DEFENDING DIGITAL DEMOCRACY PROJECT

FINAL WEEK CYBERSECURITY CONSIDERATIONS
TOP TAKEAWAYS

This election has already faced threats from cyber adversaries seeking to influence its outcome. The joint CISA-FBI alert confirming Russian state-sponsored activity targeting government networks on October 22 builds on other advisories around potential cyberattacks on election systems ahead of the election, including advisories of DDOS attacks against election infrastructure.

What is a Distributed Denial of Service Attack?

DDoS attacks attempt to overwhelm a website or network with malicious traffic, usually originating from thousands or even millions of computers across the internet. Once a DDoS attack is launched against a target website or network, it can be difficult or even impossible to quickly halt the attack at the source.

Making unplanned or last-minute changes ahead of election day can introduce serious risks, especially given the short window to test changes. Here are some considerations as you work to address and prepare to counter potential cyber threats:

- **SOPs:** Make plans to adhere as closely to your planned standard operating procedures as possible.
- **Decision to Patch:** You should weigh the risk of pre-election vulnerability exploitation against the risk of making significant, last-minute changes to a mission-critical system. Any decision to patch must include adequate time to properly test and validate the entire system after changes have been made.
- **Responding to a Vulnerability Notification:** If a trusted party contacts you directly about a potential vulnerability in your election website(s), engage with them. You should be prepared for a scenario where you may have to operate at least some of your systems unpatched through election day. Ask the notifying party if they are able to share any indicators of compromise or observable symptoms of the problem. Whether you are able to patch your systems or not, knowing what indicators to look for could help you recognize if and when to activate your cyber incident response and incident response communications plan.

Plan to operate at a heightened security posture until official election operations are complete and all results are reported. Threats to this election were anticipated, and now that they have been confirmed, it is especially important that you maintain backup communications mechanisms and exercise or create an incident communications response plan.

See Election Battle Staff Communications | Top Takeaways for ideas on back up communication planning.

Additional Resources:

Reporting:

- Coordinate with your precinct, local and state jurisdictions.
- Report to EI-ISAC: SOC@cisecurity.org
- Additional contacts: CISAServiceDesk@cisa.dhs.gov, cywatchfbi.gov

D3P State and Local Election Cybersecurity Playbook (PDF)

- Security Insights by Election System (p.19-20)
- Election Reporting Systems and Communications Channels (p.40-42)