Robis Elections, Inc. AskED ePollbook CA Electronic Poll Book System Security and Telecommunications Test Report for California

ROB-18001SECTR-01

Prepared for:

Vendor Name	Robis Elections, Inc.
Vendor System	AskED ePollbook CA

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
August 28th, 2018	1.0	*J. Panek, J. Peterson*	Initial Release
September 7th, 2018	1.1	*J. Panek, J. Peterson*	Minor updates

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 **Robis AskED ePollbook CA** 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 **Robis AskED ePollbook CA** 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 **Robis AskED ePollbook CA** 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 **Robis AskED ePollbook CA** 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 **Robis AskED ePollbook CA** 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 **Robis AskED ePollbook CA** 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 **Robis AskED ePollbook CA** electronic poll book system for compliance with the California Electronic Poll Book Regulations.

The **Robis AskED ePollbook CA** 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 AskED ePollbook solution incorporates a proprietary case that utilizes hook-and-loop fasteners to secure the ePollbook Atlas device into the case. There are no physical deterrents to prevent the device from being removed from the case.
- The protective case doesn't have protective measures to prevent manipulation of any of the ports or power inputs.
- The commercial off-the-shelf (COTS) full sized printers don't have any built-in port protection or recommended actions to prevent the printers from being connected to a LAN environment.
- In its tested configuration, the Pepwave router has wired network ports disabled and it was presented verbally that security seals could be used to cover exposed network ports with a tamper evident seal. No documentation was presented for security seal placement.
- The Pepwave router's cellular broadband modem could easily be removed.

The review concluded that the lack of built in case deterrents may require the jurisdiction to incorporate additional deterrents to secure the ePollbook solution physically.

It should be noted that each of the ATLAS ePollbook devices is encrypted utilizing Bitlocker drive encryption which reduces the ability to circumvent electronic security and protects the voter registration database should the laptop be stolen or lost. The documentation references a self-destruct option that allows the AskED ePollbook to automatically self-destruct voter data after a specified number of hours. This is the closest functionality to remotely wiping the data should the devices be lost or stolen. No functionality was found to be present for remote device location discovery.

Each ePollbook device and its accessories comes in a padded fabric carrying case that can be locked using security seals or padlocks to ensure secure transportation and delivery of the device.

The nature of the fabric carrying case may present the opportunity to easily access the device(s) while in storage or transit.

The **Robis AskED ePollbook CA** 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 include setup of both the physical configuration, including connecting the different printer options, and setting up the ePollbook for use during an election.
- It should be noted that the documentation provided does not detail physical security measures in place to secure the entire solution. The documentation does not provide specific suggestions for placement of security seals.
- Detailed security measures, while not necessary for public consumption, may be required by the jurisdiction / state requirements.

The **Robis AskED ePollbook CA** 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 there are no physical security measures in place to remove access to the device's externally accessible ports. A USB hub is placed within the carrying case and isn't generally accessible under foam padding.
- The ATLAS ePollbook device utilizes BitLocker drive encryption which helps ensure that the data contained on the device is secure and unalterable should the device be lost or stolen. No device tracking or remote wipe ability was observed.
- Two of three COTS printers had live hard-wired network interfaces enabled.
- All ports are active and able to be manipulated.

Physical Telecommunications Review Analysis

SLI conducted a physical telecommunications review of the **Robis AskED ePollbook CA** electronic poll book system for compliance with the California Electronic Poll Book Regulations

The **Robis AskED ePollbook CA** 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 actual outcome for this review was a determination that the physical communications equipment used by the solution is split up into distinct communications systems.
  - Bak Atlas Ultrabook
  - PepWave small office, home office (SOHO) router
  - Verizon USB cellular modem
- Documentation on processes, procedures, and telecommunications ability was reviewed for the overall design and architecture of the system. No specific documentation was found detailing the setup and configuration of any of the communications devices.
- The analysis of each of the three communications systems determined that their system design and architecture were within the California Electronic Poll book security requirements.

The **Robis AskED ePollbook CA** 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 actual outcome for this review was a determination that the documentation and written procedures for the telecommunications systems were incomplete. Utilizing resources from Robis and industry documentation for COTS and third-party services the following items were reviewed:
  - Pepwave SOHO Surf router
    - Wired communications were currently disabled
    - Wireless communications
      - Wireless connectivity (WPA2)
    - Cellular communications
  - Robis hosted server(s) connectivity
    - Data center access controlled by Robis
    - Onsite CCTV, data center entry point monitoring
    - Intrusion detection employed on all ingress and egress points. 24/7 logging, analysis and response.
  - COTS Printers
    - OKI C532 Printer
    - OKI C711 Printer
    - Bixolon SPP – R200lIliK
  - Signature Pad
    - SigPlus T-L460
    - SigPlus T LBK750
  - Barcode Scanner

- DS Series
- LI2208 Linear Imager

The **Robis AskED ePollbook CA** 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 that for each of the three communications systems, the system design and architecture was within the California Electronic Poll book security requirements.
- It should be noted that due to the nature of some of the third-party services and unavailable hardware, the only verifications performed were for documentation or direct consultation with Robis resources for the following:
  - Data Center hosting services for Robis hosted servers
  - Verizon USB cellular modem
- Where applicable, hardware devices were examined. These devices included
  - Pepwave SOHO Surf router
  - Robis Hosted server(s) connectivity
  - COTS Printers
    - OKI C532 Printer
    - OKI C711 Printer
    - Bixolon SPP – R200lllik
  - Signature Pad
    - SigPlus T-L460
    - SigPlus T LBK750
  - Barcode Scanner
    - DS Series
    - LI2208 Linear Imager

Logical Security Review Analysis

SLI conducted a logical security review of the **Robis AskED ePollbook CA** electronic poll book system for compliance with the California Electronic Poll Book Regulations

The **Robis AskED ePollbook CA** 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 was a determination that Robis utilizes technology that meets the requirements in these ways:
  - Provides Advanced Encryption Standard (AES 256-bit encryption for data at rest and in transit.
  - Utilizes (IEEE) 802.11 Wireless Lan Standards
    - 256-bit data encryption
    - WPA2 Security
    - Dedicated wireless access point (WAP)
  - Utilizes device(s) equipped with multifactor authentication
  - Is capable of utilizing Wide Area Network (WAN) to transmit voter registration data Including:
    - Hardware Virtual Private network
    - A dedicated cellular connection void of public or guest access

The **Robis AskED ePollbook CA** 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 actual outcome for this review was a determination that the documentation was adequate.
  - Documentation related to setup and configuration of the solution was available.
  - Documentation on how to use and administer specific sections of the solution was adequate.

The **Robis AskED ePollbook CA** 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 actual outcome for this review was a determination that the solution delivered and setup is the AskED ePollbook solution, consisting of connectivity to the command center hosted remotely and Bak Atlas laptop computer devices configured with AskED ePollbook software per the Robis documentation for running voter check-in services.
- The outcome for this review was unable to confirm the following due to lack of documentation or physical access to equipment or solution component.
  - The backend server setup and configuration for the Robis Command center service were not verified for correct setup and configuration and best practices as these resources are hosted remotely on Robis controlled equipment.

- Detailed documentation was not provided for the setup and management of the backend server instance infrastructures.
- No documented configuration management system for controlling / deploying the AskED solution.
- No documented validation or verification procedures to determine if software configured and executed on the solution is the certified version.
- Pre-Shared Key (PSK) management for Pepwave wireless devices.
- Management of MAC filtering on a wide scale.
- Configuration and hardening of Pepwave routing equipment both on the client side as well as the server side.

The **Robis AskED ePollbook CA** 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 technology in a properly configured and managed environment the **Robis AskED ePollbook CA** solution may provide a safe, secure hardware environment to host an Electronic Poll Book system.
- Utilization of a combination of WPA2 wireless security, wired LAN connectivity, and cellular communications provides the ability to support whatever networking environment is required by the jurisdictions.
- Utilization of custom hardening procedures to lock down each Bak Atlas ePollbook device to a specific level of access determined by the jurisdiction. This includes such restrictions and functionality as:
  - Separate administrative and user access levels
  - Kiosk mode with a custom-built shell.
  - Group policy security features
  - Vendor controlled networking environment
- The Command Center utilizes self-hosted infrastructure. There is little to no documentation to determine exact security measures in place, for both physical and logical security.
  - Encrypted traffic: TLS 1.2, certificate authority signed certificates
  - Verbal mention of distributed denial-of-service (DDOS) attack protection (unconfirmed)
  - Firewalls locked down to allow only HTTP and HTTPS ports
  - IP Filtering at the webserver level.
  - Encrypted Database Management (BitLocker)
    - On ePollbook device only

- Unable to confirm Command center and SQL Server encryption at the data center level due to missing documentation and authorized access to remote infrastructure.

Logical Telecommunications Review Analysis

SLI conducted a logical telecommunications review of the **Robis AskED ePollbook CA** electronic poll book system for compliance with the California Electronic Poll Book Regulations

The **Robis AskED ePollbook CA** 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 actual outcome for this review was a determination that the communications systems used by the solution consist of:
  - Wired network connectivity provided by the Pepwave routing device (disabled for current testing engagement).
  - Wireless network connectivity provided by the Pepwave routing device (enabled, WPA2).
  - Cellular network; cellular broadband connectivity.
  - Robis's hosted Data Center network connectivity.
- Documentation on processes, procedures, and telecommunications ability was reviewed for the overall design and architecture of the system. Per Robis, specific security related documentation is not readily available outside of the company. SLI was unable to verify documentation for any security measures associated with the solution, with the exception of the following high-level items.
  - Basic encryption assumptions:
    - 256bit encryption
    - Connections are IP restricted and utilize SSL TLS 1.2
    - Privately generated certificates for two factor authentication
    - Dedicated routers with whitelisting for unauthorized traffic protection
  - Multiple types of connectivity
    - Wireless
      - 256bit WPA2 connections with 63-character passwords
    - Wired
      - Not tested due to being disabled
    - Cellular broadband
      - Was reviewed on a reconnaissance basis only
  - Operation logs

- Self-destruct option for automatic destruction of voter data after election day
- Security updates for Windows operating systems
- VPN capability
  - Unable to confirm if this functionality is currently present
- Role-based security
- No public cloud.

- For each of the communications systems, it was determined that the system design and architecture are within the California Electronic Poll book security requirements.
- The documentation supplied by the vendor is inadequate to reliably verify, validate. and configure all security features and systems in place.
  - No documentation on how to configure the Pepwave router
  - No documentation on how to configure the Bak Atlas wireless / wired connections
  - No documentation about how Bak Atlas machines are configured / hardened

The **Robis AskED ePollbook CA** 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 actual outcome for this review was a determination that documentation and procedures for the communications systems of the solutions did not adequately document the security of the overall solution. In response to queries, Robis supplied the following information:
  - Regarding wireless communications:
    - Wireless connectivity utilizes a 63-character randomly generated WPA2 pass phrase
    - Utilizes MAC address filtering
    - Utilizes content filtering
    - Utilizes IP address filtering
  - Regarding the Robis-hosted Data Center
    - Command Center access is protected by IP restrictions, self-generated client certificates, and SSL/TLS 1.2.
      - It should be noted that the servers still respond with a 403 forbidden when coming from an unauthorized IP address or with an invalid certificate.
      - The IP address restrictions are at the IIS server level, not at the firewall level.

- Remote and physical access are heavily restricted
- There is no public cloud; all systems and services are controlled by Robis.

The **Robis AskED ePollbook CA** 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 actual outcome for this review was a determination that the solution delivered and setup is the **Robis AskED ePollbook CA** system, with a jurisdiction computer allowing access to the Command Center, and secure FTP (SFTP) server. The ePollbook devices are configured per the Robis documentation for running voter check in services.
- The following systems and services were reviewed for relevant software and system configuration:
  - Jurisdiction computer (normally supplied by the customer)
  - BAK USA Atlas laptop devices
  - Pepwave: Surf SOHO
  - Command Center

The **Robis AskED ePollbook CA** 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 of this review was a determination that:
- The Pepwave: Surf SOHO router was secured with non-default settings including a new network configuration, administrative credentials.
- The Pepwave: Surf SOHO router incorporates the ability to disable or restrict wired LAN ports.
- The Pepwave: Surf SOHO router incorporates basic MAC address filtering for wireless connections.
- The Pepwave: Surf SOHO router incorporates content filtering for connected clients giving the ability to control client connectivity destinations.
- Utilization of WPA2 wireless security and Mifi / cellular WAN connectivity as well as the ability to configure the router for multiple types of WAN connectivity options provides the ability to support whatever networking environment is required by the jurisdictions.
- The Robis Central command utilizes vendor hosted servers.
  - Encrypted traffic: TLS 1.2, certificate authority signed certificates.

  - Per Robis, DDOS prevention is in place; however, there is no substantiating documentation.
  - Firewalls appear to only allow ports 22, 80 and 443.
- 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 **Robis AskED ePollbook CA** electronic poll book system physical security review, as well as potential impacts.

Physical Security Review Discrepancies

During the physical inspection of the AskED ePollbook devices, it was noted that the case has no security measures to prevent access to ports or power connections. The case made no extra effort to limit the removal of the ePollbook device from the case or location assigned.

Device BitLocker encryption reduces the ability to manipulate or access the data stored on the drive in the event that the device is lost or stolen. No device tracking or remote wipe ability was observed.

The solution was missing detailed documentation about placement of security ties/seals or case locks to physically secure the solution.

Physical Telecommunications Review Discrepancies

During the physical investigation of the solution, there were three discrepancies found. These included open ports or the ability to access or disrupt the device's communications ability.

Three items of note:

- RJ-45 network ports on the OKI C711 and the OKI C532 printers were accessible
- An active, unprotected USB 2.0 slot
- Pepwave SOHO Router is able to be physically reset utilizing a button accessible with a small pointed object.
- Data ports on the OKI C711 are accessible and enabled.

Logical Security Review Discrepancies

During the logical security investigation of the solution, the following discrepancies were noted:

- Lack of documentation for individual ePollbook device configuration
- Lack of documentation for overall security posture of the solution
- Lack of documentation for communications setup and configuration
- Lack of documentation for Command Center / backend SQL database security
- Router management interface accessible from public internet

Logical Telecommunications Review Discrepancies

For the logical telecommunications investigation, the ATLAS ePollbook devices were configured per the vendor documentation. The wireless connectivity settings, the routers, and ATLAS devices are preconfigured for connectivity with the Pepwave router from the vendor. For testing purposes, a security testing device was utilized to give a wider range of testing tools. This allowed for communication monitoring as well as attempts to compromise / authenticate encryption.

At the time of the review, there were two discrepancies found, as well as a number of other concerns from the results.

The three discrepancies are:

1. COTS Printers C532 and C711 both come with active network interface cards that are by default enabled and waiting for a dynamically assigned IP address to be assigned. Both of the printers were configured with default credentials for complete access to the printer functionality.
2. The PepWave Surf SOHO router's administrative interface is accessible publicly from the public internet.
3. Certificates used for two factor authentication aren't tied to specific devices. Allowing for the export of the certificate and installation of the certificate on unauthorized devices.

Other items of concern include:

- During the course of the security audit it was discovered that the certificate(s) used to provide authentication to the AskED servers are not created per individual device but is instead a single certificate. This allows for the export and re-use of the authentication certificate on unauthorized devices if the opportunity is presented.
- The IP filtering of the Command Center web server appears to be utilizing the Dynamic IP address restrictions functionality of the IIS server. As a result of this:
  - Connectivity to the same server for SFTP is not IP restricted
  - Connectivity to the same server for SSH is not IP restricted

  - Basic HTTPS access appears to be restricted by IP / certificate by a windows IIS server(s); however, this allows the connection to establish with the server and delivers a 403 Forbidden: message to the source browser. This is most likely due to not having the proper requirements to access the URL's.
- The PepWave Surf SOHO router's administrative interface is accessible publicly from the public internet.

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: Usually has a 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: Usually has 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 review of the physical security of the solution it was determined that there were no specific vulnerabilities beyond the ability to take the device from the Polling place.

The solution offers a way to secure the device before and after the election process by utilizing a padded case which offers the ability to use 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. However, these seals are only tamper-evident and are easily circumvented.

Physical Telecomm Vulnerabilities

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

Logical Security Vulnerabilities

Command Center Vulnerabilities:

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

- **SQL Injection: (High – Firm)**

  The **SESSIONID** parameter appears to be vulnerable to SQL injection attacks. The payload **'** was submitted in the SESSIONID parameter, and a database error message was returned. The database appears to be Microsoft SQL Server.

  SQL injection vulnerabilities arise when user-controllable data is incorporated into database SQL queries in an unsafe manner. An attacker can supply crafted input to break out of the data context in which their input appears and interfere with the structure of the surrounding query.

  A wide range of damaging attacks can often be delivered via SQL injection, including reading or modifying critical application data, interfering with application logic, escalating privileges within the database and taking control of the database server.

- **SSL cookie without secure flag set: (Medium – Firm)**

  The following cookie was issued by the application and does not have the secure flag set:

ASP.NET_SessionId. The cookie appears to contain a session token, which may increase the risk associated with this issue. You should review the contents of the cookie to determine its function.

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.

- **Session token in URL (Medium – Firm)**

  Sensitive information within URLs may be logged in various locations, including the user's browser, the web server, and any forward or reverse proxy servers between the two endpoints. URLs may also be displayed on-screen, bookmarked, or emailed around by users. They may be disclosed to third parties via the Referrer header when any off-site links are followed. Placing session tokens into the URL increases the risk that they will be captured by an attacker.

- **Open Redirection (DOM-based) (Low – Tentative)**

  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.

This determination was identified utilizing tools that use static code analysis and, as such, may lead to false positives that are not exploitable.

- **Password field with autocomplete enabled (Low – Certain)**

  Most browsers have a facility to remember user credentials that are entered into HTML forms. This function can be configured by the user and by applications that employ user credentials. If the function is enabled, then credentials entered by the user are stored on their local computer and retrieved by the browser on future visits to the same application.

  The stored credentials can be captured by an attacker who gains control over the user's computer. Further, an attacker who finds a separate application vulnerability, such as cross-site scripting, may be able to exploit this to retrieve a user's browser-stored credentials.

Logical Telecomm Vulnerabilities

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

It should be noted, however, that the systems tested onsite utilized wireless communications. In the tested configurations, Robis is responsible for setting up and maintaining the wireless/wired Pepwave routers. At this time, it was confirmed that the wired access can be enabled or disabled depending upon requirements specified by the jurisdiction. It should be noted 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 as an example.

CONCLUSIONS

Physical Security

No specific findings were located within the physical portion of the **Robis AskED ePollbook CA** electronic poll book system.

No Vulnerabilities were located within the physical portion of the **Robis AskED ePollbook CA** electronic poll book system.

It is noted that physical security related documentation was not provided to detail how security seals or locks were to be applied.

It should be noted that jurisdictional polling place security processes and procedures play a large role in making sure that the **Robis AskED ePollbook CA** system 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 Telecommunications

Findings were located within the **Robis AskED ePollbook CA** electronic poll book system, in relation to physical communication hardware.

- All RJ-45 network ports on the COTS OKI printers were enabled.
- All physical access to the Pepwave SOHO router should be restricted, because the Pepwave SOHO router has the ability to be reset utilizing a small pinhole reset button.
- Ports on the Bak Atlas devices are enabled / accessible.
- Data ports on the OKI C711 are accessible and enabled.

No specific vulnerabilities were located within the **Robis AskED ePollbook CA** electronic poll book physical communication hardware.

Logical Security

Discrepancies were located within the **Robis AskED ePollbook CA** electronic poll book system during review. These discrepancies pertained to lack of documentation related to the procedures, configuration, and security hardening of all systems involved with the solution.

Five types of vulnerabilities were located within the **Robis AskED ePollbook CA** electronic poll book system related to the Command Central web application. These vulnerabilities ranged in severity from high to low. All vulnerabilities found were considered of minimal impact to the overall security of the **Robis AskED ePollbook CA** solution, due to in place security measures including IP filtering at the web server, as well as two factor authentication utilizing certificates. The web vulnerability scan of the application was completed using an administrative credentialed account.

The Bak Atlas devices sufficiently meet requirements by:

- WPA 2 Security with maximum character PSK.
- AES 256bit Encryption
- KIOSK mode enabled with a custom shell, Group Policy objects enabled and custom registry edits.

Notes:

1. The **Robis AskED ePollbook CA** system incorporates self-signed certificates for all devices that require access to backend / servers. The certificates generated are not tied to a specific user or computer which allows the certificates to be exported and imported onto unauthorized devices.
2. The Pepwave SOHO Device is setup to incorporate MAC address filtering. MAC address filtering by itself is easily circumvented utilizing passive reconnaissance.
3. The solution uses 63-character pre-shared keys (PSK) without a defined process or procedure. To control / create these keys may be cumbersome to jurisdictions or precincts that utilize this solution on their own.
4. The compromise of any single Bak Atlas machine may compromise the entire ePollbook solution at a specific location. Compromise allows an attacker access to:
    a. WPA2 pre-shared key (PSK)
    b. Certificate that controls part of the two-factor authentication to the Command Center.
    c. Connectivity from a trusted IP address to help bypass IP filtering
    d. The BitLocker recovery key (for the compromised machine)
5. The Pepwave management interface is accessible from the public internet.
6. IP filtering is being used as an authentication mechanism on the Microsoft IIS server. This still allows for incoming connections from unauthorized hosts and serves a 403 forbidden instead of just dropping traffic from unauthorized sources.

Logical Telecommunications

Three findings were located within the **Robis AskED ePollbook CA** electronic poll books system.

7. COTS Printers C532 and C711 both come with active network interface cards that are by default enabled and waiting for a dynamically assigned IP address to be assigned. Both of the printers were configured with default credentials for complete access to the printer functionality.
8. The PepWave Surf SOHO router's administrative interface is accessible publicly from the public internet.
9. Certificates used for two factor authentication aren't tied to specific devices. Allowing for the export of the certificate and installation of the certificate on unauthorized devices.

No vulnerabilities were located within the **Robis AskED ePollbook CA** telecomm system of the electronic poll books system.

While there are no specific logical telecommunications vulnerabilities to report with the components of the solution, the following concerns should be noted:

- Through passive monitoring and reconnaissance, MAC address filtering will not sufficiently stop an attacker.
- Certificates used for authentication that are not tied to a specific object will allow for the exportation and reuse of the certificate on unauthorized systems / users.
- The compromise of any single ePollbook device may compromise the entire polling place voter check-in system at a polling place. Much of the documentation describing the processes and procedures for administration and configuration of the ePollbook solution is missing, requiring the jurisdiction to rely on the vendor for all issues regarding connectivity.

Testing was conducted in an attempt to circumvent or exploit vulnerabilities within the communication systems as applicable and within Legal boundaries in respect to third party services where applicable.

The use of WPA 2 and a PSK that is 63+ characters in length, MAC address filtering, and the content filtering in use on the router fulfill the requirements for connectivity for ePollbook systems.

End of Security and Telecommunications Test Report