ES&S Security Overview
Pima County Election Integrity Committee

June 22, 2018

Agenda

- Introductions
- ES&S Commitment to Security
- Product Security
- EAC / VSTL Security Test Procedure
- Open Discussion

Introductions

- **Steve Pearson** – Sr. Vice President of Certification
- **Chris Wlaschin** – Vice President of System Security

Our Commitment to Security

- **Our Mission:**
  - To providing valuable, trusted, and proven election equipment and services to our election administrators
  - Continually evolve to meet the needs of our customers and technology's ever-changing environment
  - Delivering the highest standards of accuracy, security, and reliability in our election products and services

- In history of our company, there's been nothing like the last 24 months to make these words more important and challenge our commitment to security

Our Commitment to Security

ES&S: The Leader in Designing, Building, Testing, and Delivering Secure Election Systems, Software, and Services

Designing

- Contributed to the development of the *Center for Internet Security (CIS) Handbook for Elections Infrastructure Security.* ES&S has adopted and is actively using the CIS Handbook.
- Active participation in working groups shaping the VVSG 2.0 guidelines

Building

- ES&S added an executive who is solely focused on security of not only ES&S' internal networks but the voting systems deployed or currently in development
- Actively engaged with technologists in leading organizations to validate the security techniques of our voting systems (example: Bulletproof and Delkin)

Our Commitment to Security

ES&S: The Leader in Designing, Building, Testing, and Delivering Secure Election Systems, Software, and Services

Testing

- Adopted nationally recognized best practices around cybersecurity threat assessments and vulnerability scanning to continually assess our cybersecurity posture
- Nationally recognized organizations include: Department of Homeland Security (DHS), Multi-State Information Sharing and Analysis Center (MS-ISAC), and National Institute of Standards and Technology (NIST)
- Testing for vulnerabilities, sharing cyber security information, threat/incident reporting, and ongoing risk assessments further protect our voting system networks, processes, and technologies.

Delivering

- Security Seminars to county/state officials beginning in summer 2018

Federal Certification

- EAC Testing & Certification Testing Program v2.0
- Testing performed by EAC/NVLAP accredited Voting System Test Laboratories (SLI and Pro V&V)
- Security overview:
  - Hash Validation
  - Digital Signature verification for all transportable data
  - FIPS 140-2 level encryption
  - Certified USB media only
  - Strong User Access Controls

Product Security

Election Management System (EMS) w/Hardening – ES&S Policy

- Hardened environment - Only essential applications available
- Malware protected
- No Internet access
  - *Standalone*: Disable all wireless/network ports
  - *Client/Server*: Disable wireless ports – assign static IP address for closed network
- Requires a 'boot' password to continue booting to Windows OS
- Windows OS Users:
  - *sysadmin* – full control – can install/uninstall programs
  - *EAdmin* – only has access to ES&S programs
  - Strong passwords required – expires every 90 days, 12 characters in length, and contain a character in 3 of 4 categories

Product Security

Electionware (EMS) Access Controls

- Username and password required for entry
- Election Administrator creates users, assigns access levels, and defines password expiration (in days)

Tabulation Hardware Access Controls

- Password entry required for loading the election and to enter administrative menu. Optional password entry to close polls

Physical Security

- Locks and tamper evident seals on all devices
- Support for only certified ES&S Delkin USB Memory Devices
- Media Restore - protection tool to restore to “factory” state prior to next election use

Product Security

Encryption & Digital Signatures on all removable media (USBs)

- Only NIST approved cryptographic modules
- AES-256 Encryption
- RSA BSAFE Crypto-C ME and OpenSSL for Digital Signatures

System Logs

- *Windows Event Viewer* – Operating System events
- Each product has an audit log that records all user actions
- Logging must be active for EMS operation

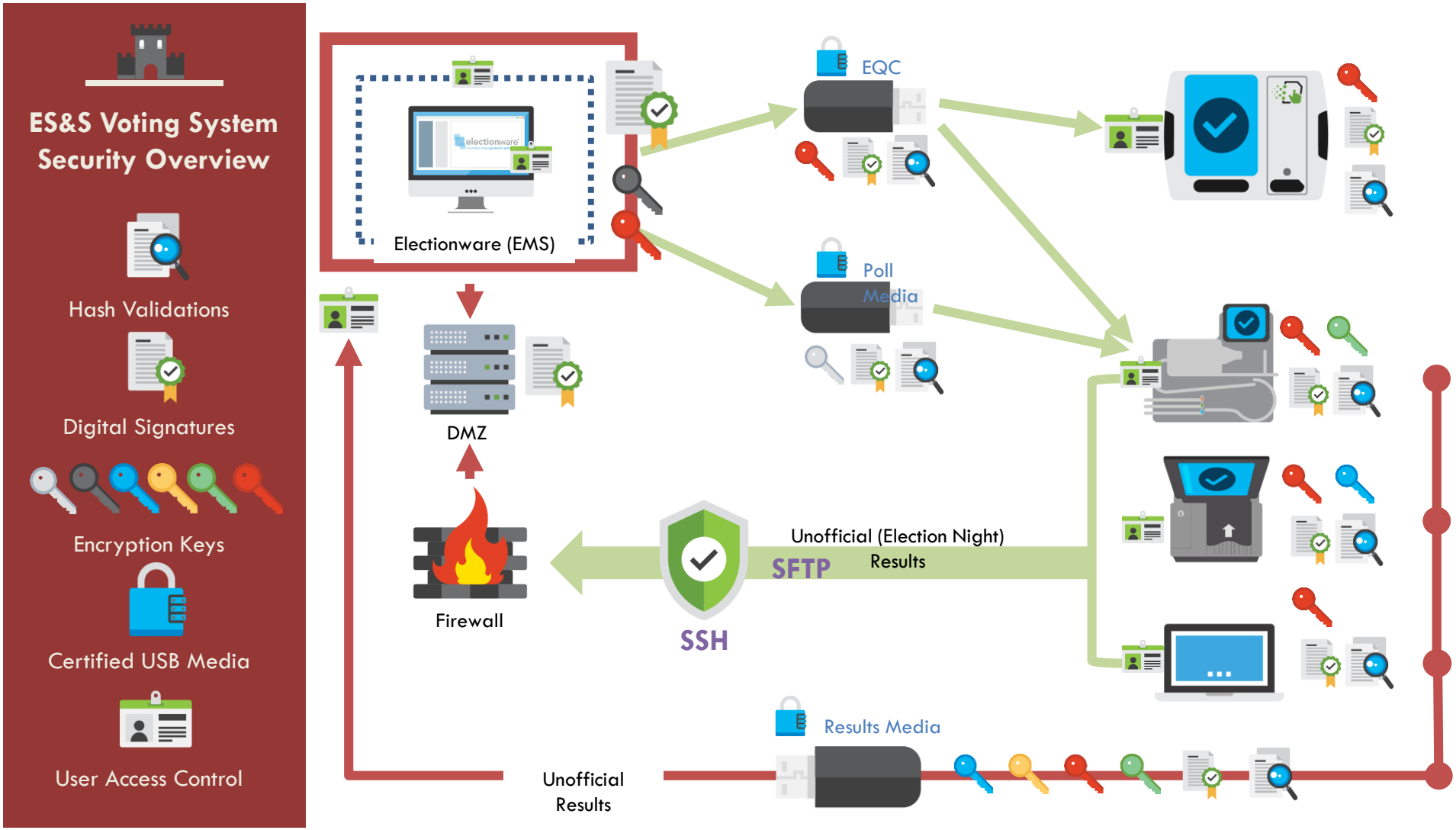
EAC / VSTL Security Test Process

- VSTL test suites designed to meet VVSG Vol. 1, Sect. 7
- Incorporates:
  - Systems security provisions
  - Unauthorized access
  - Deletion or modification of data
  - Audit trail data
  - Modification or alteration of security mechanisms
  - Vendor documentation detail and accuracy for best practices
  - Specific threat testing per “Known Vulnerabilities” data determined and maintained by VSTL’s
  - Testing performed at the individual component level and across the system

EAC / VSTL Security Test Process

- More examples:
  - Access controls and user privileges
  - Alteration of election results, audit trails, etc.
  - Physical security – polling place & central count location
  - Software security
    - SCAP and Nessus security content and vulnerability
    - Software and Firmware distribution and installation
    - Protection against malicious software
    - Hashes, digital signatures, and validation
    - Complete source code review for VVSG compliance
  - Telecommunications and Data Transmission
    - Maintaining date integrity, external threat protection and detection

ES&S Voting System Overview



Agenda

- ❑ Introductions
- ❑ ES&S Commitment to Security
- ❑ Product Security
- ❑ EAC / VSTL Security Test Procedure
- ❑ Open Discussion