Foreign entities often use cyberattacks and social media infiltration to actively spread misinformation and attempt to influence elections outcomes. It is widely reported that cyberattacks have targeted state elections information technology (IT) infrastructure around the United States including elections systems vendors. There is no evidence that any vote in a U.S. election has ever been compromised by a cybersecurity breach. These statistics include Washington DC. It is important to note that DC's voting machines are never connected to the internet; voting machines have tamper-resistant seals; and our machines are audited regularly while we continually update our equipment with the latest technologies and protections. These measures provide an environment that would require extraordinary measures to gain access to our electronic systems and the data the systems contain and process. The lack of internet access to our systems alone is a major protection. However, news reports revealed that hackers targeted state and local voter registration databases and managed to access elections systems in several states. U.S. investigations found that Russian hackers attempted to access the voter registration files or public election sites in 21 states. Many experts believe this will remain an issue in the 2020 elections.

In January 2017, the Department of Homeland Security (DHS) designated elections systems as critical infrastructure. The significance of this critical infrastructure designation enables DHS to prioritize cybersecurity and physical security assistance to election officials upon request. Federal Government, state and local government officials and the private sector can establish mutually recognized information sharing to prevent or mitigate incidents that undermine the integrity of or public confidence in the election system.

DCBOE is focused on continuing to do what is necessary to secure our systems from potential cyber-attacks. DCBOE, in collaboration with federal and local enforcement partners, remains vigilant on current and emerging threats that might impact elections.

In preparation for the 2020 elections, and with the constant support of Federal Authorities, including the Federal Bureau of Investigation (FBI) and DHS, DCBOE is taking the following measures to secure the agency's elections systems' voting equipment, tabulation system and voter registration database.

Partnering with Federal and Local Partners:

- DCBOE works with the Center for Internet Security (CIS) and the Multi-State Information Sharing and Analysis Center (MS-ISAC) to gather and share intelligence about cyber threats (such as website defacement) that target government or government-affiliated systems.

- DCBOE also participates in CIS's Elections Infrastructure Information Sharing and Analysis Center (EI- ISAC), an elections-focused cyber defense suite

providing additional free support and resources including forensic analyses and emergency response teams.

- DCBOE has partnered with the leaders of the U.S. intelligence community and law enforcement like the DHS, DC Homeland Security Emergency Management Agency (DC HSEMA) the Department of Justice (DOJ) and FBI to work on a strong and unified incident response and shares information as well as best practices with all partners.

- We have visited the fusion center of The Office of the Chief Technology Officer (OCTO) to better coordinate in the event of a cyber-threat or emergency incident.

- DCBOE staff attended the Tabletop 2019 National Election Cyber exercise prepared by the Cybersecurity and Infrastructure Security Agency (CISA) for the purpose of identifying best practices and areas of improvement.

Protecting Election Infrastructure:

- DCBOE uses Election Assistance Commission (EAC) certified voting equipment. Any modification or upgrades have to be certified through EAC's Testing and Certification Program. As part of the 2020 Election preparation, DCBOE is working with the vendor to upgrade and update its current version of the tabulation system to enhance security.

- To strengthen physical security DCBOE is in the process of reviewing and updating standards and procedures to protect voting systems and related facilities and equipment from natural and environmental hazards, tampering, vandalism and theft. It is conducting a security review of its "chain of custody" procedures handling ballots, voting equipment, and peripheral devices at various points during the election process. A security protocol is in place for accessing the warehouse as well as the main office.

- DCBOE staff conducted an audit of the Board's firewall and anti-virus software and upgrades were made to detect "Advanced Persistent Threats". The Board also regularly conducts vulnerability and intrusion testing on its network.

- The DCBOE will also, in conjunction with OCTO, provide social engineering and phishing training to employees urging them not to open suspicious emails, click links contained in such emails, post sensitive information online, and never provide usernames, passwords, and/or personal information to any unsolicited request.

- DCBOE completed the Cyber Resilience Review (CRR) and the Cyber Infrastructure Security (CIS) assessment from DHS in July 2018 and is planning to conduct another assessment prior to the 2020 elections.

- DCBOE is in the process of hiring cybersecurity professionals to review essential critical services during operational challenges and crises and integrate performance comparisons for each of the 10 security domains identified by center information security covered in the assessment.

- OCTO currently manages the security sensors and monitors and reports any network activity to and from DCBOE's network to DHS security alerts for both traditional and advanced network threats.

- We also are expanding the post-election audit program and hiring new data staff.

- By the 2020 elections, all early voting centers will offer an option of voting by paper ballots or machines that produce paper ballots.

Elections Cybersecurity:

- DCBOE recently implemented a Security Information and Event Management (SIEM) system. This solution collects and aggregates log data generated throughout the organization's technology infrastructure, from host systems and applications to network and security devices such as firewalls and antivirus filters. The software then identifies and categorizes incidents and events as well as analyzes them.

- Our agency works closely with the DHS, which regularly monitors the DCBOE election systems to detect unauthorized access and weaknesses.

- We are training DCBOE staff on detection, prevention and the proper response to cyberattacks.

- We are working with OCTO's Chief Information Security Officer (CISO) Cyber Advisory Panel and security experts to help continue to harden our systems. Additionally**,** DCBOE has taken advantage of election security-related services offered by DHS. The services include:

    - Regular cybersecurity scans of our elections systems to identify vulnerabilities.

    - In 2018, a DHS security team spent days at the Board's office conducting a thorough review of our systems with a few recommendations for security improvement. We are instituting those recommendations.

- DCBOE staff members have obtained security clearances required to participate in classified briefings on election-related issues.

- DHS is in the process of providing physical security assessments for our office.

- DCBOE officials are in regular communication with DHS officials, in the District of Columbia (DC HSEMA) as well as additional local and federal partners, including the DHS Cybersecurity Advisor, DHS Regional Director, DHS protective Security Advisor, DHS Intelligence Officer, and DHS Critical Infrastructure Specialist.

We are upgrading the City Wide voter registrations system:

- This is the DCBOE's largest IT project in over two decades.
- Modernizing the DCBOE city wide voter registrations system will improve functionality and security of the DCBOE database.

Providing Ongoing Training Opportunities:

- Provide training in conjunction with OCTO's cybersecurity training, email phishing expedition exercise for the full time staff and develop cybersecurity awareness training for election workers.

- Use the Election security video prepared by the EAC as part of ongoing training.

- The DCBOE IT Staff attends the monthly free webinar in conjunction with MS-ISAC, DHS, CIS, and other security experts.

- Our staff has participated in nationally-recognized election cybersecurity trainings, including a table-top training exercise by Harvard Kennedy School's Belfer Center. We are planning to conduct similar trainings, mock election exercises, and issue other resources to BOE staff, including tabletop exercises to train election, IT, and security personnel in incident response and preparation, simulating scenarios that could impact voting operations.

- Our staff participated in the Election Day Preparedness Table Top exercise in June 2019 in Conjunction with State and Federal offices of Homeland Security.

- We have issued guidance, training, and resources to BOE staff on strong cybersecurity practices for voting system and network preparation and security, including pre-election testing, password

and permissions management, restricting access, file transfers, and vote canvassing. We are also providing anti-phishing and security training and tools to all BOE staff in partnership with OCTO's security office.

Finally, DCBOE will be urging voters on our website, twitter and other communications outlets, including by mail, to be vigilant about election information they consume and share on social media.

We are committed to securing the vote of all our District voters in this ever-changing election environment. Our goal has always been making sure our elections are accessible fair and accurate. DCBOE will continue to work individually and with the collective efforts of its federal, local and private sector partners to ensure election security, reduce risks, and sustain the integrity of the election.

.