County of San Mateo

Inter-Departmental Correspondence

Department: ASSESSOR-COUNTY CLERK-RECORDER-ELECTIONS
File #: 18-225 Board Meeting Date: 3/27/2018

Special Notice / Hearing: None
Vote Required: Majority

To: Honorable Board of Supervisors

From: Mark Church, Chief Elections Officer & Assessor-County Clerk-Recorder

Subject: San Mateo County Election Infrastructure Security

RECOMMENDATION:
Accept the Election Infrastructure Security Report from the Chief Elections Officer.

BACKGROUND:
The importance of the security and integrity of the County Election Infrastructure and Voter Registration and Voting Tabulation Systems cannot be overstated. On January 6, 2017, the Department of Homeland Security (DHS) formally designated the nation's election infrastructure as "Critical Infrastructure" for federal protection and support. This designation recognizes the vital role elections play in our nation as the foundation of our democratic process and elevates the protection of our election infrastructure as a priority within the National Infrastructure Protection Plan. It allows the election infrastructure to enjoy all the benefits and protections the U.S. Government has to offer particularly in the areas of cybersecurity and risk management.

San Mateo County voters can rest assured that their confidential voter information and voting tabulation systems are safe and secure. These systems are protected in a multi- layered cyber and physical infrastructure environment. Our election systems and infrastructure are protected with the highest levels of security that bring together federal, state, local and private sector resources to bolster our cybersecurity defenses. Election security depends on a well-coordinated, multi-organizational effort to protect the integrity of election systems. It is a responsibility that cannot be performed by one entity alone given the broad reaches of current cybersecurity threats.

We live in an age where the threat of sophisticated cyberattacks are very real across all technology sectors. Last year, cybercriminals attacked one of the largest credit bureaus in the nation and stole the personal data of 145 million people. Over 3 billion accounts of a major internet provider were compromised exposing sensitive customer data. Hackers have even successfully penetrated systems at the National Security Agency and the U.S. Department of Defense.

Malicious nation actors such as Russia, North Korea, China and Iran invest huge sums of money into cyber warfare and pose as one of the largest threats to our national security and to our election infrastructure. Only through a vigilant, well-funded and coordinated cyber defense effort between federal, state and local agencies, in partnership with the private sector, can we safeguard our democratic process.

In this report we will provide an overview of the County's election infrastructure, Voter Registration and Voting Tabulation Systems and the cybersecurity protections and protocols in place to protect these systems. The report will also briefly discuss some of the future and ongoing needs of elections cybersecurity in our new elections paradigm.

DISCUSSION:
As previously mentioned, the Department of Homeland Security has designated the nation's election infrastructure, as critical infrastructure, for purposes of protection and support. Election infrastructure is defined as election storage facilities, polling places, centralized vote tabulation locations used to support the elections process, and information and communications technology, including voter registration databases, voting machines, and other systems to manage the elections process and report and display results on behalf of state and local governments.

In San Mateo County, election infrastructure is broken down into two major categories:
Election System Technology, which comprises our Voter Registration and Voting Tabulation Systems; and Physical Assets, which include our human resources, facilities and equipment.

ELECTION SYSTEM TECHNOLOGY

Voter Registration System
San Mateo County uses an Election Information Management System from DFM Associates, Inc. called EIMS. This system stores all the voter data and voter participation history in addition to other items. Below are some of the systems and protocols in place to protect the County's Voter Registration System.

County Network
One of the first lines of defense for the County's Voter Registration System is our County Network. The voter registration database servers are located inside the County network, behind the County firewall which is constantly monitored and patched. The County subscribes to the Department of Homeland Security's Cyber Hygiene Service which performs regular vulnerability scans of the County's network.

All users must have a unique login and password to sign into the County network. All remote users entering the County network must use a secure VPN connection to access the network.

At the County, there are multiple security systems to help protect the internal users from phishing and malware. Mimecast scans all inbound emails and evaluates potential suspicious emails that could negatively impact the computer environment. Zscaler monitors all internet traffic, protecting the County network against phishing and malware attacks.

All computers and fileservers connected to the San Mateo County network must have the most recent version of anti-virus software that has been tested and approved by ISD, installed, and actively running on these devices and configured for daily virus definition file updates. Similarly, all computers and fileservers must be configured to receive updates and patches. Internal vulnerability assessments are also conducted, and all laptops must be protected with full disk encryption.

Election Information Management System (EIMS)

Users can only log in to EIMS if they have a County login and are connected to the County network. Users are assigned roles in EIMS with limited access and rights within the application. A seasonal worker will not be able to view or change certain items while a permanent employee would be able to do so. All changes to records are logged and are auditable.

EIMS servers are County owned and located in secured County buildings. The EIMS application runs on County servers that reside in a secured data center. No election data is stored in the cloud. The EIMS servers' backups are run on a set timetable and the backups are replicated to at least one other site. All servers are running an operating system that is up-to-date and have anti-malware software that is updated on a routine basis.

Vote Center Connections to County Network and EIMS

Commencing with the June 2018 election, San Mateo County will be moving to a new All-Mailed Ballot/Vote Center election model. Vote Centers will be replacing polling places and will require real time connections to EIMS. The Division is working with ISD to ensure that the connections from Vote Centers to the County Network are secure, restricted and stable.

Laptops will be purchased for use only at Vote Centers. Each laptop will login to a Virtual Private Network (VPN) via a username and password. The VPNs will create private, encrypted connections from the Vote Center to the County network. After the VPN connection is created, a user must login to the County network using a unique username and password. All laptop data/drives will be fully encrypted, and each laptop will be trackable via hardware and software when connected to the internet. These features permit the County to locate and disable any lost or stolen laptops.

Once connected, three of the laptops at each Vote Center will only have access to EIMS and a fourth laptop will only be able to access the Secretary of State's (SOS) website for online voter registration. Other websites and email will be blocked.

Vote Centers will not have access to the full EIMS application. The users will be limited in what they can access and change. Users will not be able to download the entire voter registration database.

All unused port and connections on the laptops and other devices will be sealed and/or blocked from use. Laptops will be sealed with tamper-evident seals when not in use and stored in a secure location when not in use.

VoteCal

EIMS is connected to the Secretary of State voter registration database called VoteCal, via a secure point-to-point T1 connection. VoteCal links all the voter registrations databases in the 58 California counties. Voter registration data is sent back and forth between VoteCal and EIMS to update voter status. The County has a security appliance between the County and the SOS that limits what the State connection can do inside the County network. This security appliance also limits who can exit through the T1 line and access the VoteCal data. Only authorized Election staff at Tower Road can access VoteCal.

The county EMS is connected to the VoteCal portal using the router and communication line that is secured by the SOS software. The portal currently connects each county to VoteCal for the exchange of VoteCal batch files by utilizing defined security roles. The EMS vendors work with each county to establish the connection between the EMS and VoteCal for checking voter status statewide.

Many safeguards are in place to protect VoteCal from unauthorized access, intrusion, manipulation, or corruption.

First, VoteCal adheres to industry standard security controls established by the National Institute of Standards and Technology (NIST 800-53r4) and the International Organization for Standardization (ISO 27001).

Second, VoteCal has utilized industry standard best practices to implement recommendations from the Department of Homeland Security (ST16-001) for "Securing Voter Registration Data." These recommendations, which were distributed by the National Association of Secretaries of State Elections Committee, are designed to prevent malicious actors from using a variety of means to interfere with voter registration websites and databases.

Third, VoteCal's database resides on servers located on a secure internal network. VoteCal's data does not reside in a cloud, such as Amazon Web Services, but rather resides locally. Only specific authorized staff from specific machines can access the database. Network safeguards and server hardening/security enhancement techniques have been employed to protect the system from outside intrusion.

Fourth, the SOS conducts routine vulnerability scans and security audits to proactively identify and address security vulnerabilities. In addition, the SOS routinely applies the latest software security patches to ensure that VoteCal remains protected against emerging security threats. The SOS also deploys malware/anti-virus software on infrastructure and end-point devices.

Finally, VoteCal's data is encrypted at rest and in transit. No access exists between the VoteCal public website servers, used for the public website, and the VoteCal database servers, where voter data resides.

Voter Lookup

Voters can verify 24 hours a day, 7 days a week that they are correctly registered via the Voter Lookup tool on the Division's website. The Voter Lookup tool uses Hyper Text Transfer Protocol Secure (HTTPS) which means that all data sent and received is encrypted.

The data for this voter lookup is an extract from the voter registration database servers. The lookup does not have access to live data and the extract only pulls data that is necessary to run the voter lookup.

Voter Data

Voter data may be provided to a candidate for office, a ballot measure committee or to persons or groups for elections, scholarly, journalistic, political or governmental purposes as determined by the SOS. All other requests for voter data are denied.

Voting Tabulation System

San Mateo County uses the Hart Voting System by Hart InterCivic to create ballots, scan ballots, and tabulate the results. Hart equipment is also used at Vote Centers for voters to vote electronically.

Federal Certification of Hart Voting System

The current Hart Voting System version 6.2.1 was certified by the National Association of State Election Directors (NASED) in 2006 under the 2002 Voting System Standards.

To be certified, all systems must undergo rigorous testing to ensure that the voting system meets the standards. Under the NASED, the testing is conducted by accredited independent testing authorities. Testing includes review of the source code, functionality testing, and durability testing. All components must pass the testing for a voting system to be certified. The Hart Voting System underwent multiple rounds of NASED certification and review prior to federal certification.

California Certification of Hart Voting System

The Hart Voting System version 6.2.1 was certified by the SOS for use in California in 2006. At the time, California required that all Direct Recording Electronic (DRE) voting systems used in the state be federally certified prior to state certification. Once a system is certified, any modification must be approved by the SOS.

Testing in California is similar to federal testing. Equipment and software are sent to a third-party lab, which tests items including hardware, software, security, and quality assurance. The SOS holds a public hearing and requests comments when testing is completed. The certification is then approved or denied.

Top-to-Bottom Review

In 2007, the SOS conducted a top-to-bottom review of all voting systems certified in the state. The review was supervised by University of California computer scientists. After the review, approval for use was withdrawn for all voting systems including Hart. Voting systems were then conditionally reapproved for use under strict security requirements and use conditions. San Mateo County has complied with all the security requirements and use conditions.

Symantec Review

In 2003, Hart engaged Symantec to perform a security risk assessment and a review of the development process of the Hart Voting System. Because of the assessment, Hart made significant changes to the system code and the development process. Improvements which were incorporated and are in the version used by San Mateo County include triple redundant storage of vote records, user account management and password storage, digital signatures of ballots, and two factor authentication.

San Mateo County Security of Hart Voting System

The following methods are employed to secure and protect the County’s voting tabulation systems and equipment.

No Internet or County Network Connections - Hart equipment is never connected to the internet or the County network. It is not connected to the Voter Registration system.

Hart Software - Computers that have Hart software are all password protected. Passwords are changed every election. Users have defined roles as well as passwords for each application. Critical data is encrypted.

All Hart software keeps audit logs. Hart software is not updated unless the update has been certified by the SOS. Two “computer hash” programs are run, prior to and following elections to ensure that the certified version of the software was used and to prove that the software used has not been altered.

Voting Equipment

The Hart voting equipment used at Vote Centers consists of a Judge’s Booth Controller (JBC) and eSlates with Verifiable Ballot Options (VBOs). One JBC is used in combination with multiple eSlates and VBOs at each voting location. The VBOs create a Voter-Verified Paper Audit Trail. A paper record is printed before a voter finishes casting his/her ballot. The voter verifies that the paper record matches his/her electronic ballot. The paper record is kept with the voting machine in the VBO and ultimately stored in the Elections secured facility for the required retention period.

After the vote is cast, the vote is stored in four locations: on a memory card in the JBC; internally on the JBC; internally on each eSlate; and on the paper record in the VBO making lost data or undetectable fraud virtually impossible. After the election, the number of votes on all equipment is verified and reconciled.

Time-stamped transaction logs are created for every system action related to the voting process.

The eSlate has no external port or openings that could create a breach in the system’s security that might provide access for people seeking to tamper with it. The eSlate also uses a Select Wheel, not a touch-screen, which eliminates the need for calibration at each election and the possibility of mismarked ballots.

Voting Equipment - Pre-Election Processing - All voting equipment is reset and tested prior to an election and the software version is confirmed. Logged tamper-evident seals are placed in multiple locations to show that the equipment has completed testing. Equipment is assigned to a specific Vote Center and the serial numbers are logged and tracked.

Voting Equipment from Warehouse to Vote Centers - All voting equipment that is sent out to voting locations is scanned and logged in our electronic inventory system. In addition, equipment remains sealed with the logged tamper-evident seals. Equipment is stored in secured locations between the time delivered and used. Detailed logs are kept of who takes custody of the JBCs and the ballots.

Voting Equipment Use during Voting Period - Seal numbers are checked before the equipment is used and compared to the seal numbers that were logged prior to leaving the warehouse. If the seal numbers do not match, the equipment is not used.

All equipment is within sight of staff at a Vote Center while also maintaining the privacy of voters. Staff is instructed to immediately report any suspicious incidents or if tampering is suspected. Poll workers keep a log of any incidents for future reference, which are stored in a secure place for the required retention period.

The Hart voting equipment creates time-stamped transaction logs for every system action related to the voting process. All machines are sealed at the end of the day and the seal numbers are verified at the start of the next day. Ballots and JBCs will also be stored in a secured location.

Voting Equipment on Election Night - On Election Night, the JBC and all paper ballots are returned to the Elections Division. Chain of custody documents track who picked up the equipment. Seals are checked at the Elections Division to confirm the JBC was not tampered with in transport. Equipment that is left at the Vote Centers is sealed for delivery back to the warehouse.

Computer Tally Room for Ballot Creation and Vote Total Reporting

The Hart software for creating the ballot and tallying the votes is in the Computer Tally Room at the Elections Division. This is a physically secure, video-surveilled room that requires a card key entry and compliance with the "two-person integrity" rule (i.e., the presence of at least two employees at all times). Staff must sign a log sheet each time they enter or exit the Computer Tally Room in addition to badging in. Large windows allow everything done inside to be observed.

All staff actions within the Hart software application are logged and any changes made can be traced back to unique user identifications. All databases used to create the ballot and tally the votes are backed up at specified times to external hard drives.

Vote by Mail

The Vote by Mail procedures also require that two (2) employees be present at all times when voted ballots are being handled or stored.

All computers used to scan ballots are password protected and keep audit logs. The software creates a ballot image after ballots are scanned. The databases with the images are backed up daily.

All scanned ballots are verified to make sure they were properly scanned. Ballots where voter intention is not clear are flagged in the software. These ballots include overvotes, undervotes, damaged ballots, and write ins. Two staff members work together on these flagged ballots to determine voter intent.

Election Results

Election results are reviewed by multiple staff and are posted in multiple formats (PDF, HTML, text, and RaceTracker) for the community on the Elections Division's secured website. The source of the election results data is maintained at the Elections Division's secured facility. Any attempt to alter the posted election results would require breaching the security of all four reporting formats. The hard copy of the results printed directly from the Hart software is compared by multiple people to the results posted at specified times on Election Day.

1% Manual Tally

Prior to an election being certified, a 1% manual tally is required. During the tally, a random 1% of precincts in the election are selected and all the votes in those precincts are hand counted including the paper records for the eSlates. Any discrepancies between the manual count and the electronic count must be resolved before the election can be certified. In the 10 years that San Mateo County has used the electronic voting machines, there has never been a discrepancy between the electronic and manual count for the eSlates.

PHYSICAL ASSETS

Registration and Elections Division Facility

All voting equipment and databases are located at the Elections Division's facility, which has a security system with cameras. Access to the voting equipment warehouse, voter registration database servers, and the Vote by Mail area is restricted to staff with card keys, which create audit trails. The voter registration servers are located behind locked doors with very limited access.

All visitors must sign in at the front counter and are escorted at all times by a staff member.

Human Resources / Elections Staffing

All new staff are fingerprinted and background-checked. There is rigorous staff training to mitigate risks and cybersecurity breaches. Staff are required to complete an information security class each year.

Elections staff follow an on-boarding procedure for new staff, assigning roles and security rights. When staff leave, off-boarding procedures terminate computer system and building access immediately.

ELECTIONS CYBERSECURITY - ONGOING NEEDS

The resiliency and success of our cyber defense systems depends on a continuous and ongoing commitment to deploy only the very best technologies and personnel at all levels of our defense network. It is important that we recognize the high level of sophistication and resources deployed by malicious nation actors and hackers. Many of these nations spend a significant portion of their resources investing in cyberwarfare. It is essential that our efforts at the local level, not only be well coordinated, but funded with adequate resources to counterbalance those threats. A well-funded and coordinated approach to cyber defense requires the efficient allocation of assets, people, information, technology, and facilities.

A well rounded and defined cyber defense program includes the following components:

1. Cybersecurity Assessments
2. Cyber Resilience Reviews
3. Vulnerability Assessments
4. Incident identification and management
5. Service Continuity
6. Risk Assessment
7. Phishing Campaign Assessments
8. External Dependency Assessment
9. Training and Education
10. Situational Awareness
11. Validated Architectural Design Reviews
12. Coordinated Multi Agency Networking
13. Facility Security Assessment and Improvements

The above will be the subject of a separate report in consultation with agencies at the federal, state and local levels.

SHARED VISION 2025

Careful consideration of this report contributes to the Shared Vision 2025 outcome of a Collaborative Community by ensuring the voters of San Mateo County have confidence in the voting systems used.

CONCLUSION:

The threat of cyberattacks from malicious actors are very real and an ever-increasing danger to voting systems. The sophistication of these cyberthreats threaten the very core of the United States critical infrastructure including transportation systems, power grids, water supplies and nuclear power plants. The Department of Homeland Security designation of the nation's election infrastructure, as critical infrastructure, was a vital first step in the defense of our election systems. Much still needs to be done in this ongoing battle to defend our election infrastructure and democracy.

Today's national, political and technological environments mandates that we take an intelligent, aggressive and well-funded approach to cyber defense. Cyberwarfare is real and we are the front line of this war on our democratic process and institutions.

San Mateo County voters can be assured that every effort will continue to be made at all levels of government, to protect the County's election infrastructure through a well-funded coordinated approach utilizing cutting-edge cyber defense technology and security protocols.