# 選舉無休息時間：阻斷服務風險緩解指南

## 概述

本指南提供適用於選舉官員和選舉技術提供者的積極步驟，以降低阻斷服務 (DoS, denial-of-service) 事件的可能性和影響，包括分散式阻斷服務 (DDoS, distributed denial-of-service) 攻擊和非惡意服務中斷。

選舉官員及其私部門合作夥伴越來越依賴網站、網頁應用程式及其他網站連線系統，以便向選舉人提供資訊和服務。選舉辦公室網站和網頁應用程式通常會受到巨量網際網路流量的影響，且可能繼續成為網路威脅發動者的誘人目標，他們會設法中斷或削弱美國選舉的信心。在 2022 年期中選舉週期中，多個州級和地方選舉辦公室的網站因 DDoS 攻擊和非惡意服務中斷而暫時中斷。

在選舉中，DoS 事件可能讓選舉辦公室的網站、網頁應用程式或其他依賴網際網路的系統暫時無法存取，有可能影響選舉人能否接收選舉資訊或充分利用線上選舉服務（例如檢查選舉人登記狀態和投票站資訊、檢視選票樣本、領取郵寄/不在籍選票、登記投票等）。這可能包括重要系統在選舉週期的關鍵時刻無法使用，例如接近選舉人登記截止日期時的線上選舉人登記入口網站，或者選舉日當天的投票地點查詢工具。此類中斷（無論是否因 DDoS 攻擊或非惡意服務中斷而引起）還會讓國外的威脅發動者有機會散播假資訊，並且就選舉網站中斷提出或放大虛假或超額索賠，藉此設法削弱美國選舉的公眾信心。

### DoS 和 DDoS

阻斷服務 (DoS) 事件發生在合法使用者無法存取資訊系統、裝置或其他網路服務的情況下。受影響的服務可能包括電子郵件、網站、線上帳戶（包括銀行），或者其他依賴受影響電腦或網路的服務。利用流量對目標主機或網路進行泛洪攻擊即構成 DoS 條件，該攻擊將持續至目標無法回應或直接當機，阻止了合法使用者的存取權。發生 DoS 事件時，可能是非惡意原因（例如造成網站中斷的巨量合法網際網路流量）或網路威脅發動者的行動。

DoS 事件歸類為當超載流量源自一部以上共同操作的攻擊機器時，進行分散式阻斷服務 (DDoS) 攻擊。DDoS 攻擊者通常會利用殭屍網路：一組遭駭的網際網路連線裝置，以執行從目標實體角度看來似乎來自多個不同攻擊者的大規模攻擊。

### 可能遭遇 DoS 事件的系統

供大眾使用的服務

- 選舉人或選舉資訊網站
- 選舉之夜報導網站
- 線上服務（例如選舉人資訊查詢、投票站查詢、選舉人登記、郵寄/不在籍選票領取、候選人申請等）。

依賴網際網路的辦公室系統

- 電子選民名冊
- 業務流程系統（人力資源、會計、電話線）
- 電子郵件應用程式
- 網際網路語音通訊協定 (VOIP, Voice over Internet Protocol) 電話系統

## 非惡意服務中斷

每個選舉週期，司法管轄區都會遭遇到因網際網路頻寬受限、錯誤配置或其他未充分規劃或執行之相關原因的非惡意服務中斷。在很多情況下，線上流量大可能直接讓系統癱瘓並使其暫時無法使用。另請注意，其他非惡意事件（例如切斷電話、電纜或光纖電纜的天氣事件或施工災禍）可能導致網站或系統中斷，這些事件可能貌似但並非 DDoS 攻擊。

### 當 IT 很重要的時候

選舉行事曆上的重要日期和活動會讓選舉網站和線上服務的流量增加。如果司法管轄區未做好適當準備，增加的流量可能造成服務中斷。
應牢記的重要日期和活動包括：

- 國家選舉人登記日
- 選舉人登記鼓勵活動、競選活動和截止日期
- 郵寄/不在籍選票申請截止日期
- 提前的現場投票日期
- 投票時間內的選舉日
- 結果報告

## 準備好應對 DoS 事件

選舉官員和選舉技術提供者可以採取積極步驟，以降低 DoS 事件的可能性和影響。

### 與服務提供者進行協調

在緩解與潛在 DoS 事件相關的風險時，關鍵的第一步為選舉官員在事件發生前檢閱現行合約，並且與網站服務提供者和網際網路服務提供者進行協調。這確保了選舉官員知道發生事件時該與誰聯絡，並且了解其服務提供者可能已設置完畢的保護措施。

接著，選舉官員應識別其他可用的 DoS 緩解和冗餘措施。大多數主要服務提供者都保護措施可供使用，其中的基本服務可能為免費提供，還有額外付費的進階服務。CISA 保護選舉的網路安全工具包和資源包括一系列由 CISA、CISA 聯合網路防禦協作機制 (JCDC, Joint Cyber Defense Collaborative) 成員，以及跨網路安全社區之其他人員提供的免費工具、服務和資源，且選舉官員可用於防範 DoS 事件。

最後，選舉官員也應提前與所有服務提供者（包括網路服務提供者、網際網路服務提供者，以及 DoS 保護服務提供者）進行協調，以分享關於重要選舉日期和地點的資訊，同時要求在關鍵期間提供充足的疑難排解步驟，並且確保互相了解任何可能影響選舉操作的預防性維護。

### 監控您的地點和活動

若要偵測和識別 DoS 事件，最佳方法就是監控和分析網路流量。網路流量可透過防火牆或入侵偵測系統進行監控。行政人員甚至可制定在偵測到異常流量負載後發出警示的規則，並且識別符合特定標準的流量或丟棄的網路封包來源。

選舉官員應與其服務提供者互動，以進一步了解他們正在監控的活動，以及其網站的「正常」流量樣貌。除了與服務提供者進行協調之外，選舉官員還可在自己的系統中，直接尋找可能指出潛在 DoS 事件的特定指標。如以上討論內容，成功識別不尋常、意外或異常活動的能力取決於了解每個系統或服務的「正常」基線模式。

這些指標可能包括：

- 網路效能異常緩慢（例如開啟檔案或存取網站時速度緩慢）
- 特定網站不存在
- 無法存取任何網站
- 應用程式效能遲緩
- 處理器和記憶體使用率特別高
- 網路流量異常高

## 準備好應對 DoS 事件

對於成功的選舉操作（包括網路操作）而言，韌性流程相當關鍵。這表示有資源且熟練的組織網路安全應變和溝通計畫，其中包括應對和緩解 DoS 事件的影響。

### 識別問題

如果選舉官員評估潛在 DoS 事件正在發生，則應聯絡其網路管理員，以確認是否因維護或內部網路問題而引發中斷狀況。網路管理員還可監控網路流量，以便應用防火牆規則並可能透過 DoS 防護服務重新路由流量，藉此確認事件、識別來源和緩解情況。

在聯絡網路管理員後，選舉官員可能需要與網站服務提供者聯絡，以詢問該端是否出現中斷狀況，或甚至是他們的網路是否是攻擊目標，網站則為間接受害者。在此實例中，網站服務提供者或許能夠提出適當行動步驟的建議。如果服務中斷發生在關鍵的選舉期間或需要一些補救時間，選舉官員應準備好實施採用備用或替代選項的緊急應變或持續營運計畫，直到正常服務恢復到可接受的程度。

如果出現攻擊，選舉官員不應忽略網路上的其他主機、資產或服務。攻擊者可能透過 DDoS 攻擊轉移其預期目標的注意力，並且找機會對網路內的其他服務進行第二次攻擊。

CISA 建議選舉官員和選舉技術提供者將可疑的網路攻擊迅速回報給：

- CISA，透過 report@cisa.gov 或 (888) 282-0870
- FBI，透過適當的 FBI 地方分局
- EI-ISAC，透過 SOC@cisecurity.org 或 866-787-4722
- 與司法管轄區相關的其他國家或地方當局

### 備妥分享資訊的替代方法

成功的選舉操作重點在於韌性。這表示制定有資源且熟練的緊急應變或持續營運計畫，其有助於緩解 DoS 事件。

選舉辦公室在遭遇 DoS 事件後，可能無法與大眾、其他選舉辦公室，甚至是其他在同棟大樓的辦公室進行通訊。在每次選舉前，選舉官員應備妥宣傳非官方選舉結果等選舉資訊的替代方法，以免 DoS 事件讓網站或其他應用程式變得無法使用。這可透過多種方法達成。國家或地方司法管轄區或許能夠在與主要網站完全獨立的基礎設施上託管備用網站，這在維護或升級期間對辦公室的效益很大。有選舉之夜報導網站的選舉辦公室可能也會考慮將 PDF 版的結果內容，上傳至主要網站及其他位於國家或區域網路的網站。最後，鼓勵選舉辦公室與媒體管道建立關係，協助在發生事件時傳遞資訊，例如正確的投票地點資訊或非官方選舉結果。

### 針對 DoS 事件制定內部通訊計畫

與事件應變規劃相當，選舉官員應將 DDoS 攻擊和非惡意服務中斷納入其溝通規劃中。溝通計畫應識別危機溝通團隊（包括 IT 和溝通團隊的成員）、定義職位和職責，並且建立在事件期間維護溝通管道的程序。危機溝通團隊應準備好維護溝通效果，且不需要進入主要辦公室的網路或行動電話。選舉官員也可能會考慮制定一系列與 DoS 事件相關的關鍵術語和定義供全體工作人員使用。

選舉官員也應考慮準備可在 DoS 事件期間視需要改動和使用的保留聲明。保留聲明不只要提供給資深工作人員和溝通官，還有接聽大眾和媒體來電和受理問題的前線工作人員。

## 適用於 DoS 事件的計畫和訓練

如以上強調內容，選舉官員應在緊急應變、持續營運、事件應變和復原計畫中加入 DoS 事件情境。這些計畫應引導組織識別、緩解此類事件並快速從中復原，並且在事件應變和復原期間維持有效溝通。CISA 適用於選舉安全的網路事件偵測與通知規劃指南可能有助於制定組織的事件應變計畫。

DoS 事件應變計畫（與其他網路事件相同）應明確指定所有利害關係人的職位和職責，包括組織領導人和服務提供者。該計畫至少應概述確認事件、了解事件性質、部署緩解措施、監控有效性和復原的程序。

DoS 事件規劃也應考量持續營運和災害復原程序，特別是在內部溝通管道受到中斷影響的情況下（例如網際網路語音通訊協定電話系統無法使用）。組織領導階層應熟悉備用或替代的溝通管道，以便迅速有效地聯絡工作人員、服務提供者或選舉人，例如電話樹、替代電子郵件或緊急通知系統。

在發生事件且服務復原後，選舉官員應提出事件簡報，已討論從事件應變和溝通計畫實施中學到的教訓，並視情況更新相關程序。

最後，全體工作人員均應接受事件應變的訓練並加以實踐。選舉官員可考慮將 DoS 事件納入桌上模擬演習或其他情境型訓練。對於確保所有人員了解其在事件期間的職位和職責、協助識別應變計畫中的差距、讓利害關係人實踐真實事件的急迫性和步調，並且在現行計畫和緩解措施中建立信心。CISA 的整體式選舉網路桌上模擬演習資源包括演習情境一部分的 DDoS 攻擊。CISA 的區域網路安全顧問 (CSA, Cybersecurity Advisors) 還可用於提供評估和保護性資源，包括關於 DoS 事件的風險管理指引。

## 其他資源

本指南中提供的資源以整份文件和下方連結的其他資源作為補充內容。鼓勵選舉官員和選舉技術提供者檢閱這些資源，以進一步準備應對和緩解與潛在 DoS 事件相關的風險。

- CISA FBI MS-ISAC 了解和應對分散式阻斷服務攻擊
- CISA 了解阻斷服務攻擊
- CISA 保護選舉的網路安全工具包和資源
- CISA 分散式阻斷服務 (DDoS) 快速指南
- CISA 適用於選舉安全的網路事件偵測與通知規劃指南
- CISA 整體式選舉網路桌上模擬演習
- CISA 能力增強指南：針對網頁服務的體積型 DDoS 技術指引