EIS Communiqué

Sharing Election Infrastructure News and Resources

June 6, 2018 Volume 1, Issue 11

Tip of the Week!

A denial-of-service (DoS) attack occurs when an attacker "floods" a website with spam or viewing requests which then block legitimate users from accessing information or services such as email, websites, or online accounts. Indicators of a DoS attack include unusually slow network performance or inability to access a specific website. To reduce the chances of your elections webpage becoming a DoS victim, consider the following best practices: 1) Install and maintain anti-virus software, 2) Configure a firewall to restrict traffic, and 3) Apply e-mail filters to reduce spam. For more information, view our Security tip here.

Physical Security Best Practices for Election Infrastructure Partners

Low Cost Measures Can Enhance Security at Voting Locations

The emphasis on election security has rightly focused on cyber intrusions and prevention. The 2016 election highlighted vulnerabilities that can be exploited by nation-state and other actors in an effort to influence the results of our election processes so integral to a free society. However, in addition to cyber precautions, the evolving threat environment also highlights the need to enhance physical security in election infrastructure locations to maintain the safety of people and property.

As demonstrated by events domestically and abroad, terrorists and other extremist actors are encouraged by the potential to leverage easy-to-use tools with few identifiable indicators to inflict physical harm. Malicious actors leverage these tools and tactics to attack segments of society inherently open to the public which, by nature of their purpose, do not incorporate strict security measures. Voting locations, particularly those with large waiting lines, pose potential risks to voters from attacks ranging from an active assailant to a vehicle-ramming scenario.

To ensure voters are safe and elections are conducted without disruptions, consider incorporating some low-cost security measures to enhance the physical security at voting locations, including:

- **Coordinate with local law enforcement** to maintain presence before, during and after polling hours.

- **Develop and test plans for security and emergency response** with local law enforcement before an election.
- **Define the perimeter and areas that require restrictions** from vehicle entrance, and leverage barriers as necessary to prevent vehicle access.
- **Evaluate vehicle traffic patterns** near the venue and implement strategies to reduce vehicle speeds.
- **Keep vehicles at a safe distance** from areas where large numbers of people congregate.

For more information, please contact your local Protective Security Advisor (PSA) or email NICC@hq.dhs.gov to identify a PSA, or visit https://www.dhs.gov/hometown-security.

Enhancing Preparedness for a Potential Active Shooter Incident

The Department of Homeland Security maintains a comprehensive set of resources aimed at better positioning the public and private sectors to reduce the impacts of an active shooter incident. Resources include in-person and online training and guides focused on behavioral indicators, potential attack methods, how to develop an emergency action plan, actions to be taken during an incident, and how to quickly and effectively recover from an incident.

- In-person workshops leverage a curriculum that incorporates interactive breakout sessions and hands-on planning techniques that provide participants with the necessary information to develop an effective emergency action plan.
- DHS's Active Shooter Preparedness website contains a variety of instructional videos and resources on actions individuals can take to increase the probability of survival during an incident and instructions for organizations to develop an emergency action plan. There are several reference materials in nine different languages that provide insight into the active shooter threat, behavioral indicators, and actions to take.

These resources equip venue operators, election officials, and local planners with the necessary information to develop emergency action plans that can be used to train with local law enforcement before election day. DHS also maintains a cadre of Protective Security Advisors (PSAs), who are security subject matter experts serving in 50 states, Washington, D.C., and Puerto Rico, and can share information, conduct vulnerability assessments, and brief on effective planning strategies venue operators can adopt to mitigate the effects of an active shooter incident.

For more information on workshops or emergency action plans, please contact your local PSA or email NICC@hq.dhs.gov to identify a PSA, or visit https://www.dhs.gov/hometown-security.

Protective Security Advisors and Elections Infrastructure Engagement

Since the initial joint cyber-physical security outreach meetings with Secretaries of State and Elections Officials last fall, PPSAs have been coordinating closely with state officials to provide services across the nation.

In preparation for the high-priority effort, several National Protection and Programs Directorate (NPPD) supervisory PSAs developed a tailored Election Infrastructure Outreach Security Checklist containing relevant questions for the Election Infrastructure Sub-Sector. The core of the checklist derives from the FEMA 426, Reference Manual to Mitigate Terrorist Attacks Against Builidngs- Building Vunerability Assessment Checklist, but also includes ties to the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity.

PSAs have also completed numerous visits to election infrastructure sites in conjunction with senior state election officials, and continue to work with their counterparts. These visits have included an overview of the elections infrastructure security initiative, and physical and cyber resources available to officials. PSAs have also conducted security walk-throughs, which identified security options for the respective offices. These engagements also provide valuable face-to-face contact with county election offices and other interested entities.

This effort has made great use of the Protected Critical Infrastructure Information (PCII) Electronic Submission process. State officials, including several Secretaries of State, have praised the comprehensive and team-focused efforts of the PSAs and Cybersecurity Advisors. The coordinated effort is expected to continue through the primary season up to and including Election Day.

Election Security Web Page Up!

Remember –– NPPD has created a new webpage focused on elections infrastructure security-related issues is now available on the DHS website. NPPD created the webpage to more effectively share elections infrastructure information and pertinent elections community documents. Content includes overviews on NPPD cyber services available at no cost to the state and local elections community. Other content includes information on the

electoral process, coordinating councils, and elections security. Additional information is added frequently. To see what may be of benefit for you, visit: https://www.dhs.gov/topic/election-security.

EIS Background

The Department of Homeland Security (DHS) designated election infrastructure as critical infrastructure on January 6, 2017. The designation created the Election Infrastructure Subsector under the Government Facilities sector, with DHS as its Sector Specific Agency (SSA). The designation set several actions in motion, such as the formation of coordinating councils, coordinated federal support, and the availability of services and tools for the Election Infrastructure Subsector. For more information on the topics of this Communiqué, please contact the EISSA at EISSA@hq.dhs.gov.

Purpose

The EIS Communiqué series will periodically inform subscribers of the myriad DHS services available to the EI community. DHS provides services on a no-cost, voluntary basis to state and local election officials.

Future EIS Communiqués will highlight various services and tools, such as assessments, threat information-sharing programs, network protection, best practices, incident response, and developments at the federal level.

Thank you,

Election Infrastructure SSA

We want to hear from you! Send us your comments on how we may better serve you as well as questions, feedback, and ideas for future Communiqué topics at EISSA@hq.dhs.gov.