個人安全考量行動指南：關鍵基礎設施員工

簡介

在當今的威脅環境中，保持警惕並為個人安全負責對於工作中或工作外的所有關鍵基礎設施工作人員都至關重要。關鍵基礎設施員工執行廣泛服務，運轉及維護現代美國生活所需的關鍵系統及資產。注意與您工作領域相關的任何風險或威脅，遵循所有安全程序，這將有助保護您、您附近的人及您服務的基礎設施。個人安全可分為三個主要部分：人身安全、狀態意識及網路安全。此非詳盡的行動指南可協助您評估安全狀態，提供可考慮的選項以減輕威脅。[1]

評估關鍵基礎設施員工的適當保護等級

本指南全面概述如何在家中、工作、民眾及線上保持安全。您可以決定哪些措施最適合您的生活方式、安全漏洞及您可能遇到的情況，例如，某些因素可能會增加工作場所暴力的可能性：

- **單獨工作**或在孤立地區工作。
- **提供面對面服務**或照護。
- **處理危險物質**或國家安全敏感資訊。
- 地方或國家關鍵基礎設施**保護責任**。

當評估您的安全需求時，請考慮下列事項：

- **您的職業及專業角色。**您的工作或職業是否使您成為關注目標？
- **特定威脅。**是否有可靠的證據代表您有風險？
- **您的個人歷史。**您過去是否被目標或受到威脅？
- **您的個人視覺識別碼。** 您是否顯示任何團體關係使您成為關注目標？

如今，關鍵基礎設施員工可能面臨各種威脅，包括常見的犯罪活動到暴力極端主義陰謀。如果您對上述任何或全部問題回答是，這可能代表您及您與您合作的其他潛在關鍵基礎設施員工處於風險，您應該評估您的安全性需求。當您評估個人安全時，採取均衡的方法，並記得考慮您的家庭及工作生活是非常重要的 – 在個人安全措施及習慣**保持警覺，並持續評估周圍環境。** 您採取的措施應適合感知的威脅。過度的安全行動可能會導致不必要的壓力及不便；然而，努力不足可能會使您面臨風險。

識別弱點的能力對於加以避免或在發生時做好準備極為重要。漏洞是實體特徵或作業屬性，使實體、資產、系統、網路或地理區域開放，或容易遭受特定危險。[2]攻擊者在瞄準個人時可以發揮創意。攻擊者的目標可能是造成羞辱、不便、困擾，或者他們可能打算造成身體傷害、破壞健康或威脅人類生命。

1 ProtectUK。2022 年。公共場所 (PAL) 指南：個人安全。2023 年 8 月 8 日摘錄。protectuk.police.uk/personal-security。

2 美國國土安全部。風險指導委員會。2010 年。DHS 風險詞彙表 2010 年版。2023 年 8 月 8 日摘錄。cisa.gov/resources-tools/resources/dhs- risk-lexicon。

人身安全

保護您的家園

有多種簡單措施需要考慮，來幫助保護您及您的家。從安裝或改進您住宅或財產周圍的安全系統開始。使用鎖、鑰匙、警報器、燈光固定任何門或窗戶，並評估閉路電視 (CCTV) 系統的要求。考慮使用有畫面（多視圖功能）影像監控系統的先進門窗上鎖系統。

維護牆壁及圍欄等戶外建築結構，並確保可用於進入您家的任何工具或梯子都可以安全存放。考慮移除任何可能造成損壞的東西，例如鬆散的磚塊、大石頭及花園裝飾品。確保灌木、雜草等被修剪及維護，以便葉子：

- **不能使**入侵者隱藏或進入房屋。
- **不會阻擋**住宅內部的外部視野。

使用適當的鎖定裝置確保外門窗安全，其中可包括電子及程式鎖機制。最好在緊急情況保存一組額外鑰匙或輸入代碼。如果輸入代碼遭到破壞或鑰匙遺失，請考慮更改整個上鎖系統。

投資並保持外部照明，照亮房屋周圍的外門、停車區及行人道。考慮安裝帶有門窗視圖的攝影機。策略性放置這些燈光及攝影機，消除人們可逃避偵測的任何盲點。

如果您擁有車輛，但無法將其停在車庫或上鎖區域，請嘗試將其放在民眾視野。停在光線充足的區域，在 CCTV 視野或有人的停車場。即使您只是離開幾分鐘，始終關閉任何窗戶，將貴重物品從視野移除並鎖上您的汽車。了解如何利用車內防盜警報系統的類型。除了車輛定位服務之外，還有系統包括聲音及視覺通知，以幫助加快警察做出反應。

提前規劃

考慮制定家庭緊急行動計畫，練習在緊急情況該做什麼。如需協助制定計畫，請造訪：

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

槍械攻擊

主動槍手定義為或多人積極參與在人口稠密區殺死或試圖殺死人們的個人。[3]主動槍擊事件通常是不可預測，並且發展迅速。任何人都可在混亂減輕主動槍擊事件的影響並發揮不可或缺的作用。

由於主動槍擊情況通常在執法人員到達現場之前的 10 到 15 分鐘內結束，個人必須在精神及身體做好準備，應對主動槍擊事件。

如果發生攻擊槍擊事件，請考慮根據組織的安全性原則來實施實務反應策略，例如「逃跑」、「隱藏」、「對抗」模式。其他資訊及資源請查找 CISA 現場行兇槍手備戰首頁。

火焰武器

燃燒係指任何故意或惡意燃燒或試圖燒毀（有或沒有欺詐意圖）的住宅、公共建築物、汽車、飛機或其他個人財產。[4]縱火者的動機可能包括復仇、破壞、欺詐或隱藏犯罪等。可以促燃劑及火焰或一類即興燃燒裝置 (IID) 來啟動火焰。

在攻擊進行之前，火焰作為武器的威脅可能很難偵測。如果您聞到煙霧或看到著火，您需要了解採取的步驟。

3 聯邦調查局，未標示日期。現場行兇槍安全資源。2023 年 12 月 1 日摘錄，fbi.gov/how-we-can-help-you/active-shooter-safety-resources。

4 網路安全暨基礎設施安全局。2021 年。火焰武器行動指南。2023 年 8 月 8 日摘錄。 cisa.gov/resources-tools/resources/fire-weapon-action-guide。

如果發生火災，請致電 9-1-1 並按照緊急人員的指示。立即離開著火區域，如果可能的話，警告其他人。避開可以聞到煙霧或看到火焰的區域。疏散室內場所；關閉後面的所有門以抑制火災。如果您無法疏散，請盡可能遠離危險，並根據需要使用滅火器。保持狀態意識，並注意可疑活動或其他威脅。

請參閱 CISA 的 火焰武器行動指南 了解更多有關緩解使用火焰作為武器時的提示。

簡易爆炸裝置 (IED)

IED 是以臨時方式放置或製造的裝置，其中含有破壞性、致命、有害性、煙火或燃燒化學品，意在破壞、使其使用能力、騷擾或分散注意力。[5]根據炸彈製造商可用的目標及材料，IED 包括小型、粗糙的裝置，例如過壓裝置或通常裝滿爆炸粉末的管式炸彈，到包含大量爆炸物的大型車載裝置。

威脅可以採取不同的形式。如果您擔心某種情況或可疑物品，請立即致電地方執法機關。指出炸彈的例子包括無法解釋的電線或電子產品，其他可見的類似炸彈的組件，以及不尋常的聲音，蒸汽，霧或氣味。涉及可疑裝置的簡易爆炸裝置事件，需要拆彈小組回應，以及診斷並「呈現安全」可行的裝置。

如需識別可疑物品的詳細資訊，請參閱 無人看管及及可疑物品明信片和海報 並觀看影片「應做事項：可疑或無人看管的物品。」

抗議及示威

無論任何目的或意圖，如果您的家、營業地點甚至您的財產附近發生民眾抗議或示威，請保持冷靜。抗議可能看起來令人恐懼，但不太可能導致人身威脅。即使情況變得緊張，也要保持冷靜。留在室內，關閉並鎖上門窗，並拉上窗簾/百葉窗。如果您感到不安全或情況惡化，請致電地方執法機關。

如有必要，請注意附近個人及車輛的說明。向警方提供任何影像監控影像、手機影像或照片，因為這可能在進行調查時有所幫助。

CISA 在 公共示威期間保護基礎設施情況說明書 為民眾示威期間可能成為違法行為目標的企業提供安全建議。

狀態意識

狀態意識是了解周圍發生的事情，考慮一切並調整您的行為，以降低您、您的家人或同事受傷的風險。

訪客

在讓訪客進入您家之前，始終確定訪客。考慮安裝窺視孔或門攝影機，以幫助您識別門另一側的人。在開門之前，請未知的訪客識別自己。一旦進入您的住宅，請將它們放在附近，最好在您面前或在可以視訊監控的位置。考慮隨時攜帶手機。

敏感材料

請務必妥善處理或銷毀可能含有敏感或個人身份識別資訊 (PII) 的機密資料。PII 包括任何個人性質的資訊，可能用於識別您的身份。

行人安全

在公共空間旅行，步行或慢跑時，優先考慮您的個人安全。採取適當的預防措施可以幫助您減少弱點及遭受暴力或侵略的風險。考慮簡單措施，例如提前規劃安全路線，在往常規地點時改變路線，以及避免潛在危險點，例如安靜或光線不足的小巷、荒涼的停車庫及偏遠的停車場。

5 美國國土安全部。美國聯邦調查局。未標示日期。*安全與彈性指南：反簡易爆炸裝置 (C-IED) 概念、共同目標和可用援助*。2023 年 8 月 8 日摘錄。第 4 頁。cisa.gov/resources-tools/resources/security-and-resiliency-guide-srg-and-annexes。

每當您在民眾場所時，請謹慎行動並採取預防措施隱藏任何工作證明或個人資訊。在公共空間佩戴徽章或輸入密碼時要小心。有關更多事實及提示，請造訪國家公路交通安全管理局網站的 行人安全。

維持情況意識

如果您在公共區域／環境感到擔心或開始感到不安全，請靠近人群。如果不可能，請調整您的動作以最大化您的狀態意識，並**採取以下預防措施：**

- **將您的手機**保持在可以撥打緊急電話的位置。
- **保持警覺，**並隨時了解您的確切位置及周圍環境。
- **避免展示**任何珠寶或貴重物品。
- **考慮區域照明，位置及與**其他地方企業**的鄰近性。**
- **步行時面對接近的交通，**避免車輛從後方接近。
- **保持雙手放鬆，**並保持注意周圍環境。
- **避免在電話上說話，**戴著耳機或傳送長文。
- **步行時**保持警覺，避免時間過長。
- **使用銀行 ATM 時，**請勿在公眾視野中露出錢財。

共享乘車服務

使用共享乘車應用程式時，請考慮通知朋友或同事您的位置及目的地的詳細資訊。
接受乘車並進入車輛之前，請檢查司機及車輛的詳細資訊。

識別並通報可疑活動

識別並通報可疑活動-例如在您家中、工作場所或車輛周圍而沒有特定原因流行的人，或者試圖以秘密方式對您拍照的人。如果您發現有人在您的家、工作場所或車輛附近丟棄物品或包裹，請立即向警方通報。了解有關通報可疑活動的更多資訊，請造訪「If You See Something, Say Something®」宣傳活動。

個人防護裝置

考慮攜帶胡椒噴霧、有聲響警報器或額外個人防護裝置，以使攻擊者失去方向、通知旁觀者並為自己提供逃脫機會。在可能的情況，根據聯邦及地方法律法規，攜帶及使用個人防護裝置。

仔細關注並及時通報以下警告標誌，有助減輕潛在事件：

- 對您、您的居家、財產或工作地點的**口頭或書面威脅。**
- 系統及設備**受損或遭破壞。**
- **可能含有危險物質的可疑或無人看管物品，**包括袋子、盒子、隱藏容器。
- 對建築物平面圖、出入口位置、電梯、滅火器、供水以及暖氣、通風及空調 (HVAC) 系統的**質疑。**
- **易燃或易燃材料的異常數量或位置，**包括加速劑、油漆、脫脂劑、酒精清潔劑、噴霧劑及丙烷氣**體罐。**
- 推廣任何攻擊性圖像或想法的**社群媒體訊息。**

如需詳細資訊，請參閱可疑活動通報指標及範例。

防禦

發現自己處於面對的情況可能會帶來壓力。注意力應專注於可觀察的行為，這些行為可能代表潛在暴力。在這些情況，保持冷靜並評估情況，以確定參與是否安全很重要。考慮自己的能力限制，並在安全的情況盡快尋求保全人員或執法機關的協助。

如果您經過訓練且熟練，請考慮包括的聆聽及溝通的有目的行動來安全降低緊張的情勢。請記住「緩解衝突」不是您該做的事情；而是目標。

請造訪 CISA 緩解衝突系列，了解保持警覺及處理潛在惡劣情況的提示。

機動車輛及旅行

離開您的家或工作場所之前，請四周看看並記住任何可能潛伏或徘迴的可疑車輛。檢查車輛周圍的區域是否有不應該在車上或附近的任何東西。如果確實發生情況，這些資訊可能對警方有所幫助。

如果可能，請避免重複的旅行安排模式，以便潛在惡意人士無法預測您的所在位置。盡可能更改航線並更改出發時間。確保所有車門及行李箱在旅途保持鎖定。僅打開窗戶使足夠通風。安全駕駛並與前車保持安全距離。此外，請務必確保您的車輛有足夠的燃油（或如果是電動，則充足的電量），以適合您的旅程。

如果您認為自己被追蹤，請盡量保持冷靜並保持車輛移動。關閉所有窗戶並確保您的車門已鎖上。立即聯絡執法機關。如果可以，請前往最近的警察局，不要開車回家。請注意任何可疑車輛的車牌號、品牌及型號。

如果您涉及車輛碰撞或遇到機械故障，請考慮周圍環境，並立即聯絡緊急服務人員及拖車服務。遵循執法機關的指示。

匿名電話及威脅[6]

匿名電話及威脅通常意在引起恐懼、警覺及緊張。請務必採取下列步驟：

- **保持冷靜，**不要掛電話。
- **盡可能讓來電者**長時間保持在線上。要有禮貌並表達興趣，讓他們保持說話。他們可能會洩露重要資訊，這些資訊可在警方進行調查時有幫助。
- 如果可能，**請發出信號或傳遞**給周圍其他人，以聆聽並協助通知主管機關。
- 盡可能**記下**資訊（呼叫者 ID 號碼、威脅的確切語言、語音或行為類型等），這將為調查人員提供幫助。
- 如果可能且法律允許，**錄下通話**。

威脅性或濫用電話違反聯邦法律。如果您收到這樣的電話，請聯絡地方執法機關。此外，您可以向聯邦調查局通報威脅。請查看 FBI 威脅恐嚇指南 提示。

由於大多數炸彈威脅都是電話發出，請參閱DHS 炸彈威脅清單 及 CISA 炸彈威脅指南，其中提供有關如何應對炸彈威脅的說明，以及有助執法機關進行炸彈威脅調查的全面資訊清單。

網路安全

僅從信譽良好的「應用程式商店」安裝應用程式，避免潛在的有害下載。請勿從未知或無法驗證來源下載應用程式。請注意應用程式存取手機其他資訊的權限。

建立並維護每個裝置或帳戶專屬的強大密碼，並使用密碼管理器加以整理。為每個帳戶或應用程式開啟多因素身份驗證 (MFA)。啟用 MFA 有助保護個人資訊，例如您的電子郵件、社群媒體、財務及其他重要資訊。

在您的網頁瀏覽器，尋找以「https」而不是「http」開頭的統一資源定位器 (URL)，表示網站使用加密。超文字安全傳輸通訊協定 (HTTPS) 係網際網路通訊協定，用於在使用者網路瀏覽器及其連線網站之間加密及安全傳輸資訊。意在更加保護使用者存取網站時的資訊完整性及機密性。[7]

查看 CISA 保護我們的世界 了解有關保持線上安全的更多資訊。

軟體更新

讓軟體保持最新狀態，以免攻擊者利用敏感資訊或弱點。許多作業系統提供自動更新。如果這是選項，請在裝置的應用程式安全設定開啟自動更新。

6 美國聯邦調查局。未標示日期。威脅恐嚇指南。2023 年 8 月 8 日摘錄。fbi.gov/file-repository/threat-intimidation-guide-english-022322.pdf/view。

7 美國國土安全部。2018 年。超文本傳輸協定安全 (HTTPS)。2024 年 2 月 12 日摘錄。cisa.gov/resources-tools/resources/hyper-text-transfer- protocol-secure-https。

電子裝置的使用

行動裝置及網路可以存放各種個人資訊，例如網上銀行資訊、電子郵件、簡訊、聯絡人、社群媒體及圖片。為了確保您的裝置安全，請使用所有安全功能並確保持續更新裝置軟體。為手機及 SIM 卡建立複雜密碼，停用不必要的定位服務。[8]

務必變更存取語音信箱的預設 PIN 碼。考慮限制手機的定位服務，並查看隱私設定，以防止其他人透過第三方應用程式追蹤您的移動，以及識別您的居家地址或工作地點。查看 Apple 及 Android 隱私及安全保護措施，以增強裝置安全性。

社群媒體

網際網路可以成為資訊、教育及娛樂的寶貴來源。然而，必須保持警覺並採取預防措施，限制您在網上發佈的個人資訊量，尤其是在社群媒體。

流行的社群媒體網站允許個人建立個人資料並在線上與他人互動。人們可以在商業網路網站向其個人檔案添加更多詳細資訊，並包括工作歷史記錄及其他背景資訊。儘管這些工具可幫助您與他人溝通並宣傳您的專業背景，但線上發佈個人資訊會帶來潛在風險。

小心發佈個人資訊。惡意人士可在駭客入侵或進行身份盜竊時使用來自照片、生日、全名、居家地址及電子郵件詳細資料的位置資料。此外，有關就業、家庭成員、興趣或車輛細節的資訊對罪犯及敵對勢力而言極有價值。如果您的家人及朋友不採取適當措施來保護自己的個人資料資訊，也可能無意分享您的相關資訊。請記住，網際網路沒有「刪除」按鈕。小心分享，因為即使您從個人資料刪除貼文或圖片，也可能有人仍然能夠看到。

某些社交網站擁有您發佈的任何資料，並將您的詳細資訊出售給第三方。定期檢閱這些網站的隱私權及位置標記設定，否則您的個人資料的部分或全部風險會被大量觀眾看到，而您不知道。[9, 10]

8 聯邦通訊委員會。2019 年。保護您的智慧型裝置。2023 年 9 月 20 日摘錄。fcc.gov/consumers/guides/protect-your-mobile-device。
9 英國政府。國家網路安全中心。2019 年。社群媒體：如何安全使用。2023 年 9 月 20 日摘錄。ncsc.gov.uk/guidance/social- media-how-to-use-it-safely。
10 網路安全暨基礎設施安全局、國家網路聯盟。2019 年。社群媒體網路安全。2023 年 9 月 20 日摘錄。cisa.gov/sites/default/files/ publications/NCSAM_SocialMediaCybersecurity_2020.pdf。

查看社群媒體隱私及位置設定

X，過去稱為 Twitter

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

Instagram

- help.instagram.com/811572406418223
- **IOS:** help.instagram.com/171821142968851
- **Android:** 在您的 Android 裝置，瀏覽到設定 > 應用程式 > Instagram > 權限 > 位置

Facebook

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

Snapchat

- help.snapchat.com/hc/en-gb/sections/5690164367636-Privacy-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-settings/location-services-on-tiktok

DOXING

Doxing 係指從開放來源或遭入侵的材料收集個人身份識別資訊 (PII)（或組織的敏感資訊），並公開發放或將其用於惡意目的之做法。[11, 12] 罪犯可以將這些資訊用作勒索或激發潛在目標的恐懼。

當您在網上發佈時，重要的是要了解您將發佈什麼以及如何發佈。如果您在不套用適當的隱私設定的情況張貼過多資訊，則可能會危害您的個人安全。人們可以這些資訊來建立圖片，顯示您的人際關係、意見、感興趣的地方，以及其他可在未來利用的主題。

資料訊息代理程式還可以收集這些個人資訊並將其出售給其他公司。為盡可能減少資料到達訊息代理程式：

- **避免**共用個人資料。
- **不要**在社群媒體接受您在現實生活不認識的人。
- **確保**您使用的應用程式具有端對端加密。
- **限制**應用程式權限。
- **設定**姓名 Google 警示。
- **考慮花時間**選擇退出主要資料訊息代理程式及尋人網站，或訂閱服務來做到這一點。

位置型資訊可能發佈於社交網路，尤其是具有 GPS 功能的手機及行動裝置。這些資訊並部安全，任何人都可以看到，包括可能想傷害您的人。記錄您發佈的內容並做負責任的發佈，確保您公開的資訊不會對任何人造成風險。

如果您認為自己的身分遭到盜用：

- 向地方執法機關以及您可能已發佈個人資訊的任何線上平台**通報事件**。
- **記錄**發生的事情並拍攝螢幕截圖以與調查人員分享。
- **確定**哪些資訊遭利用，威脅的嚴重性及洩漏點。
- **配合網站管理員，**從網站或應用程式移除資訊。
- **將隱私權設定為**最私密的選項。
- **注意**身份盜用跡象、監控財務帳戶、設定詐騙警報，以及更改所有線上帳戶的登入及密碼資訊。

身分盜用法律因司法管轄區而有所不同，因此在考慮緩解及預防方案時，在您所在地區進行查詢很重要。如果擔心人身安全，請聯絡地方執法機關了解下一步。

識別及通報網路釣魚

犯罪分子通常會使用網路釣魚策略來讓您開啟有害連結、電子郵件或附件，這些連結可能會要求您的個人資訊或感染您的裝置。這些訊息通常會設計看起來像來自信任的人或組織。

網路釣魚訊息可以電子郵件、簡訊、社群媒體的直接訊息或電話形式發生。小心緊急或情感性語言，傳送個人資訊的請求，不受信任的短 URL 以及錯誤的電子郵件地址及連結。

如果您懷疑自己是網路釣魚企圖的目標，請勿點擊任何連結或附件。反之，請通報然後刪除郵件。

11 國土安全部。2024 年。合作與參與辦公室。提供個人有關人肉搜尋威脅的資源。2024 年 2 月 9 日摘錄。dhs.gov/ publication/resources-individuals-threat-doxing。

12 歐洲核子研究理事會。2017 年。電腦安全：進入下一個等級：Doxware。2023 年 12 月 12 日摘錄。home.cern/news/news/computing/computer- security-enter-next-level-doxware。

資源

人身安全

- CISA 安全與彈性指南
- CISA 現場行兇槍手備戰
- FBI 威脅恐嚇指南
- CISA 炸彈威脅
- CISA 緩解衝突系列

狀態意識

- 跟蹤預防、意識和資源中心 (SPARC)

網路安全

- CISA 保護我們的世界
- CISA 隱私和行動裝置應用程式
- CISA 分析：減輕人肉搜尋對關鍵基礎設施的影響
- CISA 社群媒體網路安全