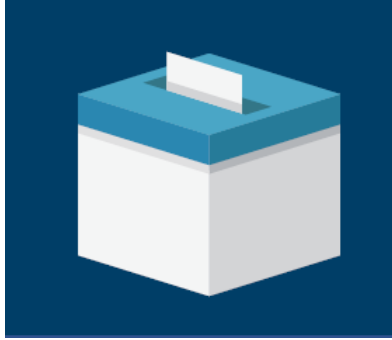


選舉基礎設施分部的安全資源



網絡安全和基礎設施安全局（CISA）與聯邦調查局（FBI）為州、地方、領土和部落（SLTT）選舉官員及其私營部門合作伙伴提供了整個聯邦政府一些可用資源的摘要，以協助應對對人員的威脅，並指導評估和減輕其有形資產的風險。

雖然其中許多資源沒有明確以選舉安全為重點，但選舉基礎設施部門可能會發現這些資源在工作過程中很有用。由於實體安全和網絡安全之間的界限越來越模糊，本文檔中還包括了以網絡安全為重點的精選資源。用戶可在下面列出的網站上找到此處引用的所有免費提供資源。

對選舉官員和基礎設施的威脅

為了回應于 2020 年美國選舉周期後針對選舉工作人員暴力威脅的增加，聯邦調查局與網絡安全和基礎設施安全局優先考慮相關措施，以應對這些威脅。聯邦調查局與網絡安全和基礎設施安全局對所有暴力威脅都慎重處理，包括那些針對選舉工作人員的威脅，因為他們在保障所有選民的選舉過程中，發揮着關鍵作用。司法部設立了“對選舉工作人員的威脅專案組”，以大力調查和起訴這些威脅。如果您是受威脅而受害的選舉工作人員，請採取以下步驟：

- 如果生命受到迫在眉睫的威脅，請撥打 911
- 要報告威脅，請聯繫在您當地聯邦調查局辦公室的選舉罪行協調人（www.fbi.gov/contact-us/field-offices）；上網在 tips.fbi.gov 提交線索；或致電 1-800-CALL-FBI（225-5324），提示 1，然後提示 3。報告選舉威脅的最佳方法，是聯繫您當地聯邦調查局辦公室的選舉罪行協調員。
- 最後，請聯繫您的網絡安全和基礎設施安全局區域辦事處，獲得根據您的司法管轄區和設施量身訂製的實體安全風險指導。網絡安全和基礎設施安全局的保護安全顧問（PSA）可以執行評估，例如安全評估和首次進入（SAFE）工具，從而顯示實體選舉基礎設施的弱點，包括選舉辦公室，選票處理地點，存儲區，投票中心和其他選舉設施。在此處查詢您當地的保護安全顧問：www.cisa.gov/cisa-regions

保護實質性安全：指導文件和其他資源

- 網絡安全和基礎設施安全局在投票地點和選舉設施的安保準備工作上為選舉官員提供了可操作的步驟，以改善其管轄範圍內的實質性安全態勢，提高選舉運作的應變能力：
www.cisa.gov/sites/default/files/publications/physical-security-of-voting-location-election-facilities_v2_508.pdf
- 網絡安全和基礎設施安全局的最後一環（最後一英里）產品是種可訂製的工具，選舉官員可以使用這些工具提高基礎設施的安全性。這些產品的示例包括選舉安全規劃快照、選舉緊急應變指南、選舉防護和其他模板。有關詳細信息並要求訂製最後一英里產品，請聯繫：
electionsecurity@hq.dhs.gov
- 網絡安全和基礎設施安全局軟目標和擁擠場所安全計劃概述和資源指南，給公共和私營部門合作伙伴提供相關信息，以加強其準備和安全：
www.cisa.gov/sites/default/files/publications/DHS-Soft-Target-Crowded-Place-Security-Plan-Overview-052018-508_0.pdf
www.cisa.gov/sites/default/files/publications/19_0424_cisa_soft-targets-and-crowded-places-resource-guide.pdf
- 網絡安全和基礎設施安全局在公共示威期間保護基礎設施，為可能成為公眾示威期間非法行為之目標的企業提供安全建議：
www.cisa.gov/sites/default/files/publications/protecting_infrastructure_during_public_demonstrations_508.pdf
- 網絡安全和基礎設施安全局減輕曝光秘聞對關鍵基礎設施的影響，定義並提供曝光秘聞示例，說明曝光秘聞對關鍵基礎設施的潛在影響，並提供保護和預防措施、緩解選項以及供給個人和組織額外的資源：
www.cisa.gov/sites/default/files/publications/cisa_insights_mitigating_the_impacts_of_doxxing_508.pdf
- 國家情報總監辦公室（ODNI）公共安全人員反恐指南，協助首批響應者識別和報告可疑活動，發現暴力動員指標，並應對和減輕恐怖襲擊：
www.dni.gov/nctc/jcat/index.html

關鍵網站/關係信息

- 網絡安全和基礎設施安全局選舉安全網頁包含網絡安全和基礎設施安全局所有的選舉安全工具和資源，其中包括本文件列出的所有聯邦政府資源：www.cisa.gov/election-security
- 網絡安全和基礎設施安全局家鄉安全計劃網站提供工具和資源，以支持社區安全和恢復能力：www.cisa.gov/hometown-security
- 網絡安全和基礎設施安全局機構間安全委員會處理政府為聯邦設施提供持續性的安全，並創建了許多標準，政策和最佳實踐文檔，可供個人和組織審查：www.cisa.gov/isc
- 網絡安全和基礎設施安全局防轟炸辦公室提供各種資源，培訓，工具和產品，以幫助州和地方當局，私人合作伙伴和其他組織瞭解及減輕簡易爆炸裝置的威脅，並保護關鍵基礎設施：www.cisa.gov/obp
- 網絡安全和基礎設施安全局中心是網絡安全和基礎設施安全局關鍵基礎設施合作伙伴與利益相關者請求援助及服務的中樞。網絡安全和基礎設施安全局中心每週運營 7 天，每天 24 小時：Central@cisa.gov 或 [888-282-0870](tel:888-282-0870)
- 聯邦調查局線索熱線是聯邦調查局報告有關選舉和非選舉涉及威脅和罪行的中心：<https://tips.fbi.gov> 或 1-800-CALL-FBI (225-5324)
- 聯邦調查局選舉罪行和安全網頁提供有關瞭解和報告選舉罪行的信息：www.fbi.gov/elections
- 聯邦調查局受保護之聲計劃為政治競選活動，公司和個人提供工具與資源，以保護應對在綫外國影響的操作和網絡安全的威脅：www.fbi.gov/protectedvoices
- 國家情報總監辦公室的國家反恐中心 (NCTC) 首批響應者工具箱提供信息，以幫助在反恐利益相關方之間做好防備，協調，應對，安全，安保和調查工作：www.dni.gov/index.php/nctc-how-we-work/joint-ct-assessment-team/first-responder-toolbox
- 美國選舉援助委員會 (EAC) 是選舉管理信息的國家信息交換中心，並具有額外的選舉安全相關資源，資料可在此鏈接找到：www.eac.gov/election-officials/election-security

培訓和演習

- 網絡安全和基礎設施安全局選舉安全培訓，給選舉利益相關者在管理風險和加強選舉基礎設施的韌性上，提供額外指導。要安排或瞭解有關這些培訓的更多信息，請發送電子郵件至：electionsecurity@hq.dhs.gov
- 網絡安全和基礎設施安全局的機構間安全委員會 (ISC)，其專注於所有聯邦設施的安全，提供可能有用的在綫和交互式培訓課程，以保護您的實質性基礎設施：www.cisa.gov/interagency-security-committee-training
- 網絡安全和基礎設施安全局的防轟炸辦公室 (OBP) 提供現場，虛擬和基於網絡的獨立學習培訓。這些課程幫助公共和私營利益相關方對簡易爆炸裝置 (IED) 威脅的認知和應對能力：tripwire.dhs.gov/training-education/counter-ied-training-0
- 網絡安全和基礎設施安全局演習，包括桌面演習，提供基於情景的培訓，以幫助確定需要改進的地方，分享最佳做法，並加強對選舉基礎設施和人員威脅的準備工作：www.cisa.gov/critical-infrastructure-exercises

警戒和公共服務公告

- 選舉基礎設施信息共享和分析中心 (EI-ISAC) 提供一套選舉安全資源，包括威脅情報產品，威脅和漏洞監測，事故響應和補救，以及其它產品和服務：www.cisecurity.org/ei-isac/
- 聯邦調查局互聯網罪行投訴中心 (IC3) 接受互聯網罪行受害者的在綫投訴，並發佈與網絡犯罪有關的問題，為行業和消費者提供預警：www.ic3.gov
- 網絡安全和基礎設施安全局的國家網絡意識系統 (NCAS) 是網絡安全和基礎設施安全局的警告儲庫，用以針對當前安全，漏洞和漏洞利用相關的問題：www.cisa.gov/uscert/ncas/alerts