Attachment 2

CITY AND COUNTY OF SAN FRANCISCO
DEPARTMENT OF ELECTIONS
John Arntz, Director

DRAFT: Overview of San Francisco Election System Security

August 16, 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. Tabulation System

A. The City's tabulation system consists of:
   1. A primary database server to be used for tabulation and adjudication
   2. A secondary database server to be used for backup of critical tabulation and adjudication activities
   3. Network switches
   4. Election management system tabulation and reporting workstations
   5. Adjudication workstations
   6. Central scanners and workstations

B. The system and all of its components exist on a standalone, air-gapped network (*a network security measure employed on one or more computers to ensure that a secure computer network is permanently and physically isolated from unsecured networks, such as the public Internet or an unsecured local area network*[1]).

C. The voting system and all related devices are never attached to another network, including the internet and the City's network.

D. Wireless connectivity is not available on any of the voting system devices.

E. The voting system that the Department operates was reviewed and tested by a test laboratory accredited by the U.S. Elections Assistance Commission. The voting system was also reviewed and tested for approved for use in California by the Secretary of State's Office of Voting Systems Technology Assessment.

II. Voting System Security Checks

The City's voting system has several checks in place to ensure the integrity of election results.

A. The City's voting system is paper-based and all votes are counted using paper ballots.

B. Before every election, the Department conducts logic and accuracy testing on all tabulation equipment used in all polling places and the scanners located in City Hall primarily used to tabulate vote-by-mail ballots. During logic and accuracy testing, pre-marked 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 the City Hall scanners (Image Cast Central scanners) to ensure each unit continues to accurately process votes from each 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 on the Department's website. The results of the manual counts are compared to the results from the machine counts to again assess that the equipment properly captured votes from the ballot cards.

E. The Department has implemented many physical security measures associated with the tabulation system as well as to support election integrity in addition to live-streaming operational activities to increase public transparency of elections.
   1. The room containing the tabulation system is continuously locked with keyless locks that require a multi-digit pin number to access the room.

2. Security cameras monitor tabulation equipment stored at the department's warehouse and any after-hours movement or intrusion is immediately communicated to the director.
3. 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.
4. 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).
5. The Department uses webcams to livestream from its website the activities associated with central tabulation, ballot sorting, ballot extraction and ballot remake processes.
6. 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.
7. 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.

F. 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, and computers 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, containing only an air-gap network connection.
3. The tabulation system devices do not communicate 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 a minimum of every 90 days.
6. The tabulation system integrates AES for cryptography (data confidentiality), digital signatures SHA-256 and HMAC for data signing (data authenticity and integrity).

G. Election Management System (EMS)

1. The EMS requires role-based access controls for all software and hardware components.
2. Network communications between the client and server are protected through encryption and signing.
3. Users of the Adjudication system are assigned roles within the Adjudication application. The Administrator defines the actions that users are able to interact with by defining the Outstack Conditions during election setup.
4. EMS Database Election Data
    - a. 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, which allows for consistency checks within the EMS platform
    - b. 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 the access control through using physical security tokens. Without these tokens, and the corresponding passwords, the system cannot function.
5. Adjudication Data
    - a. The system ensures the integrity and confidentiality of data transferred between the services and clients by making use of 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.

6. Anti-virus protection
   a. Anti-virus software is enabled on all server and client machines with heuristic virus checking activated.
   b. The virus prevention/detection packages are updated to the latest version of the application and virus/spyware definition databases every week.
   c. Updates are introduced via a mobile storage device since no external access to the network is permitted.
   d. Servers are locked in racks and behind, which are enclosed behind a fence in the computer room, with entry using a PIN code, to which specific personnel have access.
7. Central scanners and workstations
   a. User accounts are created for users accessing the central scanning workstation 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.
   b. The operator uses a workstation security token reader to log into the system.
   c. Physical security tokens are used for multi-factor authentication on the machines and are programmed with a signing key, vector, username and password hash.
8. Accessible ballot-marking device (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 disks. The data on the USB flash disks is encrypted.
   e. The BMDs log all activity on the device in the systems event log.
   f. Only authenticated users with valid smart cards can access the ballot making devices. System authentication is comprised of smart cards which require a valid PIN to unlock encrypted data on the card.
      i. Smart card contents utilize an election identifier (GUID) unique to the election for which they are programmed and are unique to the election.
      ii. The password (PIN) for technician and poll worker smart cards protect the contents of those cards and are stored via a hash. If more than five attempts are made to unlock the card contents with and incorrect PIN, the card must be reprogrammed via the EMS.
   g. There are two types of smart cards:
      i. Tech Advisor - Used to configure the device and load election files, and cannot be used while the poll is open
      ii. 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 recorded and then verified prior to use by election workers. If the serial numbers do not match the Department's records or are broken, poll workers are trained to inform the director who decides whether the machine needs to be replaced.
9. Ballot Scanning Machines (BSM)
   a. BSMs are precinct scanners and are standalone units that do not communicate on any wired or wireless network.
   b. Election setup and result file loading using data from/to the EMS platform and precinct-level BSM is performed only through compact flash memory cards. The data on the compact flash cards is encrypted.
   c. During the voting session, BSM devices constantly keep and update system auditing reports.

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. Built-in circuits on the motherboard are powered by a coin cell, with a microprocessor to separately record every instance where the unit is physically opened. Each tamper switch is tripped when the protected devices access door is opened. There are eight such switches positioned inside the machine.

h. The plastic ballot box has security locks for both the main and auxiliary compartments. The secondary compartment is only accessible through the main compartment door. The coroplast ballot box is sealed during use.

III. Security of Voter Registration Systems

A. All California counties's local registration systems are connected to VoteCal, a statewide voter registration database administered by the Secretary of State's Office. The counties constantly communicate with the statewide system via a private and secure Intergovernmental Network (IGN). This continuous connection is necessary in order to receive new registrations and keep the two systems in sync.

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[2].

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.

IV. 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 on 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.
6. Provides automated security monitoring and network intrusion protection.

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.

V. City's Unified Cyber Command

A. The City's Department of Technology operates a Unified Cyber Command to continuously monitor technologies to protect systems such as websites.

B. The Unified Cyber Command utilizes cyber commands installed in Department networks, servers, and workstations.

C. The cyber alarms are frequently updated based on information assessed worldwide regarding attacks and infections.

D. A Managed detection and response (MDR) service that 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.

VI. California Secretary of State[3]

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.

VII. Additional 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 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 markings 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 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 and will begin hashes to all transaction logs and cast vote records with the November 2019 election.

F. For results from vote-by-mail ballots from the November 2019 election, the Department will implement post-election risk-limiting auditing either as a trial case on a small sample size 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.

G. The Department places no personal information of voters in applications that are public facing protect such data

H. 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)

I. 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.

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

[1] "Air gap (networking)" *Wikipedia: The Free Encyclopedia*. Wikimedia Foundation, Inc. 22 August 2016.

[2] "Foreign hackers broke into state election systems" *Politico*, 29 August 2016.

[3] California Secretary of State website: www.sos.ca.gov/elections/ovsta/security