NO DOWNTIME IN ELECTIONS: A GUIDE TO MITIGATING RISKS OF DENIAL-OF-SERVICE

OVERVIEW

This guide offers proactive steps for election officials and election technology providers to reduce the likelihood and impact of denial-of-service (DoS) incidents, including distributed denial-of-service (DDoS) attacks and non-malicious service interruptions.

Election officials and their private sector partners increasingly depend on websites, web applications, and other network-connected systems to inform and provide services to voters. Election office websites and web applications are often subject to high volumes of internet traffic and may continue to be attractive targets for cyber threat actors seeking to disrupt or undermine confidence in U.S. elections. Multiple state and local election offices experienced temporary website outages resulting from DDoS attacks and non-malicious service interruptions during the 2022 midterm election cycle.

In elections, DoS incidents could render election office websites, web applications, or other internet-reliant systems temporarily inaccessible, potentially impacting voters' ability to receive official election information or take advantage of online election services (e.g., checking voter registration status and polling site information, viewing a sample ballot, requesting a mail-in/absentee ballot, registering to vote, etc.). This could include disruptions to the availability of important systems at key moments in the election cycle, such as an online voter registration portal near the voter registration deadline or a polling place lookup tool on Election Day. Such disruptions, whether resulting from a DDoS attack or non-malicious service interruptions, can also provide opportunities for foreign threat actors to spread disinformation and seek to undermine public confidence in U.S. elections by, for example, making or amplifying false or inflated claims about an election website outage.

DoS and DDoS

A **Denial-of-Service (DoS)** incident occurs when legitimate users are unable to access information systems, devices, or other network resources. Services affected may include email, websites, online accounts (e.g., banking), or other services that rely on the affected computer or network. A DoS condition is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users. DoS incidents can occur for non-malicious reasons (e.g., high volumes of legitimate internet traffic causing a website outage) or due to the actions of a cyber threat actor.

A DoS incident is categorized as a **Distributed Denial-of-Service (DDoS)** attack when the overloading traffic originates from more than one attacking machine operating in concert. DDoS attackers often leverage a **botnet**—a group of hijacked internet-connected devices—to carry out large-scale attacks that appear, from the targeted entity's perspective, to come from many different attackers.

Systems that may Experience DoS Incidents

Public-Facing Services

- Voter or election information websites
- Election night reporting websites
- Online services (e.g., voter information look-up, polling site look-up, voter registration, mail-in/absentee ballot request, candidate filing, etc.)

Internet-Reliant Office Systems

- Electronic poll books
- Business process systems (HR, accounting, phone lines)
- Email applications
- Voice over Internet Protocol (VOIP) phone systems

NON-MALICIOUS SERVICE INTERRUPTIONS

Each election cycle, jurisdictions across the country experience non-malicious service interruptions resulting from limited internet bandwidth, misconfigurations, or other reasons related to insufficient planning or execution. Oftentimes, high online traffic can simply overwhelm a system and render it temporarily unavailable. It should also be noted that other non-malicious incidents, such as a weather event or construction mishap that cuts a telephone, cable, or fiber line, can result in website or system outages that may appear to be, but are not DDoS attacks.

When IT Matters

Important dates and events on the election calendar drive increased traffic to election websites and online services. Increased traffic can cause service interruptions if jurisdictions are not properly prepared. Important dates and events to keep in mind include:

- National Voter Registration Day
- Voter registration drives, campaigns, and deadlines
- Mail-in/absentee ballot application deadlines
- Early in-person voting dates
- Election Day during voting hours
- Results reporting

BE PREPARED FOR DOS INCIDENTS

Election officials and election technology providers can take proactive steps to reduce the likelihood and impact of DoS incidents.

Coordinate with Service Providers

A key first step in mitigating risk associated with potential DoS incidents is for election officials to review existing contracts and coordinate with both website service providers and internet service providers before an incident occurs. This ensures election officials know who to contact in event of an incident and understand the protections their service providers may already have in place.

Next, election officials should identify what additional DoS mitigation and redundancy measures are available. Most major service providers have protections available, which may be offered at no cost for basic services, or at additional cost for advanced services. CISA's Cybersecurity Toolkit and Resources to Protect Elections includes a list of no cost tools, services, and resources provided by CISA, members of CISA's Joint Cyber Defense Collaborative (JCDC), and others across the cybersecurity community that election officials can use to protect against DoS incidents.

Lastly, election officials should also coordinate in advance with all service providers—website service providers, internet service providers, and DoS protection service providers--to share information about important election dates and locations, requesting that ample troubleshooting is available during key periods, and ensuring mutual awareness of any planned maintenance that could impact election operations.

Monitor Your Sites and Activity

The best way to detect and identify a DoS incident is via network traffic monitoring and analysis. Network traffic can be monitored via a firewall or intrusion detection system. An administrator may even set up rules that create an alert upon the detection of an anomalous traffic load and identify the source of the traffic or dropped network packets that meet certain criteria.

Election officials should engage with their service providers to better understand what activities they already monitor, and what "normal" traffic looks like for their websites. In addition to coordinating with service providers, there are certain indicators that election officials can directly look for on their own systems, which may indicate a potential DoS incident. As discussed above, the ability to successfully identify unusual, unexpected, or abnormal activity depends on understanding what the "normal" baseline looks like for each system or service.

These indicators may include:

- Unusually slow network performance (such as slow to open files or access websites)
- Unavailability of a particular website
- Inability to access any website
- Sluggish application performance

- Unexpectedly high processor and memory utilization
- Abnormally high network traffic

BE READY TO RESPOND TO A DOS INCIDENT

Resilient processes are critical to successful election operations, to include cyber operations. This means having resourced and practiced organizational cyber incident response and communications plans that include responding to and mitigating the impacts of DoS incidents.

Identifying the Issue

If election officials assess a potential DoS incident is occurring, then they should **contact their network administrator** to confirm whether the interruption is due to maintenance or an in-house network issue. Network administrators can also monitor network traffic to confirm an incident, identify the source, and mitigate the situation by applying firewall rules and possibly rerouting traffic through a DoS protection service.

After reaching out to the network administrator, election officials may need to **contact their website service provider** to ask if there is an outage on their end or even if their network is the target of the attack and website is an indirect victim. In this instance, website service providers may be able to advise on an appropriate course of action. If the service outage falls within a critical election period or will take some time to remediate, election officials should **be prepared to implement contingency or continuity of operations plans** that use backup or alternative options until normal services can be restored to an acceptable level.

In the case of an attack, election officials should not lose sight of the other hosts, assets, or services residing on the network. Attackers may conduct DDoS attacks to deflect attention away from their intended target and use the opportunity to conduct secondary attacks on other services within the network.

CISA recommends that election officials and election technology providers promptly report suspected cyber-attacks to:

- CISA, at report@cisa.gov or (888) 282-0870
- The FBI, via the appropriate local FBI field office
- The EI-ISAC, at SOC@cisecurity.org or 866-787-4722
- Other state or local authorities, as relevant to the jurisdiction

Have Alternative Methods for Sharing Information Ready to Go

Successful election operations are all about resilience. This means having resourced and practiced contingency or continuity of operations plans that address mitigating DoS incidents.

Election offices experiencing a DoS incident may be prevented from communicating with the public, other election offices, and even other offices in the same building. Well in advance of each election, election officials should prepare alternative methods for disseminating election information, including unofficial election results, in case a DoS incident renders websites or other applications unavailable. This can be achieved in multiple ways. State or local jurisdictions may be able to host a backup website on completely separate infrastructure from the primary website, which may also benefit offices during maintenance or upgrade periods. Election offices with election night reporting websites may also consider uploading a PDF of results to their main website and other websites on their state or local network. Finally, election offices are encouraged to establish relationships with media outlets that could help relay information, such as correct polling location information or unofficial election results, in the event of an incident.

Develop an Internal Communications Plan for DoS Incidents

Parallel to incident response planning, election officials should incorporate both DDoS attacks and non-malicious service interruptions into their communications planning. Communications plans should identify a crisis communications team (including members of the IT and communications teams), define roles and responsibilities, and establish procedures for maintaining communication channels during an incident. The crisis communications team should be prepared to maintain communications without access to the primary office network or mobile phones. Election officials may also

consider developing a list of key terms and definitions related to DoS incidents for use by all staff.

Election officials should also consider preparing holding statements that can be adapted and used as needed during a DoS incident. Holding statements should not only be provided to senior staff and communications officers, but also to frontline staff who answer calls and receive questions from the public and media.

PLAN AND TRAIN FOR DOS INCIDENTS

As highlighted above, election officials should include DoS incident scenarios in their contingency, continuity of operations, incident response, and recovery plans. These plans should guide the organization in identifying, mitigating, and rapidly recovering from such incidents, as well as maintaining effective communications throughout incident response and recovery. CISA's Cyber Incident Detection and Notification Planning Guide for Election Security may be helpful in developing the organization's incident response plan.

Plans for responding to DoS incidents, as with other cyber incidents, should clearly designate roles and responsibilities for all stakeholders, including organizational leaders and service providers. At a minimum, the plan should outline procedures for confirming the incident, understanding the nature of the incident, deploying mitigations, monitoring effectiveness, and recovering.

Planning for DoS incidents should also consider continuity of operations and disaster recovery procedures, especially if internal communication channels are impacted by the interruption (e.g., an inaccessible Voice over Internet Protocol phone system). Organizational leadership should be familiar with backup or alternative communication channels to contact staff, service providers, or voters quickly and effectively, such as phone trees, alternate emails, or emergency notification systems.

Following an incident, once services have been restored, election officials should conduct an incident debrief to discuss lessons learned from the implementation of the incident response and communications plans, and update procedures accordingly.

Finally, all staff should train and regularly practice incident response. Election officials may consider including DoS incidents in tabletop exercises or other scenario-based trainings. Routine practice is critical for ensuring that all individuals understand their roles and responsibilities during an incident, help identify gaps in the response plan, enable stakeholders to practice the urgency and cadence of a real event, and build confidence in both the plan and mitigation measures in place. CISA's Elections Cyber Tabletop in a Box resource includes a DDoS attack as part of the exercise scenario. CISA's Regional Cybersecurity Advisors (CSAs) are also available to provide assessments and protective resources, including risk management guidance on DoS incidents.

ADDITIONAL RESOURCES

The information provided in this guide is complemented by additional resources linked throughout the document and below. Election officials and election technology providers are encouraged to review these resources to further prepare for and mitigate risks associated with potential DoS incidents.

- CISA FBI MS-ISAC Understanding and Responding to Distributed Denial-of-Service Attacks
- CISA Understanding Denial-of-Service Attacks
- CISA Cybersecurity Toolkit and Resources to Protect Elections
- CISA Distributed Denial-of-Service (DDoS) Quick Guide
- CISA Cyber Incident Detection and Notification Planning Guide for Election Security
- CISA Elections Cyber Tabletop in a Box
- CISA Capacity Enhancement Guide: Volumetric DDoS Against Web Services Technical Guidance