DEAN C. LOGAN
Registrar-Recorder/County Clerk

September 19, 2016

TO: Supervisor Hilda L. Solis, Chairwoman
Supervisor Mark Ridley-Thomas
Supervisor Sheila Kuehl
Supervisor Don Knabe
Supervisor Michael D. Antonovich

Sachi A. Hamai, Chief Executive Officer

FROM: Dean C. Logan, Registrar-Recorder/County Clerk

2016 PRESIDENTIAL GENERAL ELECTION INFORMATION SECURITY PREPAREDNESS

This memorandum is intended to notify your Board of the measures the County currently has in place to ensure its cybersecurity preparedness for the November 8, 2016 Presidential General Election.

Recent media reports of voter registration system security breaches have raised concerns nationwide regarding the cybersecurity of critical elections infrastructure. We received sensitive communication from the Federal Bureau of Investigations (FBI) regarding known cybersecurity threats to voter registration systems. Additionally the U.S. Election Assistance Commission (EAC) has issued a security checklist to State and local election administrations regarding voter registration data. We have confirmed the County's compliance with all federally recommended measures. We have attached this correspondence for your review.

With respect to cybersecurity preparedness for elections, there are two important points to remember.

1. Cybersecurity is no different for elections than it is for other critical sectors, including healthcare, public safety, or financial services. The best cybersecurity practices adopted by IT professionals across the spectrum of government and industry are equally applicable to elections administration.

2. Cybersecurity involves several layers of protection against attack, including physical security, general IT security protocols, and system-specific security features. Each of these layers is present in the cybersecurity defenses protecting the County's elections infrastructure, and each involves people and processes in addition to hardware, software, and facilities.

Department IT staff work regularly with IT professionals from the Internal Services Department (ISD) and 3rd party vendors with expertise in cybersecurity, to ensure the security, integrity and availability

of the critical election IT assets highlighted below.

Website and Network

All public-facing departmental websites, as well as the enterprise network, are protected and monitored 24/7 for malicious attacks by intrusion detection software and teams of dedicated IT professionals. The Department's public-facing web applications have been tested for security vulnerabilities and identified risks and weaknesses have been mitigated.

Voter Registration System

The Department's DIMSNet voter registration system is not public-facing and is not connected to the Internet. Voter registration data made available to public-facing web applications are read-only copies that cannot adversely affect the integrity of the eligible voter rolls. Application security and user roles strictly control employee access to the system and its various modules.

Voting Devices

The Precinct Ballot Reader (PBR) devices deployed in the polling places to support Help America Vote Act (HAVA)-compliant voting are physical secured with tamper-evident seals, and are never connected to the Internet nor to each other, reducing the likelihood of a malicious attack. Most importantly, they do not count the votes on the ballots, so a security threat to a device would not affect the tally of election results. The function of these devices is to check for over-votes and blank ballots.

Tally System

The Microcomputer Tally System (MTS), which reads and tallies the votes and generates election results, is housed in a highly secured room within the Department's headquarters in Norwalk. MTS operates on an isolated token ring network and has no Ethernet connectivity to the local or enterprise networks.

Finally, it should be noted that all of these election IT assets are protected by a physical security layer of security guards, surveillance cameras, intrusion detection alarms, and keycard access controls, as well as a regular regimen of best practice IT security protocols.

Please refer to the attached Cybersecurity Preparedness Fact Sheet for more details.

If you have any questions, please contact me at (562) 462-2716, or your staff may contact Jeramy Gray, Assistant Registrar-Recorder/County Clerk at (562) 462-2714.

DL: JG: fp
Attachment
c: Executive Office, Board of Supervisors
RR/CC Board Deputies
County Counsel
Internal Services Department

Cybersecurity Preparedness Fact Sheet
Los Angeles County Critical Election Infrastructure

Website and Network

Dedicated Internal Services Department (ISD) and RR/CC IT Security professionals actively monitor potential threats to the County's enterprise network and to RR/CC's website (LAVote.net). The web servers and database servers are located on the ISD eCloud environment where monthly Operating System and Application patching is managed by a team of IT professionals. In addition to the routine security scans and security patching, LAVote.net environment utilizes the following security technologies, protocols, and architecture:

- ISD's Advanced Cyber threat analytics and analysis solution that is actively monitored by both ISD and third-party cyber security professionals.
- ISD's Enhanced Web Application Firewall (WAF) which actively monitors for and mitigates threats to the Lavote.net web servers.
- Transport Layer Security encryption to secure communications between the server and browser for web applications that pass sensitive data.
- Robust Data Architecture that isolates the data access layer from the public facing web servers. This software architectural design removes direct database access from the web servers and utilizes stored procedures that eliminates the risk of SQL injection attacks.

Voter Registration System

DIMS is the County's voter registration database and election management system. The system is hosted within a secure private infrastructure and is not connected to the Internet. DIMS has an external interface with California's statewide voter database called VoteCal. This interface consists of a secure private point-to-point connection. Application security is integrated with industry-standard network operating system security protocols to control and authorize access to the system. Roles are used to ensure access is limited to only those DIMS modules and functions that fit the user's duties and responsibilities. System security logs are regularly audited to detect and prevent unauthorized system access.

Voting Devices

The Precinct Ballot Reader (PBR) used in the polling places to support HAVA-compliant voting is a stand-alone system that is never connected to the Internet.

- When PBRs are loaded with election data at the Election Operations Center, an "air gap" exists between the switch and hub network that allows multiple PBRs to be loaded simultaneously from a single laptop and the Department's Local Area Network (LAN). The laptop loads data from a secure, encrypted file on CD.

- Prior to being deployed to the precincts, PBRs are secured with tamper-evident seals making it impossible to access a PBR's computer or Ethernet port without detection. Moreover, PBRs are not connected to each other, so any malicious attack on a PBR in the field would be limited to that specific device.
- All PBRs are inspected for evidence of tampering, both in the polling place by poll workers, and by department staff when they are returned to the Election Operations Center.

Tally System

The Microcomputer Tally System (MTS) reads the InkaVote ballots, counts the votes on Election Night, and reports the totals on an isolated token ring network with no Ethernet connectivity to the department's LAN. The server that handles the periodic exporting of election results is fed directly to an Election Contest and Ballot Management System (ECBMS) workstation using a mono-directional RS-232 serial port. While MTS is running, the port is locked for single application use, so no other applications can access the port for purposes of malicious attack.

General IT Security Protocols

In addition to system specific security protocols, the department also practices the following general security protocols per Board Policy:

- Routine application of patches and virus detection software updates to ensure protection from known vulnerabilities
- Requirements for strong passwords that must be changed every 90 days
- Periodic review of access permissions at all levels to ensure compliance with policies and procedures
- Restricted access to the data center, telecommunications closets and keycard access controls to the various areas of the department
- Holding of an annual security awareness campaign to publicize the importance of practicing information security to the general user community

Physical Security

The County's information technology assets supporting election operations reside in County facilities with a very high degree of physical security. These facilities include RR/CC headquarters in Norwalk, the Election Operations Center in Santa Fe Springs, and the ISD Data Center in Downey. Each of these facilities employs 24/7 video camera surveillance, intrusion detection and alarm systems, restricted keycard access, and on premise security. On Election Night, access to the various floors and rooms of RR/CC headquarters in Norwalk is controlled through badge identification of all people in the building and Sheriff's Deputies deployed throughout the building. All voted ballots are transported from polls to check-in centers by two-person teams of poll workers, and from check-in centers to RR/CC headquarters by Sheriff's Deputy Patrol Units.