Tenex Software Solutions Precinct Central 4.0 Electronic Poll Book System Security and Telecommunications Test Report for California

TEN-18001SECTR-01

Prepared for:

Vendor Name	Tenex Software Solutions
Vendor System	Precinct Central 4.0

Prepared by:

4720 Independence St.
Wheat Ridge, CO 80033
303-422-1566
www.SLICompliance.com

Accredited by the Election Assistance Commission (EAC) for Selected Voting System Test Methods or Services

Revision History

Date	Release	Author	Revision Summary
May 5th, 2018	1.0	*M. Santos, J. Peterson*	Initial Release

Disclaimer

The information reported herein must not be used by the client to claim product certification, approval, or endorsement by NVLAP, NIST, or any agency of the Federal Government.

Trademarks

- SLI is a registered trademark of SLI Compliance.
- All products and company names are used for identification purposes only and may be trademarks of their respective owners.

TABLE OF CONTENTS

Overview

This report discusses the results of the Security and Telecommunications testing of the **Tenex Precinct Central 4.0** electronic poll book system.

Testing was implemented without any prior knowledge of the source code.

The testing addressed four aspects:

- Physical Security
- Physical Telecommunications
- Logical Security
- Logical Telecommunications

References

The following key documents were used in preparing this work paper.

1. California Electronic Poll Book Regulations

Review Process

Physical Security Review Process

The Physical Security review was conducted to analyze the **Tenex Precinct Central 4.0** electronic poll book system for findings against the following requirements:

- Examination of the top-level system design and architecture.
- Examination of the system documentation and procedures.
- Examination and open-ended testing of hardware including, when applicable, examination of unused hardware ports and the security measures to lock/seal the hardware ports used. Physical testing may not be destructive. If a risk is identified that requires destructive testing, the contractor will discuss this and receive written approval from the Secretary of State before proceeding with a destructive test.

Physical Telecommunications Review Process

The Physical Telecommunications review was conducted to analyze the **Tenex Precinct Central 4.0** electronic poll book system for findings against the following requirements:

- Examination of the top-level system design and architecture.
- Examination of the system documentation and procedures.
- Examination and open-ended testing of hardware including, when applicable, examination of unused hardware ports and the security measures to lock/seal the hardware ports used. Physical testing may not be destructive. If a risk is identified that requires destructive testing, the contractor will discuss this and receive written approval from the Secretary of State before proceeding with a destructive test.

Logical Security Review Process

The Logical Security review was conducted to analyze the **Tenex Precinct Central 4.0** electronic poll book system for findings against the following requirements:

- Examination of the top-level system design and architecture
- Examination of the system documentation and procedures
- Examination and open-ended testing of relevant software and operating system configuration
- Examination and open-ended testing of system communications, including encryption of data and protocols and procedures for access authorization

Logical Telecommunications Review Process

The Logical Telecommunications review was conducted to analyze the **Tenex Precinct Central 4.0** electronic poll book system for findings against the following requirements:

- Examination of the top-level system design and architecture
- Examination of the system documentation and procedures
- Examination and open-ended testing of relevant software and operating system configuration
- Examination and open-ended testing of system communications, including encryption of data and protocols and procedures for access authorization

The review process for the **Tenex Precinct Central 4.0** electronic poll book system incorporated the best effort within the time allowed to find and report observations for the above categories. As such, it is understood that there may be undetected vulnerabilities in these categories.

Review Results

Physical Security Review Analysis

SLI conducted a physical security review of the **Tenex Precinct Central 4.0** electronic poll book system for compliance with the California Electronic Poll Book Regulations.

The **Tenex Precinct Central 4.0** electronic poll book system top-level system design and architecture were examined for physical security compliance.

- The expected outcome for this review was that no issue would be found.
- The actual outcome for this review was a determination that the **Tenex Precinct Central 4.0** solution incorporates a proprietary cover and stand that does not have built in protective measures around the lightning port or the 3.5mm headphone jack. The protective case also doesn't block or inhibit the On/Off – Sleep/Wake button or the built-in camera and stereo speakers. The review concluded that the lack of physical port protection or button control doesn't hinder the overall security of the **Tenex Precinct Central 4.0** device due to additional electronic management and security features that allow remote location discovery, the ability to lock the iPad device, and, if necessary, remotely wipe the data.

  Each **Tenex Precinct Central 4.0** device and accessories comes in a padded carrying case that can be locked using security seals or padlocks to ensure secure transportation and delivery, as well as presenting a tamper evident storage environment, if warranted.

The **Tenex Precinct Central 4.0** electronic poll book system's system documentation and procedures were examined for physical security compliance.

- The expected outcome for this review was that no issue would be found.
- The actual outcome for this review was a determination that the supplied documentation adequately details setup and configuration of the system. These instructions cover the setup of the physical configuration, including pairing with the Bluetooth printer and setting up the device for use during an election. Documentation also included the setup and use of the application, including updating the application using Profile Manager Mobile Device

Management (MDM), and documentation for Precinct Central management and use.

- It should be noted that the documentation provided does not detail all of the security measures in place to secure the entire solution. These include Precinct Central, Profile Manager, technology providers such as Amazon Web Services (AWS), and built in Apple iPad security. These detailed security measures, while not necessary for public consumption, may be required by the jurisdiction / State requirements for specific security measures.

The **Tenex Precinct Central 4.0** electronic poll book system was examined including, when applicable, examination of unused hardware ports and the security measures to lock/seal hardware ports used. Physical testing was not destructive.

- The expected outcome for this review was that no issue would be found.
- The actual outcome for this review was a determination that while there are no physical measures in place to remove access to the device's externally accessible ports and buttons, there are electronic security measures of both the Apple iPad and the Profile Manager MDM configurations which ensure that a lost or stolen Precinct Central device can be sufficiently tracked or located, allowing the ability to find and recover the missing device. If necessary there is also the electronic capability to remotely wipe the device such that all data and applications on the device are removed and are no longer accessible.
- Inspection of the Bluetooth wireless printer determined that there is an additional RJ-45 network connector as well as a USB 2.0 B connector. Upon plugging the receipt printer into a network switch the printer prints a configuration receipt with the dynamically assigned IP address for the printer. The printer username and password to configure the printer is a manufacturer default combination. It details settings for a wireless configuration though it would appear that it needs an additional WLAN connection
- Inspection of the Bluetooth wireless printer determined that there were no additional security concerns from external port manipulation. There is an RJ-11 port that is used for receipt printer accessories such as a kitchen buzzer or ticket alarm.

Physical Telecommunications Review Analysis

SLI conducted a physical telecommunications review of the **Tenex Precinct Central 4.0** electronic poll book system for compliance with the California Electronic Poll Book Regulations

The **Tenex Precinct Central 4.0** electronic poll book system top-level system design and architecture were examined for physical telecommunications compliance.

- The expected outcome for this review was that no issue would be found.
- The outcome for this review was that the physical communications equipment used by the solution is split up into the following distinct communications systems.
  - iPad device including zero configuration networking peer to peer communications.
  - Bluetooth Including iPad and receipt printer (Epson TM-m30)
  - Wireless network (MiFi, Cellular, WPA2 networking)
  - AWS network connectivity.
- Documentation on processes, procedures, and telecommunications capability was reviewed with regard to the overall design and architecture of the system.
- The analysis determined that for each of the communications systems, the system design and architecture met the California Electronic Poll book security requirements.

The **Tenex Precinct Central 4.0** electronic poll book system documentation and written procedures were examined for physical telecommunications compliance.

- The expected outcome for this review was that no issue would be found.
- The outcome for this review was a determination that documentation and procedures for the communication systems of the solution were not always fully documented. Utilizing resources from Tenex and industry documentation for commercial off the shelf (COTS) and third-party services the following items were reviewed.
  - Peer to peer network communications:
    - IPad specific communications leverage out of the box security measures controlled by an MDM system.
    - Utilizing the Apple Multi-peer Connectivity framework, which allows the ability for each iPad to utilize peer to peer networking in a secure encrypted fashion. Precinct Central controls the creation and access of the peer to peer networking.

- Bluetooth communications
  - Apple IOS Bluetooth security
  - Epson TM-m30 Bluetooth receipt printer
- Wireless communications
  - Wireless connectivity (WPA2)
  - MiFi communications devices
  - Cellular communications
- AWS Services
  - Data Center access controlled both at the Amazon employee level and at the third-party level as applicable
  - Onsite CCTV, data center entry point monitoring
  - Intrusion detection employed on all ingress and egress points. 24/7 AWS logging, analysis, and response.

The **Tenex Precinct Central 4.0** electronic poll book system hardware was tested including, when applicable, examination of unused hardware ports and the security measures to lock/seal the hardware ports used. Physical testing was not to be destructive.

- The expected outcome for this review was that no issue would be found.
- The actual outcome for this review was a determination one issue that, terms of access authorization, the Epson TM-m30 Bluetooth receipt printer has an accessible RJ-45 Ethernet port that has a print server that utilizes default username and password combinations to access and configure the printer. It should be noted however that the ports on the printer utilize a plastic cover to block easy access to the power and ports
- It should be noted that due to the nature of some of the third-party services as well as unavailable hardware, the only means of verification possible was review of the third-party resources' documentation.
  - Amazon Web Services
  - AT&T Velocity 2 MiFi device
- Where applicable hardware devices were examined. These devices included:
  - IPad device
  - Bluetooth receipt printer (Epson TM-m30)

Logical Security Review Analysis

SLI conducted a Logical security review of the **Tenex Precinct Central 4.0** electronic poll book system for compliance with the California Electronic Poll Book Regulations

The **Tenex Precinct Central 4.0** electronic poll book system top-level system design and architecture were examined for logical security compliance.

- The expected outcome for this review was that no issue would be found.
- The actual outcome of this review determined that Tenex utilizes Amazon Web Services to host the Precinct Central application and databases. Apple's Profile manager is used as the applications MDM environment, and utilizes Apple's enterprise development program to digitally sign and distribute the application.
- Each iPad device is setup, deployed and managed using Apple Profile Manager (MDM.

The **Tenex Precinct Central 4.0** electronic poll book system documentation and procedures were examined for logical security compliance.

- The expected outcome for this review was that no issue would be found.
- The outcome for this review was that logical security was adequately documented.
    - Documentation related to setup and configuration of the solution was available.
    - Documentation on how to use and administer specific sections of the solution was available.
    - A security document was provided with information about services and offerings tailored to the security requirements and settings of the **Tenex Precinct Central 4.0** solution.
    - Working with Tenex resources, specific security features of these third-party services were identified, including added security.
    - These services include Amazon Web services (AWS), Apple Profile Manager, Apple Enterprise developers program, and native Apple IOS security.

The **Tenex Precinct Central 4.0** electronic poll book system relevant software and operating system configuration were examined and tested for logical security compliance.

- The expected outcome for this review was that no issue would be found.

- The outcome for this review confirmed that the system uses the Precinct Central Management system, and the iPads are configured per the Tenex documentation for running voter check in services.
  - The backend setup and configuration for the Tenex AWS instance backend were not verified as this configuration is hosted on AWS equipment.
  - Detailed documentation was not provided for the setup and management of the backend server instance infrastructures.
  - ICS bench marks were used to setup and harden AWS.
  - Profile Manager MDM was utilized to manage and configure iPad devices.

The **Tenex Precinct Central 4.0** electronic poll book system communications, including encryption of data and protocols and procedures for access authorization were examined and tested for logical security compliance.

- The expected outcome for this review was that no issue would be found.
- The actual outcome for this review was a determination that by utilizing Apple iPad technology in a properly configured and managed environment the **Tenex Precinct Central 4.0** solution provides a safe secure hardware environment to host an Electronic Poll Book system.
- Utilization of WPA2 enterprise level wireless security or MiFi / Cellular connectivity provides the ability to support whatever networking environment is required by the jurisdictions.
- Utilization of AWS EC2 provides in-depth infrastructure designed and managed to align with specific regulations, standards and best-practices for FIPS 140-2. All of the security best practices are covered including but not limited to:
  - Physical and environmental security (Datacenter)
  - Business continuity management
  - Secure network architecture
  - Database encryption (data at rest)
- Utilization of Mobile Device Management services allows all poll pads to be locked down to a specific level of access determined by the jurisdiction. This includes such restrictions and functionality as:
  - Limiting access to install or uninstall applications
  - Controlling networking settings
  - Ability to track, locate and remotely wipe iPad devices.

- Monitoring all iPad device information; including connection state, model, IOS level, and disk usage

- The Precinct Central utilizes AWS EC2 to store process and report voter specific data. EC2 utilizes CIS benchmarks to isolate all network traffic within the backend server instance environment from public access. Precinct central access is controlled by IP filtering to prevent unauthorized connectivity to the web application itself AWS and Tenex manage and maintain the following best practices:
  - Encrypted traffic: TLS 1.2, certificate authority signed certificates
  - AWS Shield: provides detection and mitigation of DDOS attacks
  - Firewalls locked down to allow only HTTP and HTTPS ports
  - Virtual Private Cloud to isolate backend server and database resources from the public.
  - Application load balancing
  - Auto scaling for server resources during times of increased performance needs
  - Customizable security groups
  - Encrypted database management
  - CIS security benchmarks for server hardening.

Logical Telecommunications Review Analysis

SLI conducted a logical telecommunications review of the **Tenex Precinct Central 4.0** electronic poll book system for compliance with the California Electronic Poll Book Regulations

The **Tenex Precinct Central 4.0** electronic poll book system top-level system design and architecture were examined for logical telecommunications compliance.

- The expected outcome for this review was that no issue would be found.
- The outcome for this review determined that the physical communications equipment used by the solution is split up into distinct communications systems.
  - IPad device Apple Multi-peer Connectivity framework, to create and manage peer to peer networking. Verified only by documentation and Tenex resources as a second device was unavailable for direct testing.
  - Bluetooth connectivity Including iPad and receipt printer (Epson –TM-m30)
  - Wireless network (MiFi, Cellular, WPA2 Networking)

- AWS network connectivity.

- Documentation on processes, procedures, and telecommunications capability was satisfactorily reviewed for the overall design and architecture of the system.
- It was determined that for each of the communications systems, the system design and architecture meet the California Electronic Poll Book Regulations security requirements.

The **Tenex Precinct Central 4.0** electronic poll book system documentation and procedures were examined for logical telecommunications compliance.

- The expected outcome for this review was that no issue would be found.
- The outcome for this review was a determination that documentation and procedures for the communications systems of the solutions were not always fully documented. Utilizing resources from Tenex and industry documentation for COTS and third-party services the following items were reviewed.
  - Peer to peer network communications:

    It should be noted that Testing for the peer to peer networking was unavailable as only a single iPad Device was available.
    - IPad specific communications leverage out of the box security measures and are controlled by a Mobile Device Management system.
    - Utilizing the Apple Multipeer Connectivity framework, which allows the ability for each IPad to utilize peer to peer networking in a secure encrypted fashion. Precinct Central controls the creation and access of the peer to peer networking.
  - Apple Profile Manager
    - Ability to control network connectivity settings based on jurisdiction network requirements.
    - Ability to restrict network communications
  - Bluetooth communications
    - Apple IOS Bluetooth security
    - Epson Bluetooth receipt printer
  - Wireless communications
    - Wireless connectivity (WPA2)
    - MiFi communications devices
    - Cellular communications

- AWS services
  - Encrypted traffic: TLS 1.2, certificate authority signed certificates
  - AWS Shield: provides detection and mitigation of DDOS attacks
  - Firewalls locked down to allow only HTTP and HTTPS ports
  - Virtual Private Cloud to isolate backend server and database resources from the public.

The **Tenex Precinct Central 4.0** electronic poll book system's relevant software and operating system configuration were examined and tested for logical telecommunications compliance.

- The expected outcome for this review was that no issue would be found.
- The outcome for this review has confirmed that the solution delivered and setup is the Precinct Central Management system, and the iPad devices are configured per the Tenex documentation for running voter check-in services.
- The following systems and services were reviewed for relevant software and system configuration:
  - Apple Profile Manager MDM was utilized to manage and configure iPad devices. It should be noted that access was not provided to interact with the Profile manager, and per Tenex the jurisdictions are not given access to the MDM. MDM interface is locked down to Tenex networks specifically.
  - The Precinct Central utilizes AWS EC2 to store process and report voter specific data. EC2 Utilizes CIS benchmarks to isolate all network traffic within the backend server instance environment from public access. Precinct central access is controlled by IP filtering to prevent unauthorized connectivity to the web application.
  - IPad IOS communication security best practices for setup.
  - Bluetooth connectivity.

The **Tenex Precinct Central 4.0** electronic poll book system communications, including encryption of data and protocols and procedures for access authorization, were examined and tested for logical telecommunications compliance.

- The expected outcome for this review was that no issue would be found.
- The actual outcome for this review was a determination that, in terms of access authorization, the Epson TM-m30 Bluetooth receipt printer has an accessible RJ-45 Ethernet port that has a print server that utilizes default username and password combinations to access and configure the printer. It should be noted however that the ports on the printer utilize a plastic cover to block easy access to the power and ports.

- Utilizing Apple iPad technology in a properly configured and managed environment the Tenex Precinct Central 4.0 Solutions provides a safe secure hardware environment to host an Electronic Poll Book system.
- Utilization of WPA2 Enterprise level wireless security or MiFi / Cellular connectivity provides the ability to support whatever networking environment is required by the jurisdictions.
- Utilization of Mobile Device Management services allows all iPad devices to be locked down to a specific level of access determined by the jurisdiction. This includes such restrictions and functionality as:
  - Control networking settings
  - Ability to track, locate, and remotely wipe Poll Pad devices
  - Restrict connectivity to specific defined networks
- The Precinct Central utilizes AWS EC2 to store, process and report voter specific data. EC2 utilizes CIS benchmarks to isolate all network traffic within the backend server instance environment from public access. Precinct central access is controlled by IP filtering to prevent unauthorized connectivity to the web application itself AWS and Tenex manage and maintain the following best practices:
  - Encrypted traffic: TLS 1.2, certificate authority signed certificates
  - AWS Shield: provides detection and mitigation of DDOS attacks
  - Firewalls locked down to allow only HTTP and HTTPS ports
- Bluetooth Connectivity
  - iPad Bluetooth 4.0 security practices
  - Bluetooth receipt printers (Epson TM-m30) connectivity
- Cellular / MiFi connectivity was reviewed on a reconnaissance basis only as there are potential legal ramifications of testing a cellular/MiFi third party service.

Findings

This section discusses any Findings from the **Tenex Precinct Central 4.0** electronic poll book system physical security review, as well as potential impacts.

Physical Security Review Discrepancies

During the physical inspection of the **Tenex Precinct Central 4.0** solution it was determined that the Epson TM-m30 receipt printer had an active wired network port that when supplied with an IP via a DHCP server had the default Epson credentials

in place. The ability to affect the system is negligible at this time. This was noted as it is an active unsecured port, that could be disabled or changed from defaults to ensure no unauthorized access or reconfiguration of the printer is possible.

Physical Telecommunications Review Discrepancies

During the physical investigation of the solution, there was one discrepancy found. There are open ports or other means to access or disrupt the device's communications system.

The Epson TM-m30 Bluetooth receipt printer has an accessible RJ-45 Ethernet port that has a print server that utilizes default username and password combinations to access and configure the printer. It should be noted however that the ports on the printer utilize a plastic cover to block easy access to the power and ports.

.

Two items of note:

1. The system uses a USB Type B jack for printer connection.
2. Each receipt printer has a Drawer Kick port, which is used to send a signal to open a cash drawer upon receipt generation. Attempts to compromise this port were unsuccessful.

Logical Security Review Discrepancies

No logical discrepancies were found.

It should be noted that most of the security measures in place are dependent upon third party technology and services, including Apple native IOS Security, Apple's Profile manager MDM and Amazon Web Services. It should also be noted that compromise to the individual systems and services could affect the overall security of the solution.

Logical Telecommunications Review Discrepancies

During the analysis of the solution there was one discrepancy found.

The Epson TM-m30 Bluetooth receipt printer has an accessible RJ-45 Ethernet port that has a print server that utilizes default username and password combinations to access and configure the printer. It should be noted however that the ports on the printer utilize a plastic cover to block easy access to the power and ports.

The iPAD devices were configured per the policy settings of the Profile manager MDM with the exception of the Wi-Fi connectivity settings. For testing purposes a Wi-Fi testing network was utilized to give a wider range of testing ability than may be configured during a live election event. This allowed for communication monitoring as well as attempts to compromise / authenticate encryption.

Additionally, documentation and procedures for the communications systems of the solutions were not always fully documented.

Vulnerabilities

Should any vulnerability be discovered, SLI will identify the particular requirement applicable to each vulnerability.

To the extent possible, reported vulnerabilities will include an indication of whether the exploitation of the vulnerability would require access by:

- Voter: Usually has low knowledge of the Electronic Poll Book System's software and/or hardware design and configuration. Some may have more advanced knowledge. May carry out attacks designed by others.
- Poll worker: Usually has low knowledge of the Electronic Poll Book System's software and/or hardware design and configuration. Some may have more advanced knowledge. May carry out attacks designed by others. They have access to the software and/or hardware for up to ten days, but all physical security has been put into place before the machines are received.
- Elections official insider: Wide range of knowledge of the Electronic Poll Book System's software and/or hardware design and configuration. May have unrestricted access for long periods of time. Their designated activities include:
  - Set up and pre-election procedures;
  - Election operation;
  - Post-election procedures; and
  - Archiving and storage operations.
- Vendor insider: With great knowledge of the Electronic Poll Book System's software and/or hardware design and configuration. They have unlimited access to the Electronic Poll Book System's software and/or hardware before it is delivered to the purchaser and, thereafter, may have unrestricted access when performing warranty and maintenance service and when providing election administration services.

SLI will not verify or demonstrate exploitability of the vulnerability but the report of the vulnerability will identify factors involved in the exploitation. Any vulnerability theories developed by the source code review team members shall, to the extent possible, be referred to the Secretary of State staff.

The review process incorporated best efforts within the time allowed to find and report observations for the above categories. As such, it is understood that there may be undetected vulnerabilities in these categories.

Physical Security Vulnerabilities

During the physical investigation it was found that the wired network port on the Epson TM-m30 printer was active and seeking a DHCP IP address. The server located on the printer itself currently utilizes the default username and password for the login. While this in itself doesn't appear to affect the overall security of the solution it has been noted as a potential attack vector and should be disabled or default values changed. All four defined actors have the potential to attempt this vulnerability.

The solution offers a way to secure the device before and after the election process utilizing the padded case. The padded case allows the use of security seals and/or locks for tamper evident storage and transportation to ensure that each device can be secured prior to and after the process.

Built in Apple technology paired with an MDM management system provides the ability to remotely control / wipe a lost or stolen **Tenex Precinct Central 4.0** device.

Physical Telecomm Vulnerabilities

No specific vulnerabilities were found in the examination of the physical telecommunications aspects of the hardware.

IPad: While no specific vulnerabilities were found in the examination of the iPad technology used to run the iPad application, the application and iPad hardware utilize Bluetooth technology to connect to Bluetooth receipt printers. All attempts to compromise the iPad and the receipt printer were unsuccessful beyond basic reconnaissance data being pulled from the Bluetooth devices. There have been, and continue to be, successful attacks targeting Bluetooth technology. The limited connectivity range helps to minimize the impacts of attacks against these devices.

Each of the iPad devices utilize Apple's zero configuration peer to peer networking service to keep iPads located within the same physical location up to date on voter check-in.

All attempts to sniff, access, or compromise this network were unsuccessful.

Logical Security Vulnerabilities

Precinct Central vulnerabilities:

Vulnerabilities that would require an Election Official insider, or a Vendor Insider (aware or unaware)

- Cross-site request forgery: (Medium – Tentative)
  Cross-site request forgery (CSRF) vulnerabilities may arise when applications rely solely on HTTP cookies to identify the user that has issued a particular request. Because browsers automatically add cookies to requests regardless of their origin, it may be possible for an attacker to create a malicious web site that forges a cross-domain request to the vulnerable application. For a request to be vulnerable to CSRF, the following conditions must hold:
    - The request can be issued cross-domain; for example, by using an HTML form. If the request contains non-standard headers or body content, then it may only be issuable from a page that originated on the same domain.
    - The application relies solely on HTTP cookies or Basic Authentication to identify the user that issued the request. If the application places session-related tokens elsewhere within the request, then it may not be vulnerable.
    - The request performs some privileged action within the application, which modifies the application's state based on the identity of the issuing user.
    - The attacker can determine all the parameters required to construct a request that performs the action. If the request contains any values that the attacker cannot determine or predict, then it is not vulnerable.
- SSL Cookie without Secure Flag Set (Medium – Firm)

  If the secure flag is set on a cookie, then browsers will not submit the cookie in any requests that use an unencrypted HTTP connection, thereby preventing the cookie from being trivially intercepted by an attacker monitoring network traffic. If the secure flag is not set, then the cookie will be transmitted in clear-text if the user visits any HTTP URLs within the cookie's scope. An attacker may be able to induce this event by feeding a user suitable links, either directly or via another web site. Even if the domain that

issued the cookie does not host any content that is accessed over HTTP, an attacker may be able to use links of the form http://example.com:443/ to perform the same attack.

To exploit this vulnerability, an attacker must be suitably positioned to eavesdrop on the victim's network traffic. This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.

- Open redirection (DOM-Based) (Low – Tentative: Determined by Static Code Analysis and may lead to False positives)

  DOM-based vulnerabilities arise when a client-side script reads data from a controllable part of the DOM (for example, the URL) and processes this data in an unsafe way.

  DOM-based open redirection arises when a script writes controllable data into the target of a redirection in an unsafe way. An attacker may be able to use the vulnerability to construct a URL that, if visited by another application user, will cause a redirection to an arbitrary external domain. This behavior can be leveraged to facilitate phishing attacks against users of the application. The ability to use an authentic application URL, targeting the correct domain and with a valid SSL certificate (if SSL is used), lends credibility to the phishing attack because many users, even if they verify these features, will not notice the subsequent redirection to a different domain.
- Link Manipulation (DOM-based) (Low – Firm: Determined by Static Code Analysis and may lead to False positives)
  DOM-based vulnerabilities arise when a client-side script reads data from a controllable part of the DOM (for example, the URL) and processes this data in an unsafe way.

  DOM-based link manipulation arises when a script writes controllable data to a navigation target within the current page, such as a clickable link or the submission URL of a form. An attacker may be able to use the vulnerability to construct a URL that, if visited by another application user, will modify the

target of links within the response. An attacker may be able to leverage this to perform various attacks, including:
    - Causing the user to redirect to an arbitrary external URL, to facilitate a phishing attack.
    - Causing the user to submit sensitive form data to a server controlled by the attacker.
    - Causing the user to perform an unintended action within the application, by changing the file or query string associated with a link.
    - Bypassing browser anti-XSS defenses by injecting on-site links containing XSS exploits, since browser anti-XSS defenses typically do not operate on on-site links.
- Content type incorrectly stated: (Low – Firm)
  If a response specifies an incorrect content type then browsers may process the response in unexpected ways. If the content type is specified to be a renderable text-based format, then the browser will usually attempt to interpret the response as being in that format, regardless of the actual contents of the response. Additionally, some other specified content types might sometimes be interpreted as HTML due to quirks in particular browsers. This behavior might lead to otherwise "safe" content such as images being rendered as HTML, enabling cross-site scripting attacks in certain conditions.
  The presence of an incorrect content type statement typically only constitutes a security flaw when the affected resource is dynamically generated, uploaded by a user, or otherwise contains user input. The contents of affected responses should be reviewed and the context in which they appear, to determine whether any vulnerability exists.
- Strict transport security not enforced (Low – Certain)
  The application fails to prevent users from connecting to it over unencrypted connections. An attacker able to modify a legitimate user's network traffic could bypass the application's use of SSL/TLS encryption, and use the application as a platform for attacks against its users. This attack is performed by rewriting HTTPS links as HTTP, so that if a targeted user follows a link to the site from an HTTP page, their browser never attempts to use an encrypted connection. The sslstrip tool automates this process.
  To exploit this vulnerability, an attacker must be suitably positioned to intercept and modify the victim's network traffic. This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack.

IPad Platform: While no specific vulnerabilities were found in the examination of the iPAD technology used to run the iPad application, the application and iPad hardware utilize Bluetooth technology to connect to Bluetooth receipt printers. All attempts to compromise the iPad and the receipt printer were unsuccessful beyond basic reconnaissance data being pulled from the Bluetooth devices. There have been, and continue to be, successful attacks targeting Bluetooth technology. The limited connectivity range helps to minimize the impacts of attacks against these devices.

Each of the iPad devices utilize Apple's zero configuration peer to peer networking service to keep iPads located within the same physical location up to date on voter check-in.
Only a single iPad device was supplied so attempts to compromise this peer to peer network were unable to be tested.

Logical Telecomm Vulnerabilities

No vulnerabilities were found in the examination of the logical communications aspects of the system.

It should be noted, however, that the systems tested onsite utilize wireless communications of any type and that if the system is not setup to the specific requirements of the jurisdiction, improper configuration could lead to compromise of the system. Use of unsecure/ unauthorized networks is an example of potential compromise.

It should also be noted that the system uses both Bluetooth and peer to peer wireless communications to keep iPad devices connected to each other for real time sharing of check-in data between polling place devices. Reasonable attempts were made to sniff, access, or compromise this network and the attempts were unsuccessful.

Conclusions

Physical Security

One Finding was located within the **Tenex Precinct Central 4.0** electronic poll books system.

One potential vulnerability was located within the **Tenex Precinct Central 4.0** electronic poll book system.

It should be noted that jurisdictional polling place security processes and procedures play a large role in making sure that the **Tenex Precinct Central 4.0** solution remains secure. This would include processes and procedures for implementation of each device for use by poll workers in each jurisdiction, as well as physically securing each device before, during, and after the election process.

Physical Telecomm

One Finding was located within the **Tenex Precinct Central 4.0** electronic poll books system, in relation to physical communication hardware

This finding involved an active RJ-45 network port that allows access to a print server for configuration of the receipt printer. The printer has default username and password credentials to login and configure the receipt printer. This discrepancy is of Low impact to the overall security of the solution, and was noted as a discrepancy instead of a vulnerability.

No vulnerabilities were located within the **Tenex Precinct Central 4.0** electronic poll book physical communication hardware.

Noted items:

- Pair and reset buttons were accessible on the Bluetooth receipt printers
- There is an accessible Drawer Kick port.
- A MiFi Cellular device was supplied, however attempts to exploit a public Cellular communications medium were restricted to reconnaissance only due to possible legal restrictions. It should be noted that MiFi devices have some of the same exploit potential as other wireless communication mediums.
- The solution allows the ability to connect to any type of wireless communications networks. This access can be configured and secured utilizing the MDM to restrict or conform to requirements set forth by the jurisdiction.
    - Any Wi-Fi networking used by the jurisdictions are subject to processes and procedures set forth by the jurisdiction and were not specifically tested or reviewed.

Logical Security

No discrepancies were located within the **Tenex Precinct Central 4.0** electronic poll books system during review. It was noted that this solution is highly dependent upon third-party systems, that if compromised would reduce the overall security posture of the solution. Conscious efforts to limit the exposure of the management

system and MDM Management infrastructure by filtering IP addresses that are allowed to be accessed, go a long way to prevent unauthorized access or compromise to the Tenex Precinct Central 4.0 Solution.

Six types of vulnerabilities were located within the **Tenex Precinct Central 4.0** electronic poll book system, related to the Precinct central web application. These vulnerabilities ranged in severity from Low to Medium. All vulnerabilities found were considered of minimal impact to the overall security of the Tenex Precinct Central 4.0 Solution. The web vulnerability scan of the application was completed using an administrative credentialed account.

The iPad devices sufficiently meet requirements by:

- Offering FIPS-140-2 encryption to data both at rest and during transmissions utilizing AES 256Bit encryption or greater.
- Mobile device management gives precise control of all aspects of the iPad device configuration
  - Ability to remotely wipe IPad devices
  - Ability to track lost or stolen devices
  - Control Wi-Fi Access
  - Control applications versions
- Application Sandbox: allowing for separate environments designed to protect each application from infecting or compromising another.
- Guided access (KIOSK) mode, allows for the ability to lock down the iPad device to a single application, limiting the ability to manipulate the iPad.

Logical Telecomm

One Finding was located within the **Tenex Precinct Central 4.0** electronic poll books system.

This finding involved an active RJ-45 network port that allows access to a print server for configuration of the receipt printer. The printer has default username and password credentials to login and configure the receipt printer. This discrepancy is of Low impact to the overall security of the solution, and was noted as a discrepancy instead of a vulnerability.

No Vulnerabilities were located within the **Tenex Precinct Central 4.0** electronic poll books system.

Testing attempted to circumvent or exploit vulnerabilities within the communication systems as applicable and within legal boundaries with respect to third party

services. It should be noted that compromise to the third party services such as Cisco Meraki and Amazon webservices could have an adverse effect on the overall security of the system.

It should further be noted that while no vulnerabilities or discrepancies were found in the testing of Bluetooth devices, this is a potential attack vector above and beyond regular wireless communications.

It should also be noted that while no vulnerabilities or discrepancies were found in the testing of the peer to peer network, this is a potential attack vector above and beyond regular wireless communications.

Conscious efforts to limit the exposure of the management system and MDM Management infrastructure by filtering the IP addresses that are allowed to to be accessed, will go a long way to prevent unauthorized access or compromise to the Tenex Precinct Central 4.0 Solution and Apple Profile manager MDM service.