆的详细信息。

识别并报告可疑活动

识别并报告可疑活动，例如有人在您家、您的工作场所或车辆周围无故闲逛，或有人试图以隐蔽的方式为您拍照。如果您发现有人在您家、您的工作场所或车辆附近丢弃物品或包裹，请立即报警。如需了解报告可疑活动的更多信息，请访问“发现可疑，立即举报 (If You See Something, Say Something®)”运动。

个人保护装置

请考虑携带胡椒喷雾、声音警报器或其他个人保护装置，以干扰攻击者、通知旁观者并为自己创造逃跑的机会。请在条件允许的情况下根据联邦和当地的法律法规，携带并使用个人保护装置。

仔细留意并及时报告以下警示信号有助于缓解潜在事件：

- 针对您、您家、您的财产或工作场所的**口头或书面威胁**。
- 系统和设备**损坏或被篡改**。
- **可疑或无人看管的物品，**包括可能装有危险物质的包、箱、隐藏式容器。
- 对建筑平面图、出入口位置、电梯、灭火器、供水以及供暖、通风和空调 (HVAC) 系统发出的**可疑询问**。
- **易燃或可燃材料数量或位置异常，**包括助燃剂、油漆、脱脂剂、酒精清洁剂、气雾剂和丙烷气罐。
- **在社交媒体上传播**任何实施攻击的图像或想法。

请查看可疑活动报告指标和示例，了解更多信息。

冲突

发现自己身处冲突之中可能会让人感到紧张。应重点关注可观察到的、可表明存在潜在暴力的行为。在这种情况下，关键在于保持冷静并评估局势，以确定自己能否安全地参与其中。考虑自己的能力极限，在安全的情况下尽快寻求安保人员或执法人员的协助。

如果您接受过培训并熟练掌握相关技能，可以考虑采取目的明确的行动（包括有效的倾听和沟通），安全地缓和激烈的局势。请记住，“缓和”并非指您的行为，而是您的目标。

请查看 CISA 缓和系列内容，学习保持警惕和应对潜在敌对环境的技巧。

机动车辆和旅行

离开家或工作场所之前，请环顾四周，注意任何可能在此潜伏或游荡的可疑车辆。检查车辆周围是否有任何不应出现在车辆上或附近的东西。如果确实发生了不利情况，这些信息可能会对警方有所帮助。

如果可能，避免在旅行行程中出现重复的安排，这样潜在的恶意行为者就无法预测您的行踪。尽可能改变路线和出发时间。确保在旅途中锁好所有车门和后备箱。仅打开通风所需的窗户。安全驾驶，与前方车辆保持安全距离。此外，始终确保您的车辆有足够的燃料（如果是电动车，则有足够的电量）供您完成旅程。

如果您认为自己被跟踪，请尽量保持冷静并保持车辆正常行驶。关闭所有车窗并确保车门已上锁。立即联系执法部门。如果可以，请前往最近的警察局，切勿开车回家。尽量记下任何可疑车辆的车牌号、品牌和型号。

如果您的车辆发生碰撞或出现机械故障，请考虑周围环境并立即联系紧急救援人员和拖车服务。听从执法人员的指示。

匿名电话和威胁[6]

匿名电话和威胁通常旨在制造恐惧、惊慌和不安。切记做到以下几点：

- **保持冷静，**不要挂断电话。
- **尽可能让来电者保持通话**。礼貌对待并表现出兴趣，让对方继续说话。对方可能会透露有助于警方调查的重要信息。
- 如果可能，向周围的其他人**发出信号或传递纸条**，让他们听到并帮忙通知政府部门。
- 尽可能多地**记下**信息，如来电号码、威胁的确切措辞、声音或行为类型等，以便为调查人员提供帮助。
- 如果可能且法律允许，**对通话进行录音。**

通过电话进行威胁或辱骂的行为违反了联邦法律。如果您接到此类电话，请联系当地执法部门。此外，您还可以向 FBI 报告这一威胁。请查看《FBI 威胁和恐吓应对指南》，了解相关技巧。

由于大多数炸弹威胁都是通过电话发出的，请参阅《DHS 炸弹威胁清单》和《CISA 炸弹威胁应对指南》，这两份文件说明了如何应对炸弹威胁，以及有助于执法部门调查炸弹威胁的综合信息清单。

网络安全

请只从信誉良好的“应用程序商店”安装应用程序，以避免潜在的有害下载。请勿从未知或无法验证来源处下载应用程序。注意各应用程序访问手机上其他信息的权限

为每台设备或每个账户创建一个唯一的高强度密码并加以维护，同时使用密码管理器来管理密码。在每个提供多因素身份验证 (MFA) 的账户或应用程序上启用该功能。启用 MFA 有助于保护您的个人信息，如电子邮件、社交媒体、财务和其他重要信息。

软件更新

及时更新软件，让攻击者无法利用敏感信息或漏洞。许多操作系统都提供自动更新功能。如果可以选择自动更新，请在设备的应用程序安全设置中打开自动更新。

在您的网络浏览器中，查找以“https”开头，而非“http”的统一资源定位器 (URL)，“https”表示网站使用了加密技术。超文本传输安全协议 (HTTPS) 是一种互联网通信协议，用于在用户的网络浏览器和所连接的网站之间安全地传输加密信息。其旨在更好地保护用户访问网站时信息的完整性和保密性。[7]

请查看 CISA“保护我们的世界”页面，了解更多有关安全上网的信息。

6 联邦调查局.发布时间不详.威胁和恐吓应对指南.8 月 8 日，2023 年访问. fbi.gov/file-repository/threat-intimidation-guide-english-022322.pdf/view.

7 美国国土安全部.2018.超文本传输安全协议 (HTTPS).2 月 12 日，2024 年访问. cisa.gov/resources-tools/resources/hyper-text-transfer- protocol-secure-https.

正确使用电子设备

移动设备和网络可以保存各种个人资料，如网上银行信息、电子邮件、短信、联系人、社交媒体和图片。为保证设备安全，请启用所有安全功能，并确保持续更新设备软件。为手机和 SIM 卡创建高强度密码，并禁用不必要的定位服务。[8]

持续更改访问语音邮件的默认 PIN 码。考虑限制手机中的定位服务并查看隐私设置，以防止他人通过第三方应用程序跟踪您的行踪并找出您的家庭住址或工作地点。查看苹果和安卓的隐私和安全保护措施，以提高您设备的安全性。

社交媒体

互联网可提供宝贵的信息、教育和娱乐资源。但是，您需要保持警惕并采取预防措施，对您在网上（尤其是在社交媒体上）发布的个人信息加以控制。

流行的社交媒体网站允许个人创建个人资料并与他人在线互动。在商业社交网站上，人们可以在个人资料中添加更多细节，包括工作经历和其他背景信息。虽然这些工具可以帮助您与他人交流并宣传您的专业背景，但在网上发布个人信息也存在潜在风险。

发布个人信息时要多加小心。恶意行为者可以利用照片中的位置数据、生日、全名、家庭住址和电子邮件详细信息进行黑客攻击或身份盗窃。此外，对犯罪分子和敌对分子而言，有关就业、家庭成员、爱好或车辆详情的信息也很有价值。如果您的家人和朋友未采取适当措施保护自己的个人资料信息，他们也可能在无意中分享您的信息。请记住，互联网没有“删除”按钮。在网上分享信息时请谨慎，因为即便您删除了个人资料中的帖子或图片，他人仍有可能看到。

有些社交网站拥有您发布的任何数据，并会将您的详细信息出售给第三方。请定期查看您在这类网站上的隐私和位置标签设置，不然可能会有大量素不相识的用户看到您的部分或全部个人资料。[9, 10]

8 联邦通信委员会.2019.保护您的智能设备.9 月 20 日，2023 年访问. fcc.gov/consumers/guides/protect-your-mobile-device.

9 英国政府.国家网络安全中心.2019.如何安全使用社交媒体.9 月 20 日，2023 年访问. ncsc.gov.uk/guidance/social- media-how-to-use-it-safely.

10 网络安全和基础设施安全局，国家网络安全联盟 (National Cyber Alliance). 2019. 社交媒体网络安全.9 月 20 日,2023 年访问.cisa.gov/sites/default/files/ publications/ NCSAM_SocialMediaCybersecurity_2020.pdf.

查看社交媒体的隐私和位置设置

X（前身为 Twitter）

- twitter.com/settings/privacy_and_safety
- twitter.com/settings/location_information

Instagram

- help.instagram.com/811572406418223
- **IOS:** help.instagram.com/171821142968851
- **安卓：**在安卓设备上，打开设置>应用程序>Instagram>权限>位置

Facebook

- facebook.com/help/325807937506242/
- facebook.com/help/337244676357509

Snapchat

- help.snapchat.com/hc/en-gb/sections/5690164367636-Priva- cy-Settings
- help.snapchat.com/hc/en-us/articles/7012322854932-How-do-I- turn-on-Ghost-Mode

TikTok

- tiktok.com/safety/en/privacy-and-security-on-tiktok/
- support.tiktok.com/en/account-and-privacy/account-privacy-set- tings/location-services-on-tiktok

人肉搜索

人肉搜索指的是从公开来源或被泄露的资料中收集个人身份信息 (PII) 或组织敏感信息，并将其公开发布或用于恶意目的的行为。[11, 12] 犯罪分子可以利用这些信息进行勒索和让潜在目标感觉到恐惧。

在网上发布信息时，请务必注意发布的内容和方式。如果您发布的信息过多而又没有进行适当的隐私设置，您可能会将自己的人身安全置于危险之中。他人可以利用这类信息来了解您的人际关系、观点、感兴趣的领域和其他主题，以便在将来加以利用。

数据经纪商也会收集这类个人信息，并将其卖给其他公司。为了尽量减少您落入经纪商之手的数据，可采取以下措施：

- **避免**共享 PII。
- **请勿**在社交媒体上接受现实生活中不认识的人的好友请求。
- **确保**您使用的应用程序具有端到端加密功能。
- **限制**应用程序权限。
- 为您的姓名**设置** Google 快讯。
- **考虑花点时间**退出主要数据经纪商和人员搜索网站的数据共享，或者订阅一项服务来帮您退出。

社交网络平台允许用户发布基于位置的信息，支持 GPS 的手机和移动设备发布此类信息尤其方便。发布这类信息并不安全，任何人都能看到该信息，包括可能想伤害您的人。请监测您发布的信息，并负责任地发布信息，从而确保不会有人因您公开的信息而面临风险。

如果您认为自己遭遇了人肉搜索，可采取以下措施：

- 向当地执法部门和任何可能泄露您个人信息的网络平台**报告此事**。
- **记录下**所发生的一切并截屏与调查人员分享。
- **确定**哪些信息遭到利用、威胁的严重程度和漏洞所在之处。
- **与网站管理员合作，**删除网站或应用程序中的信息。
- **在隐私设置**中选择私密度最高的选项。
- **注意身份盗窃的迹象**，监测金融账户，设置欺诈警报，更改所有在线账户的登录和密码信息。

针对人肉搜索的法律因辖区而异，因此在考虑预防和缓解方案时，一定要查阅所在地区的相关法律。如果担心自身人身安全，请联系当地执法部门了解下一步措施。

识别并报告网络钓鱼

犯罪分子经常使用网络钓鱼策略让您打开有害链接、电子邮件或附件，这些链接、电子邮件或附件可能会要求您提供个人信息或感染您的设备。不法分子精心谋划这类信息，让其看似来自可信的个人或组织。

网络钓鱼信息可能会以电子邮件、短信、社交媒体上的直接消息或电话的形式出现。警惕紧急或情绪化的语言、让您发送个人信息的请求、不可信的缩短 URL 以及不正确的电子邮件地址和链接。

如果您怀疑自己成为了网络钓鱼的目标，请勿点击任何链接或附件。您应进行报告，并删除该邮件。

11 国土安全部. 2024.合作与参与办公室.为个人提供的有关人肉搜索威胁的资料.2 月 9 日，2024 年访问. dhs.gov/ publication/resources-individuals-threat-doxing.
12 欧洲核子研究中心. 2017.计算机安全：进入下一阶段：勒索软件.12 月 12 日，2023 年访问. home.cern/news/news/computing/computer- security-enter-next-level-doxware.

资源

人身安全

- CISA Security and Resiliency Guide（CISA 安全和防范指南）
- CISA Active Shooter Preparedness（CISA 现场行凶枪手应急准备）
- FBI Threat Intimidation Guide（FBI 威胁和恐吓应对指南）
- CISA Bomb Threats（CISA 炸弹威胁）
- CISA De-escalation Series（CISA 缓和系列）

态势感知

- Stalking Prevention, Awareness, & Resource Center（反跟踪、意识和资源中心，SPARC）

网络安全

- CISA Secure Our World（CISA 保护我们的世界）
- CISA Privacy and Mobile Device Apps（CISA 隐私和移动设备应用程序）
- CISA Insights: Mitigating the Impacts of Doxing on Critical Infrastructure（CISA 洞察：减轻人肉搜索对关键基础设施的影响）
- CISA Social Media Cybersecurity（CISA 社交媒体网络安全）