DRAFT: Overview of San Francisco Election System Security

September 13, 2019

To preserve the integrity of elections and election results, the City, the Department, and the City's voting system vendor utilize multiple methods and layers of protection that are continually reviewed, updated, and improved.

I. Results Verification

The Department verifies the accuracy of the voting system throughout the election cycle.

A. The City's voting system is paper-based so that all votes are cast using paper ballots which creates a verifiable, auditable record of the votes cast in every contest and ballot measure.
B. Before every election, the Department conducts logic and accuracy testing on all tabulation equipment used in all polling places as well as the scanners located in City Hall primarily used to tabulate vote-by-mail ballots. During logic and accuracy testing, pre-marked paper ballots or voting scripts are entered into the voting equipment to compare the system's report of results against the expected outcomes.
C. During the election cycle, the Department conducts daily testing on central scanners located in the Department's City Hall office to verify that each unit continues to accurately record votes from each contest and measure on every ballot card.
D. Following every election, the Department conducts a manual count of the ballots cast in a number of precincts equaling one-percent of the City's total number of precincts used for an election. The Department randomly selects the precincts in a public process that is streamed live to the Department's website. The results of the manual counts are compared to the results from the machine counts to verify that the equipment properly captured votes from the ballot cards.
E. Starting with the November 2019 election, the Department will implement post-election risk-limiting auditing either on a small sample size of vote-by-mail ballots or as an audit to incorporate into the official canvass. The Department is seeking methods that allow the inclusion of ranked-choice voting contests in risk limiting audits.

II. Voting System Security

A. The security of the tabulation system's network and workstations are based on multiple strategies.
    1. The tabulation system network is air gapped. The entire system of server, network switch, workstations, and voting equipment are not connected and are *never* connected to the general City network, internet, or any other unsecured network.
    2. The network switch is secured at all times in an access controlled, central tabulation room, enclosed within a security cage, and connected only to an air-gapped network.
    3. The tabulation system devices do not communicate or function using any wireless technologies.
    4. Non-routable IP address ranges are used on the internal private air-gapped network.
    5. Strong system component passwords are changed before each election.
    6. The tabulation system integrates AES for cryptography (data confidentiality), digital signatures SHA-256 and HMAC for data signing (data authenticity and integrity).
    7. After initial installation and acceptance testing, all passwords on all workstations, as well as BIOS passwords, are changed and customized by the Department and provided on a limited basis to authorized personnel.
B. Wireless connectivity functions are not available on any of the voting system devices.
C. The voting system was reviewed and tested by a test laboratory accredited by the U.S. Elections Assistance Commission. The voting system was also reviewed and tested and approved for use in California by the Secretary of State's Office of Voting Systems Technology Assessment.

III. Tabulation System Components

D. The City's tabulation system consists of:
   1. A database server used for creating election media and security keys.
   2. A second database server to be used for tabulation and adjudication.
   3. A third database server designated as a backup server.
   4. Network switches.
   5. Election management system tabulation and reporting workstations.
   6. Adjudication workstations.
   7. Central scanners and workstations.
   8. Ballot marking devices.
   9. Ballot scanning devices located in polling places.

IV. Department Processes that Protect Election Integrity

A. The Department updates custody transfer protocols before elections to identify the movement and possession of voting equipment and ballots during the election cycle.

B. Beginning with the November 2019 election, the Department will post on its website the ballot images of voted ballots for public viewing. Each of the posted ballot images will include an audit record that states how the system counted every vote marking on the ballot.

C. Also beginning with the November 2019 election, the Department will post the transaction logs exported from the voting equipment used at the polling places and from the equipment used in City Hall to process vote-by-mail ballots to verify that the equipment operated accurately.

D. The voting system tracks the votes tabulated for each contest and measure from each ballot card and then produces a "cast vote record" in JSON format that lists this ballot content. The Department will post the cast voter records on its website.

E. The Department will continue to apply SHA-512 cryptographic hashing to all results reports. The Department will also apply hashes to all transaction logs and cast vote records associated with the November 2019 election that the Department will post on its website.

F. The Department places no personal information that identifies specific voters in relation to the website applications that are public facing to protect voters' personal data from unauthorized access.

G. The Department implements and mirrors the security-related best methods recommended by:
   1. San Francisco Citywide Cybersecurity Policy.
   2. Office of Elections Cybersecurity and Enterprise Risk Management, California Secretary of State.
   3. U.S. Department of Homeland Security.
   4. National Institute of Standards and Technology (NIST).
   5. Election Assistance Commission (EAC).

H. The Department continuously monitors the most recent security recommendations and threat research via alerts from US-CERT, MS-ISAC, EI-ISAC, and the City's Cybersecurity team.

I. The Department's designated personnel participate in bimonthly citywide cybersecurity working groups to review best practices that the Department can implement.

J. The Department has implemented many physical security measures associated with the tabulation system as well as to support election integrity:
   1. The room containing the tabulation system remains locked when ballot processing is not occurring.
   2. Specific personnel are assigned a personal identification number (PIN) to access keypad locks before obtaining entry to the room containing the tabulation system.
   3. Security cameras monitor tabulation equipment stored at the department's warehouse and any after-hours movement or intrusion is immediately communicated to the director.

4. All servers and switches are located within an access controlled, central tabulation room, and enclosed within a security cage to prevent unauthorized access to the equipment.
5. During the election cycle when tabulation equipment is tested and prepared for delivery to the polling places, several webcams stream these activities on the Department's website for public viewing.
6. Multiple security cameras, monitored by the San Francisco Sheriff's Department, are present in City Hall and outside of the area in which central tabulation occurs (Department's computer room).
7. The Department uses webcams to stream to its website the activities associated with central tabulation, ballot sorting, ballot extraction and ballot remake processes.
8. From the time the Department receives ballots during an election cycle, a minimum of two people must be present in any room containing ballots, whenever entering such rooms for any reason.
9. All rooms containing ballots, including the central tabulation room, are sealed with tamper evident seals when no ballot processing is occurring such as after hours.

V. Election Management System (EMS)

A. The EMS requires role-based access controls for all software and hardware components.
B. The closed network communications among client workstations and servers are protected through encryption and signing.
C. Users of the Adjudication system are assigned roles within the Adjudication application. The Administrator defines the actions granted to users when defining the conditions during election setup for reviewing ballot markings.
D. EMS Database – Election Data
   1. Election data for a given election project is stored within the EMS Database server. To protect against the malicious modification of this data, the EMS platform implements EMS Database data integrity and consistency controls. Every election project database record is signed, or hashed, which allows for consistency checks within the EMS platform.
   2. The EMS database files are stored under the encrypted disk drive(s). The encryption platform utilizes an NIST-certified hardware-based cryptographic engine which provides real-time encryption and decryption of data using AES-256 algorithms. In addition, the encrypted storage platforms provide access control using physical security tokens that establishes multi-factor authentication. Without these tokens, and the corresponding passwords, the system remains locked and cannot function.
   1. Adjudication Data
      a. The system ensures the integrity and confidentiality of data transferred between the services and clients using a shared application key in the form of an X.509 PKI key (a Public Key Infrastructure key in the standard X.509 format). The key is used to encrypt (and therefore, ensure the privacy of data) and sign (thus ensuring the integrity and authenticity of data) all data transferred between system components.
      b. Data stored in the database is protected by access control. Only the user account running the services has access to the Adjudication databases. Adjudicated result files are protected by signing and encryption.
E. Anti-virus protection
   1. Anti-virus software is enabled on all server and client machines with heuristic virus checking rules activated.
   2. The virus prevention/detection packages are consistently updated to the latest version of the application and virus/spyware definition databases every week.
   3. Updates are introduced via a mobile storage device since no external access to the network is permitted.
   4. A reformatting laptop is used to scan all media for viruses prior to inserting the media into the election definition or reporting and tabulation systems.

VI. Central Scanners and Workstations

1. User accounts are created for specific personnel to access the central scanning workstation and to operators according to the features required to perform their functions. Credentials are in the form of a user name and password. The password is a secret for the keyed HMAC algorithm, and the digest value (result of keyed hash one-way function) is stored in the physical security token.
2. Physical security tokens are used for multi-factor authentication on the machines and are programmed with a signing key, username and password hash.
3. All operators use a workstation security token reader to log in with usernames and passwords that use hashed values to unlock the system.

VII. Accessible Ballot Marking Devices (BMD)

A. All of the City's accessible BMDs produce a paper ballot with a QR code that stores the voter's selections and a voter verifiable record of those selections made by the voter.
B. The information in the QR code is encrypted so that the data remains consistent from the time the voter prints the ballot until the ballot is scanned.
C. The BMDs are standalone units that do not communicate on any wired or wireless network.
D. Election setup using data from the EMS platform is achieved using USB flash drives. The data on the USB flash drives is encrypted.
E. The BMDs log all activity on the device in the systems event log that the Department will also post on its website to provide the public with a transparent record of all BMDs operations.
F. Only authenticated users with valid smart cards can access the ballot marking devices. System authentication is comprised of smart cards which require a valid PIN to unlock encrypted data on the card.
    1. Smart card contents utilize an election identifier (GUID) unique to the election for which they are programmed and are unique to the election.
    2. The BMDs require technicians and poll workers to enter the appropriate password, or PIN, to activate the smart cards. To protect the contents of the smart cards, the login information is hashed and the system allows no more than five attempts to unlock the card contents. After the fifth attempt the smart card is invalidated and the card must be reprogrammed using the EMS, which apply separate hash values to the EMS' login credentials.
G. The BMD uses two types of smart cards:
    1. Tech Advisor - Used to configure the device and load election files, and cannot be used while the poll is open
    2. Poll worker - Used to open poll and export logs, and cannot load election files.
H. No voter information or records of votes cast are stored on the BMDs.
I. All of the access panels to the BMD are sealed with tamper-proof seals and wire seals to prevent unauthorized access to the device.
J. All seals contain serial numbers that are unique to each seal and that are assigned to specific pieces of equipment, recorded on log sheets, and then verified prior to use by election workers and poll workers. If the serial numbers do not match the numbers recorded for a particular piece of equipment, or are broken, poll workers are instructed to inform the Department's director who decides the disposition of the equipment.

VIII. Ballot Scanning Machines (BSM)

A. BSMs are precinct scanners and are standalone units that do not communicate on any wired or wireless network.
B. The uploading of election setup and result files into the precinct-level BSMs uses compact memory flash memory cards that contain encrypted data obtained from the EMS platform
C. During the voting session, BSM devices constantly keep and update system auditing reports which the Department will post on its website for public review.
D. The BSM is encased in a hard shell, which protects the internal components of the machine from damage.

E. Tamper-proof screws are used for all external fixturing.
F. Each device door is secured with an appropriate locking mechanism (hasp-type for either physical locks or tamper seals and security screws).
G. The BSM uses built-in circuits on their motherboards that are powered by coin cells and have a microprocessor to separately record every instance any door or cover is physically opened. Each tamper switch is tripped when a door or cover is opened. There are eight such switches positioned inside the machine. (This section needs to be explained more clearly for audience comprised of the general public).
H. The plastic ballot box has security locks for both the main and auxiliary compartments. The auxiliary compartment is only accessible through the main compartment door.

IX. Security of Voter Registration Systems

A. All California counties' local registration systems are connected to VoteCal, a statewide voter registration database administered by the Secretary of State's Office. The counties registration systems constantly communicate with VoteCal using a private and secure Intergovernmental Network (IGN). This continuous connection is necessary to maintain near real-time registration records in sync amongst the counties and VoteCal.
B. VoteCal is maintained by SOS IT personnel using state of the art equipment and following best practices developed in the IT community.
C. The Department's local registration system (EIMS) resides on the Department's internal network. Voter data is protected via role-based access controls.
D. The Department routinely monitors local systems for any patches that require installation.
E. The servers on which the registration systems reside are located in a secure, locked room that require a PIN code to enter. The servers have virus and malware protection that the Department regularly updates.
F. The Department's local registration system is not directly connected to the internet and is protected by a firewall, which reduces the system's vulnerability to SQL injection attacks.
G. The Department manages several web applications, such as "Voter Registration Status Lookup", "Ballot Status Lookup", "Polling Place Lookup", among others on an offsite server, sfelections.org. These web applications interface with a replicated server with a subset of registration-related data that have no direct internet connection with the Department's production server.

X. Security of the Department's Website

A. The Department's web applications that provide voters information such as the status of their vote-by-ballot, provisional ballot, registration record, and polling place locations reside on an offsite server, sfelections.org, and are protected by Cloudflare, which offers multiple security functions:
    1. Caches information from the host server onto multiple alternative servers so that users never directly access the host server.
    2. Prevents attacks on the host server that seek to obtain voter information.
    3. Ensures the sfelections.org website itself is not attacked since Cloudflare uses a distributed network of servers that remain online and performing optimally during peak times.
    4. Prevents website defacement that can result from brute force login attacks, which prevents the Department's site from providing inaccurate information.
    5. Protects against denial of service attacks since data is replicated on multiple servers to reduce the effects from a concentration of requests that degrade responsiveness. Additionally, upon receiving repetitive requests, Cloudflare blocks the associated IP addresses across its system.
    6. Provides automated security monitoring and network intrusion protection for the Department's website.
B. The software operating the Department's applications is continually updated and the most recent patches are installed.

C. The Department's website hosted on the City's servers, sfgov.org, hosts the Department's static content associated with such subjects as being a poll worker, outreach activities and materials, how to register to vote, and vote-by-mail voting is protected by Pantheon that provides multiple security functions similar to those employed by Cloudflare.
D. The Department conducts penetration testing to audit the security posture of its website, including all applications, forms, and tools.

XI. City's Unified Cyber Command

A. The City's Department of Technology operates a Unified Cyber Command to continuously monitor technologies to protect the City's systems and networks.
B. The Unified Cyber Command utilizes cyber alarms installed in department networks, servers, and workstations.
C. The cyber alarm definitions are frequently updated based on information assessed worldwide regarding attacks and infections.
D. A managed detection and response (MDR) service actively monitors the City's networks in real time and proactively assesses systems for both known and previously undetected threats, applying such assessments with a nation-state level catalogue of threats.
E. The MDR employs analysts around the clock who track thousands of known threat actors, including those sponsored by nation states.
F. When the MDR identifies an attack on any of its monitored networks the MDR then assesses other networks under its monitoring for indications of similar attacks, and also provides methods to prevent similarly identified attacks on the other networks.

XII. California Secretary of State[1]

A. Before certifying voting systems for use in California, the SOS reviews the systems' source code and organizes "red team" testing involving experts who seek methods to comprise the systems. Additionally, the SOS conducts functional testing, volume testing, and testing to determine whether systems meet criteria associated with accessibility.
B. The SOS implemented social media monitoring software to assess attempts to propagate misinformation regarding elections and to respond to such attempts with public education.
C. The SOS interacts with federal, state, and local agencies, including the Department of Homeland Security, Federal Bureau of Investigation, California Department of Technology, California Office of Emergency Services, and the California Highway Patrol regarding security matters.
D. The SOS maintains an email account specific to the reporting of possible attempts to propagate election-related misinformation: VoteSure@sos.ca.gov.

1. California Secretary of State website: www.sos.ca.gov/elections/ovsta/security